ADMINISTRATOR-HANDBUCH

Cisco WAP571 Wireless-AC/N Premium Dual Radio Access Point mit PoE

Cisco WAP571E Wireless-AC/N Premium Dual Radio Outdoor Access Point

Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter folgender URL: www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine Partnerschaft zwischen Cisco und anderen Unternehmen. (1110R)

© 2018 Cisco Systems, Inc. Alle Rechte vorbehalten.

© 2015 Cisco Systems, Inc. Alle Rechte vorbehalten.

Inhalt

1

Erste Schritte

In diesem Abschnitt erhalten Sie eine Einführung in das webbasierte Konfigurationsdienstprogramm für WAP-Geräte (Wireless Access Points). Das Kapitel enthält die folgenden Themen:

Starten des webbasierten Konfigurationsdienstprogramms

In diesem Abschnitt werden die Systemanforderungen und die Navigation im webbasierten Konfigurationsdienstprogramm beschrieben.

Unterstützte Browser

- Internet Explorer 7.0 oder höher
- Chrome 5.0 oder höher
- Firefox 3.0 oder höher
- Safari 3.0 oder höher

Browsereinschränkungen

- Wenn Sie Internet Explorer 6 verwenden, können Sie nicht über eine IPv6-Adresse direkt auf den Access Point zugreifen. Sie können jedoch mit dem DNS-Server (Domain Name System) einen Domänennamen mit der IPv6-Adresse erstellen und diesen Domänennamen in der Adressleiste anstelle der IPv6-Adresse verwenden.

- Wenn Sie Internet Explorer 8 verwenden, können Sie die Sicherheitseinstellungen in Internet Explorer konfigurieren. Wählen Sie **Tools > Internetoptionen** und dann die Registerkarte **Sicherheit** aus. Wählen Sie **Lokales Intranet** und **Standorte**. Wählen Sie **Erweitert** und dann **Hinzufügen**. Fügen Sie die Intranetadresse des Access Points (http://*<IP-Adresse>*) der lokalen Intranetzone hinzu. Sie können die IP-Adresse auch als Subnetz-IP-Adresse angeben, sodass alle Adressen im Subnetz der 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 den Access Point zuzugreifen.

Abmelden

Standardmäßig meldet sich der webbasierte AP nach zehn Minuten Inaktivität ab. Anweisungen zum Ändern des Standard-Timeouts finden Sie unter **HTTP-/HTTPS-Service**.

Zum Abmelden klicken Sie in der rechten oberen Ecke des AP-Konfigurationsdienstprogramms auf **Abmelden**.

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:

Verwenden des Einrichtungsassistenten für Access Points

HINWEIS Wenn Sie auf **Abbrechen** klicken, um den Assistenten zu umgehen, wird die Seite **Kennwort ändern** angezeigt. Dort können Sie das Standardkennwort für die Anmeldung ändern. Für alle anderen Einstellungen gilt die werksseitige Standardkonfiguration.

Nach dem Ändern des Kennworts müssen Sie sich erneut anmelden.

SCHRITT 1 Klicken Sie auf der Willkommensseite des Assistenten auf **Weiter**. Das Fenster „Gerät konfigurieren – Firmware-Upgrade“ wird angezeigt.

SCHRITT 2 Klicken Sie auf die Schaltfläche Durchsuchen und suchen Sie die Firmware-Image-Datei in Ihrem Netzwerk.

HINWEIS 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. Oder klicken Sie auf **Überspringen**. Das Fenster „Gerät konfigurieren – Konfiguration wiederherstellen“ wird angezeigt.

HINWEIS Das Hochladen der neuen Firmware kann mehrere Minuten dauern. Beim Hochladen der neuen Firmware dürfen Sie nicht die Seite aktualisieren oder zu einer anderen Seite navigieren, da sonst der Firmware-Upload abgebrochen wird. Nach Abschluss des Vorgangs wird der Access Point neu gestartet und nimmt den Normalbetrieb wieder auf.

SCHRITT 4 Klicken Sie auf die Schaltfläche **Durchsuchen** und suchen Sie die Konfigurationsdatei in Ihrem Netzwerk.

HINWEIS Die Konfigurationsdatei muss im XML-Format vorliegen und alle Informationen zu den Einstellungen des WAP-Geräts enthalten.

SCHRITT 5 Klicken Sie auf **Upgrade**, um die ausgewählte Konfigurationsdatei zu übernehmen. Oder klicken Sie auf **Überspringen**. Das Fenster „Gerät konfigurieren – IP-Adresse“ wird angezeigt.

HINWEIS Die Wiederherstellung der Konfigurationsdatei kann mehrere Minuten dauern. Beim Wiederherstellen der Konfigurationsdatei dürfen Sie nicht die Seite aktualisieren oder zu einer anderen Seite navigieren, da sonst die Wiederherstellung der Konfiguration abgebrochen wird. Nach Abschluss des Vorgangs wird der Access Point neu gestartet und nimmt den Normalbetrieb wieder auf.

SCHRITT 6 Klicken Sie auf **Dynamic IP Address (DHCP)**, wenn das WAP-Gerät eine IP-Adresse von einem DHCP-Server beziehen soll. Wählen sie alternativ **Statische IP-Adresse** aus, um die IP-Adresse manuell zu konfigurieren. Eine Beschreibung dieser Felder finden Sie unter **IPv4-Einstellung**.

SCHRITT 7 Klicken Sie auf **Next** (Weiter). Das Fenster „Single Point Setup – Cluster festlegen“ 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 wählen Sie **Create a New Cluster** aus, und geben Sie in **New Cluster Name** den neuen Clusternamen an. Wenn Sie die Geräte mit dem gleichen Cluster-Namen konfigurieren und den Single Point Setup-Modus in 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 Clustername** 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) Sie können in das Feld „AP-Standort“ Text eingeben, aus dem der physische Standort des WAP-Geräts hervorgeht.

SCHRITT 9 Klicken Sie auf **Next** (Weiter). Das Fenster „Gerät konfigurieren – Systemdatum und -zeit festlegen“ wird angezeigt.

SCHRITT 10 Wählen Sie die Zeitzone aus, und legen Sie die Systemzeit manuell fest, oder richten Sie das WAP-Gerät so ein, dass es die Uhrzeit von einem NTP-Server bezieht. Eine Beschreibung dieser Optionen finden Sie unter **Zeiteinstellungen**.

HINWEIS Neben „Systemzeit“ wird ein Pfeil angezeigt, mit dem Sie die Zeit von Ihrem aktuellen Computer übertragen können, falls Sie Zeit und Datum Ihres Computers verwenden möchten.

SCHRITT 11 Klicken Sie auf **Next** (Weiter). Das Fenster „Sicherheit aktivieren – Kennwort festlegen“ wird angezeigt.

SCHRITT 12 Geben Sie ein **Neues Kennwort** ein und geben Sie es im Textfeld **Kennwort bestätigen** erneut ein, um es zu bestätigen. Sie können den Benutzernamen im Feld **Benutzername** ändern. Weitere Informationen zu Kennwörtern finden Sie unter **Benutzerkonten**.

HINWEIS Sie können das Kontrollkästchen „Kennwortkomplexität“ deaktivieren, wenn Sie die Regeln für die Kennwortsicherheit deaktivieren möchten. Es wird jedoch dringend empfohlen, die Regeln für die Kennwortsicherheit aktiviert zu lassen.

SCHRITT 13 Klicken Sie auf **Next** (Weiter). Das Fenster „Sicherheit aktivieren – WLAN benennen“ wird für die Funkschnittstelle 1 angezeigt.

HINWEIS In diesem Fenster und den beiden nächsten Fenstern („Wireless Security“ und „VLAN ID“) konfigurieren Sie diese Einstellungen zuerst für die Schnittstelle Radio1. Die Fenster werden dann erneut angezeigt, damit Sie diese Einstellungen für Radio 2 konfigurieren können.

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

SCHRITT 15 Klicken Sie auf **Next** (Weiter). Das Fenster „Enable Security - Secure Your Wireless Network“ wird angezeigt.

SCHRITT 16 Wählen Sie einen Sicherheitsverschlüsselungstyp aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter **Systemsicherheit**.

SCHRITT 17 Klicken Sie auf **Next** (Weiter). Der Assistent zeigt das Fenster „Enable Security-Assign the VLAN ID For Your Wireless Network“ an.

SCHRITT 18 Geben Sie eine VLAN-ID für im WLAN empfangenen Verkehr ein.

Sie sollten für WLAN-Verkehr eine andere VLAN-ID als den Standardwert (1) zuzuweisen. Dadurch soll dieser Verkehr vom Verwaltungsverkehr in VLAN1 getrennt werden.

SCHRITT 19 Klicken Sie auf **Next** (Weiter).

SCHRITT 20 Für das WAP571/E-Gerät werden die Seiten „Network Name“, „Wireless Security“ und „VLAN ID“ angezeigt, auf denen Sie das Funkmodul 2 konfigurieren können. Wenn Sie das Funkmodul 2 konfiguriert haben, klicken Sie auf **Weiter**.

Der Assistent zeigt das Fenster „Captive-Portal aktivieren – Gastnetzwerk erstellen“ an.

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, zeigt der Assistent das Fenster „Captive-Portal aktivieren – Gastnetzwerk benennen“ an.

SCHRITT 22 Geben Sie einen **Namen des Gastnetzwerks** für Funkmodul 1 an. Für das WAP571/E-Gerät können Sie auswählen, ob das Gastnetzwerk **Funkmodul 1** oder **Funkmodul 2** verwenden soll.

SCHRITT 23 Klicken Sie auf **Next** (Weiter). Der Assistent zeigt das Fenster „Captive-Portal aktivieren – Gastnetzwerk sichern“ an.

SCHRITT 24 Wählen Sie einen Sicherheitsverschlüsselungstyp für das Gastnetzwerk aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter **Systemsicherheit**.

SCHRITT 25 Klicken Sie auf **Next** (Weiter). Der Assistent zeigt das Fenster „Captive-Portal aktivieren – VLAN-ID zuweisen“ an.

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 **Next** (Weiter). Der Assistent zeigt das Fenster „Captive-Portal aktivieren – Umleitungs-URL aktivieren“ an.

SCHRITT 28 Wählen Sie die Option **Umleitungs-URL aktivieren** aus, und geben Sie in das Feld „Umleitungs-URL“ einen vollständigen Hostnamen oder eine IP-Adresse ein (einschließlich „http://“). Wenn eine URL angeben ist, werden Benutzer des Gastnetzwerks nach der Authentifizierung an diese URL umgeleitet.

SCHRITT 29 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster „Zusammenfassung – Einstellungen bestätigen“ an.

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 WAP-Setup-Einstellungen werden gespeichert, und es wird ein Bestätigungsfenster angezeigt.

SCHRITT 32 Klicken Sie auf **Fertigstellen**. Das Anmeldefenster wird angezeigt, damit Sie sich mit dem geänderten Kennwort beim Access Point anmelden können.

Erste Schritte

Zur Vereinfachung der Gerätekonfiguration durch eine Schnellnavigation enthält die Seite „Erste Schritte“ Links zum Ausführen allgemeiner Aufgaben. Die Seite „Erste Schritte“ wird immer, wenn Sie sich beim webbasierten AP-Konfigurationsdienstprogramm anmelden, als Standardfenster angezeigt.

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite
Ersteinrichtung	Einrichtungsassistenten ausführen	Verwenden des Einrichtungsassistenten für Access Points
	Funkeinstellungen konfigurieren	Funk
	WLAN-Einstellungen konfigurieren	Netzwerke
	Configure LAN Settings	LAN
	Single Point Setup konfigurieren	Single Point Setup – Übersicht
Gerätestatus	System Summary	Systemübersicht
	Wireless Status	Netzwerkschnittstellen

Kategorie	Link-Name (auf der Seite)	Verlinkte Seite
Schnellzugang	Kontokennwort ändern	Benutzerkonten
	Gerätefirmware aktualisieren	Firmware verwalten
	Konfiguration sichern/ wiederherstellen	Konfigurationsdatei herunterladen/sichern

Fensternavigation

Verwenden Sie den Navigationsbereich, um sich im webbasierten Dienstprogramm zu bewegen.

Header des Konfigurationsdienstprogramms

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

Navigationsbereich/Hauptmenü

Schaltflächenname	Beschreibung
(Benutzer)	Der Kontoname (Administrator oder Gast) des beim AP angemeldeten Benutzers. Der werksseitige Standardbenutzername lautet **cisco**.
Log Out	Klicken Sie, um sich vom webbasierten AP-Konfigurationsdienstprogramm abzumelden.
Sprache	Bewegen Sie den Mauszeiger über die Schaltfläche und wählen Sie Ihre Sprache aus.
About	Klicken Sie auf diese Schaltfläche, um Typ und Versionsnummern für den AP anzuzeigen.
Help	Klicken Sie auf diese Schaltfläche, um die 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.

Links auf jeder Seite befindet sich ein Navigationsbereich oder Hauptmenü. Der Navigationsbereich enthält eine Liste der Funktionen der obersten Ebene der WAP-Geräte. 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 Tabelle werden die am häufigsten verwendeten Schaltflächen beschrieben, die auf den verschiedenen Seiten des Systems zur Verfügung stehen.

Schaltflächenname	Beschreibung
Hinzufüg.	Fügt der Tabelle oder Datenbank einen neuen Eintrag hinzu.
Abbrechen	Bricht die auf der Seite vorgenommenen Änderungen ab.
Alle löschen	Löscht alle Einträge in der Protokolltabelle.
About	Klicken Sie auf diese Schaltfläche, um Typ und Versionsnummern für den AP anzuzeigen.
Löschen	Löscht einen Eintrag in einer Tabelle. Wählen Sie zuerst einen Eintrag aus.
Bearbeiten	Bearbeitet oder ändert einen vorhandenen Eintrag. Wählen Sie zuerst einen Eintrag aus.
Aktualisieren	Zeigt die aktuelle Seite mit den neuesten Daten erneut an.
Speichern	Speichert die Einstellungen oder die Konfiguration.
Aktualisieren	Aktualisiert die Startkonfiguration mit den neuen Informationen.

2

Status und Statistik

In diesem Abschnitt wird beschrieben, wie Sie Status und Statistiken anzeigen. Das Kapitel enthält die folgenden Themen:

- **Systemübersicht**
- **Netzwerkschnittstellen**
- **Verkehrsstatistik**
- **Wireless Multicast Forwarding-Statistik**
- **WorkGroup-Bridge senden/empfangen**
- **Zugeordnete Clients**
- **TSPEC-Clientzuordnungen**
- **TSPEC-Status und -Statistik**
- **TSPEC-AP-Statistik**
- **Funkstatistik**
- **E-Mail-Warnungsstatus**
- **Protokoll**

Systemübersicht

Auf der Seite „Systemübersicht“ werden grundlegende Informationen angezeigt, beispielsweise die Beschreibung des Hardwaremodells, die Softwareversion und die seit dem letzten Neustart verstrichene Zeit.

Um Systeminformationen anzuzeigen, wählen Sie **Status und Statistiken** > **Systemübersicht**. Alternativ können Sie auf der Seite „Erste Schritte“ unter **Gerätestatus** die Option **Systemübersicht** auswählen.

Auf der Seite „Systemübersicht“ werden die folgenden Informationen angezeigt:

- **PID: VID**: Hardwaremodell und -version des WAP-Geräts
- **Seriennummer**: Die Seriennummer des Cisco WAP-Geräts
- **MAC-Basisadresse**: Die MAC-Adresse des WAP-Geräts
- **Firmware-Version (Active Image)**: Die Firmwareversion des aktiven Images
- **Firmware-MD5-Prüfsumme (Active Image)**: Die Prüfsumme des aktiven Images
- **Firmware-Version (inaktives Image)**: Die Firmwareversionsnummer des Backup-Images
- **Firmware-MD5 Prüfsumme (inaktives Image)**: Die Prüfsumme des Backup-Images
- **Hostname**: Ein dem Gerät zugewiesener Name
- **Systembetriebszeit**: Die seit dem letzten Neustart verstrichene Zeit
- **Systemzeit**: Die aktuelle Systemzeit
- **Stromquelle**: Das System erhält Power-over-Ethernet von PoE-PSEs

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

- **Service**: Der Name des Diensts, falls verfügbar
- **Protokoll**: Das vom Dienst verwendete zugrunde liegende Transportprotokoll (TCP oder UDP)
- **Lokale IP-Adresse**: Gegebenenfalls die IP-Adresse eines Remotegeräts, das mit diesem Service im WAP-Gerät verbunden ist. **Alle** bedeutet, dass jede IP-Adresse im Gerät diesen Dienst verwenden kann.

- **Lokaler Port**: Die Portnummer für den Dienst
- **Remote-IP-Adresse**: Gegebenenfalls 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**: Gibt an, ob der WAN-Anschluss mit dem Internetdienstanbieter verbunden ist. 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.
  - **Hergestellt**: Eine Verbindungssitzung zwischen dem WAP-Gerät und einem Server oder Client ist hergestellt, abhängig von der Rolle der einzelnen Geräte im Hinblick auf dieses Protokoll.
  - **Wartezeit**: Die Schlusssequenz wurde initiiert, und der WAP wartet vor dem Schließen der Verbindung während eines vom System definierten Timeout-Zeitraums (in der Regel 60Sekunden).

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

Netzwerkschnittstellen

Auf der Seite „Netzwerkschnittstellen“ können Sie Konfigurations- und Statusinformationen zu den drahtgebundenen Schnittstellen und WLAN-Schnittstellen anzeigen. Um Netzwerkschnittstelleninformationen anzuzeigen, wählen Sie „Status und Statistiken > Netzwerkschnittstellen“ aus.

Die folgenden Informationen werden angezeigt:

- **LAN-Status** – Zeigt Informationen zur LAN-Schnittstelle an, darunter:
  - **MAC-Adresse**: Die MAC-Adresse des IP-Geräts
  - **IP-Adresse**: Die IP-Adresse des WAP-Geräts
  - **Subnetzmaske**: Subnetzmaske des USB-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
- **IP-Adresse**: Die IPv6-Adresse des IP-Geräts
- **Automatisch konfigurierte globale IPv6-Adressen –** Die automatisch konfigurierte globale IPv6-Adresse
- **IPv6-Link Local-Adresse**: Die IPv6-Link Local-Adresse des WAP-Geräts
- **IPv6-Standardgateway**: Der 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

Diese Einstellungen gelten für die interne Schnittstelle. Klicken Sie auf „Bearbeiten“, wenn Sie diese Einstellungen ändern möchten. Sie werden auf die Seite **IPv4-Einstellung** weitergeleitet.

- **Anschlussstatus**: Zeigt den Status für LAN-Schnittstellen an.
- **Schnittstellen**: Die Nummer der Ethernet-Schnittstelle
  - **Linkstatus**: Status der Ethernet-Schnittstelle
  - **Portgeschwindigkeit**: Geschwindigkeit der Ethernet-Schnittstelle
  - **Duplexmodus**: Duplexmodus der Ethernet-Schnittstelle
  - **Green Ethernet-Status**: Der Status der Ethernet-Schnittstelle

Klicken Sie auf „Bearbeiten“, wenn Sie diese Einstellungen ändern möchten. Sie werden auf die Seite **Porteinstellungen** weitergeleitet.

- **VLAN-Status**: Zeigt Informationen für alle bestehenden VLANs an, darunter:
  - **VLAN-ID**: Identifikator des VLANs.
  - **Beschreibung**: Beschreibung des VLANs
  - **Ethernet**: Die Schnittstelle gehört dem VLAN als Mitglied mit Tag oder ohne Tag an.

Klicken Sie auf „Bearbeiten“, wenn Sie diese Einstellungen ändern möchten. Sie werden auf die Seite **VLAN-Konfiguration** weitergeleitet.

- **Funkstatus**: Zeigt Informationen zu den Wireless-Funkschnittstellen an, darunter:
  - **WLAN-Funk**: Der WLAN-Funkmodus ist für die Funkschnittstelle aktiviert oder deaktiviert.
  - **MAC-Adresse**: Die MAC-Adresse, die der Funkschnittstelle zugordnet ist.
  - **Modus**: Der 802.11-Modus (a/b/g/n/ac), der von der Funkschnittstelle verwendet wird.
  - **Kanal**: Der von der Funkschnittstelle verwendete Kanal.
  - **Betriebsbandbreite**: Die Betriebsbandbreite, die von der Funkschnittstelle verwendet wird.

Klicken Sie auf „Bearbeiten“, wenn Sie diese Einstellungen ändern möchten. Sie werden auf die Seite **Funk** weitergeleitet.

- **Schnittstellenstatus**: Zeigt Statusinformationen für die einzelnen VAPs (Virtual Access Points) und WDS-Schnittstellen (Wireless Distribution System) an, darunter:
- **Schnittstelle**: 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.

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

Verkehrsstatistik

Auf der Seite „Verkehrsstatistik“ können Sie grundlegende Informationen zum WAP anzeigen. Außerdem werden Sende- und Empfangsstatistiken für die Ethernet-Schnittstelle, die VAPs (Virtual Access Points) und gegebenenfalls die WDS-Schnittstellen in Echtzeit angezeigt. Alle Sende- und Empfangsstatistiken geben die Gesamtmengen seit dem letzten Start des WAP-Geräts wieder. Wenn Sie den WAP neu starten, gehen aus diesen Zahlen die insgesamt gesendeten und empfangenen Mengen seit dem Neustart hervor.

Zum Anzeigen der Seite „Verkehrsstatistik“ wählen Sie im Navigationsbereich **Status und Statistiken** > **Verkehrsstatistik** aus.

Auf der Seite „Datenverkehrstatistik“ werden zusammengefasste Daten und Statistiken für den Verkehr in beiden Richtungen angezeigt.

- **Netzwerkschnittstelle**: Die Namen der Ethernet-Schnittstelle und der einzelnen VAP- und WDS-Schnittstellen

  Dem Namen der VAP-Schnittstelle sind die Zeichenfolgen WLAN0 und WLAN1 vorangestellt, die auf die Funkschnittstelle hinweisen. (WLAN0 steht für Funkmodul 1 und WLAN1 für Funkmodul 2.)

- **Pakete gesamt**: Die Gesamtanzahl der von diesem Funkmodul gesendeten (in der Tabell „Senden“) oder empfangenen (in der Tabelle „Empfangen“) TS-Pakete für die angegebene Zugriffskategorie

- **Bytes gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät gesendeten (in der Tabelle „Senden“) oder empfangenen Bytes (in der Tabelle „Empfangen“)

- **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 über dieses WAP-Gerät

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

Wireless Multicast Forwarding-Statistik

Die Seite **Wireless Multicast Forwarding-Statistiken** bietet einige grundlegende Informationen zum aktuellen AP. Außerdem werden Sende- und Empfangsstatistiken für die Wireless Multicast Traffic-Schnittstelle am AP und die VAPs auf beiden Funkschnittstellen bereitgestellt. Alle angezeigten Sende- und Empfangsstatistiken werden als Gesamtmengen seit dem letzten Start der AP angezeigt. Wenn Sie den AP neu starten, gehen aus diesen Zahlen die insgesamt gesendeten und empfangenen Mengen seit dem Neustart hervor.

Um die Seite „WMF-Statistik“ anzuzeigen, wählen Sie im Navigationsbereich **Status und Statistiken > Wireless Multicast Forwarding-Statistiken** aus.

Sende-/Empfangsstatistik

- **Netzwerkschnittstelle**: Die Namen der Ethernet-Schnittstelle und der einzelnen VAP- und WDS-Schnittstellen

  Dem Namen der VAP-Schnittstelle sind die Zeichenfolgen WLAN0 und WLAN1 vorangestellt, die auf die Funkschnittstelle hinweisen. (WLAN0 steht für Funkmodul 1 und WLAN1 für Funkmodul 2.)

- **Multicast-Daten-Frames**: Es werden Informationen zu empfangenen Multicast-Daten-Frames angezeigt.
- **Weitergeleitete Multicast-Daten**: Gibt weitergeleitete Multicast-Daten an.
- **Geflutete Multicast-Daten**: Gibt geflutete Multicast-Daten an.
- **Gesendete Multicast-Daten**: Gibt gesendete Multicast-Daten an.
- **Gelöschte Multicast-Daten**: Gibt gelöschte Multicast-Daten an.
- **Mfdb-Cachetreffer**: Zeigt MFDB-Cachetreffer an
- **Mfdb-Cachefehler**: Gesendete Multicast-Daten-Frames.

IGMP-Statistik

- **Netzwerkschnittstelle**: Die Namen der Ethernet-Schnittstelle und der einzelnen VAP- und WDS-Schnittstellen

  Dem Namen der VAP-Schnittstelle sind die Zeichenfolgen WLAN0 und WLAN1 vorangestellt, die auf die Funkschnittstelle hinweisen. (WLAN0 steht für Funkmodul 1 und WLAN1 für Funkmodul 2.)

- **IGMP-Frames**: Zeigt empfangene IGMP-Frames an.

- **Weitergeleitete IGMP-Frames**: Zeigt empfangene Anfragen auf IGMP-Mitgliedschaft an.
- **Weitergeleitete IGMP-Frames**: Zeigt gesehene IGMP-Mitgleidschaftsberichte an.
- **MFDB-Cachetreffer**: Zeigt MFDB-Cachetreffer an.
- **MFDB-Cachefehler**: Zeigt MFDB-Cachefehler an.

Multicast-Gruppe

- **Netzwerkschnittstelle**: Die Namen der Ethernet-Schnittstelle und der einzelnen VAP- und WDS-Schnittstellen

  Dem Namen der VAP-Schnittstelle sind die Zeichenfolgen WLAN0 und WLAN1 vorangestellt, die auf die Funkschnittstelle hinweisen. (WLAN0 steht für Funkmodul 1 und WLAN1 für Funkmodul 2.)
- **Multicast-Gruppe**: Zeigt Multicast-Gruppen-IP-Adressen an.
- **Stationen**: Zeigt die Multicast-Gruppenstations-MAC-Adresse an.
- **Pakete**: Zeigt empfangene Multicast-Gruppenstations-Pakete an.

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

WorkGroup-Bridge senden/empfangen

Auf der Seite „WorkGroup Bridge senden/empfangen“ werden Paket- und Byte-Zahlen für Verkehr zwischen Stationen in einer WorkGroup-Bridge angezeigt. Weitere Informationen zum Konfigurieren von WorkGroup-Bridges finden Sie unter **WorkGroup-Bridge**.

Zum Anzeigen der Seite „WorkGroup-Bridge senden/empfangen“ wählen Sie im Navigationsbereich **Status und Statistiken** > **WorkGroup Bridge** aus.

Für jede als WorkGroup-Bridge-Schnittstelle konfigurierte Netzwerkschnittstelle werden die folgenden Felder angezeigt:

- **Netzwerkschnittstelle**: Der Name der Ethernet- oder VAP-Schnittstelle. WLAN0 steht für Radio 1 und WLAN1 für Radio 2.
- **Status und Statistiken**: Gibt an, ob die Schnittstelle getrennt oder administrativ als aktiv oder nicht aktiv konfiguriert ist.

- **VLAN ID**: Virtuelle LAN-ID (VLAN). Mithilfe von VLANs können Sie im gleichen WAP-Gerät mehrere interne Netzwerke und Gastnetzwerke einrichten. Die VLAN-ID legen Sie auf der Registerkarte „VAP“ fest.
- **Name (SSID)**: Der WLAN-Name. Mit diesem auch als SSID bezeichneten alphanumerischen Namen wird ein WLAN eindeutig identifiziert. Die SSID legen Sie auf der Registerkarte „VAP“ fest.

Für jede WorkGroup-Bridge-Schnittstelle werden zusätzliche Informationen für die Sende- und Empfangsrichtung angezeigt:

- **Pakete gesamt**: Die Gesamtanzahl der überbrückten Pakete zwischen den drahtgebundenen Clients in der WorkGroup-Bridge und dem WLAN
- **Bytes gesamt**: Die Gesamtanzahl der überbrückten Bytes zwischen den drahtgebundenen Clients in der WorkGroup-Bridge und dem WLAN

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

Zugeordnete Clients

Auf der Seite „Zugeordnete Clients“ können Sie die Clientstationen anzeigen, die einem bestimmten Access Point zugeordnet sind.

Zum Anzeigen der Seite „Zugeordnete Clients“ wählen Sie **Status und Statistiken** > **Zugeordnete Clients** aus.

Die zugeordneten Stationen werden zusammen mit Informationen zum gesendeten und empfangenen Paketverkehr für die einzelnen Stationen angezeigt.

- **Gesamtzahl zugeordnete Clients**: Die Gesamtanzahl der Clients, die zurzeit dem AP zugeordnet sind
- **Netzwerkschnittstelle**: Der VAP, dem der Client zugeordnet ist. Dem Namen der VAP-Schnittstelle sind die Zeichenfolgen WLAN0 und WLAN1 vorangestellt, die auf die Funkschnittstelle hinweisen. (WLAN0 steht für Funkmodul 1 und WLAN1 für Funkmodul 2.)
- **Station**: Die MAC-Adresse des zugeordneten WLAN-Clients
- **Status**: Der Status „Authentifiziert und zugeordnet“ zeigt die zugrunde liegende IEEE 802.11-Authentifizierung und den Zuordnungsstatus an, der unabhängig von dem vom Client für die Verbindung mit dem WAP-Gerät verwendeten Sicherheitstyp vorhanden ist. Der IEEE 802.1X-Authentifizierungsstatus oder Zuordnungsstatus wird hier nicht angezeigt.

Berücksichtigen Sie bei diesem Feld Folgendes:

- Wenn der Sicherheitsmodus des WAP-Geräts „Keine“ oder „Static WEP“ entspricht, wird für Clients der erwartete Authentifizierungs- und Zuordnungsstatus angezeigt. Das heißt, wenn ein Client als gegenüber dem WAP-Gerät authentifiziert angezeigt wird, kann der Client Daten senden und empfangen. (Der Grund hierfür ist, dass bei „Static WEP“ nur IEEE 802.11-Authentifizierung verwendet wird.)
- Wenn das WAP-Gerät IEEE 802.1X- oder WPA-Sicherheit verwendet, kann eine Clientzuordnung als (über IEEE 802.11-Sicherheit) authentifiziert angezeigt werden, obwohl die Clientzuordnung tatsächlich nicht durch die zweite Sicherheitsebene authentifiziert wird.

- **Von Station/An Station**: Die Zähler für „Von Station“ geben die vom WLAN-Client übertragenen Pakete oder Bytes an. Für „To Station“ geben die Zähler die Anzahl der vom WAP-Gerät an den WLAN-Client gesendeten Pakete und Bytes an.
  - **Pakete**: Die Anzahl der vom WLAN-Client empfangenen (gesendeten) Pakete
  - **Bytes**: Die Anzahl der vom WLAN-Client empfangenen (gesendeten) Bytes
  - **Gelöschte Pakete**: Die Anzahl der nach dem Empfang (nach dem Senden) gelöschten Pakete
  - **Gelöschte Bytes**: Die Anzahl der nach dem Empfang (nach dem Senden) gelöschten Bytes
  - **TS-Pakete mit Verstoß (Von Station)**: Die Anzahl der von einer Clientstation an das WAP-Gerät gesendeten Pakete, die die Uplink-Bandbreite für den aktiven Verkehrsstrom (Traffic Stream, TS) überschreiten, oder für eine Zugriffskategorie, die Zugangskontrolle erfordert und für die die Clientstation nicht zugelassen ist
  - **TS-Pakete mit Verstoß (An Station)**: Die Anzahl der vom WAP-Gerät an eine Clientstation gesendeten Pakete, die die Downlink-Bandbreite für den aktiven Verkehrsstrom überschreiten, oder für eine Zugriffskategorie, die Zugangskontrolle erfordert und für die die Clientstation nicht zugelassen ist
- **Laufzeit**: Gibt an, wie lange der Client dem WAP-Gerät zugeordnet war.

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

TSPEC-Clientzuordnungen

Auf der Seite „TSPEC-Clientzuordnungen“ werden Echtzeitinformationen zu den von diesem Access Point gesendeten und empfangenen TSPEC-Clientdaten angezeigt. In den Tabellen auf der Seite „TSPEC-Clientzuordnungen“ werden die seit Beginn der Zuordnung gesendeten und empfangenen Pakete sowie Statusinformationen angezeigt.

TSPEC (Traffic Specification) ist eine Verkehrsspezifikation, die von einem QoS-fähigen WLAN-Client an ein WAP-Gerät gesendet wird und in einem bestimmten Umfang Netzwerkzugriff für den von ihm repräsentierten Verkehrsstrom (Traffic Stream, TS) anfordert. Bei einem Verkehrsstrom handelt es sich um eine Sammlung von Datenpaketen, die vom WLAN-Client als zu einer bestimmten Benutzerpriorität gehörend identifiziert werden. Ein Beispiel für einen Sprachverkehrsstrom ist ein Wi-Fi-zertifiziertes Telefonmobilteil, dessen durch einen Codec generierte Datenpakete als Verkehr mit Sprachpriorität markiert werden. Ein Beispiel für einen Videoverkehrsstrom ist eine Anwendung für Videowiedergabe auf einem WLAN-Laptop, die einen Videokonferenz-Feed von einem Unternehmensserver priorisiert.

Zum Anzeigen von Statistiken für TSPEC-Clientzuordnungen wählen Sie im Navigationsbereich **Status und Statistiken > TSPEC-Clientzuordnungen** aus.

Auf der Seite „TSPEC-Clientzuordnungen“ werden die folgenden Informationen angezeigt:

Status und Statistiken:

- **Netzwerkschnittstelle**: Die vom Client verwendete Funkschnittstelle WLAN0 steht für Radio 1 und WLAN1 für Radio 2.
- **SSID**: Die diesem TS-Client zugeordnete SSID (Service Set Identifier)
- **Station**: Die MAC-Adresse der Clientstation
- **TS-Identifikator**: Die ID der TSPEC-Verkehrssitzung (Bereich: 0 bis 7)
- **Zugriffskategorie**: Die TS-Zugriffskategorie (Sprache oder Video)
- **Richtung**: Die Verkehrsrichtung für diesen TS. Für „Direction“ ist eine der folgenden Optionen möglich:
  - „uplink“: Vom Client zum Gerät
  - „downlink“: Vom Gerät zum Client
  - „bidirectional“

- **Benutzerpriorität**: Die Benutzerpriorität (User Priority, UP) für diesen TS. Die Benutzerpriorität wird mit jedem Paket im UP-Abschnitt des IP-Headers gesendet. Die typischen Werte lauten wie folgt:
  - 6 oder 7 für Sprache
  - 4 oder 5 für Video

  Abhängig von anderen Prioritätsverkehrssitzungen sind unterschiedliche Werte möglich.
- **Mittlere Zeit**: Gibt an, wie lange der TS-Verkehr das Übertragungsmedium belegt.
- **Anzahl Überschreitungsereignisse**: Gibt an, wie oft der Client die für TSPEC festgelegte mittlere Zeit überschritten hat. Geringfügige seltene Verstöße werden ignoriert.
- **VAP-MAC-Adresse**: MAC-Adresse des virtuellen Access Points

Statistiken:

- **Netzwerkschnittstelle**: Die vom Client verwendete Funkschnittstelle
- **Station**: Die MAC-Adresse der Clientstation
- **TS-Identifikator**: Die ID der TSPEC-Verkehrssitzung (Bereich: 0 bis 7)
- **Zugriffskategorie**: Die TS-Zugriffskategorie (Sprache oder Video)
- **Richtung**: Die Verkehrsrichtung für diesen TS. Für „Direction“ ist eine der folgenden Optionen möglich:
  - „uplink“: Vom Client zum Gerät
  - „downlink“: Vom Gerät zum Client
  - „bidirectional“
- **Von Station**: Zeigt die Anzahl der Pakete und Bytes an, die vom WLAN-Client empfangen wurden.
  - **Pakete**: Die Anzahl der Pakete, die eine zugelassene TSPEC überschreiten
  - **Bytes**: Die Anzahl der Bytes, für die keine TSPEC festgelegt ist und die vom WAP-Gerät zugelassen werden müssen

- **An Station**: Die Anzahl der Pakete und Bytes, die vom WAP-Gerät an den WLAN-Client übertragen wurden.
  - **Pakete**: Die Anzahl der Pakete, die eine zugelassene TSPEC überschreiten
  - **Bytes**: Die Anzahl der Bytes, für die keine TSPEC festgelegt ist und die vom WAP-Gerät zugelassen werden müssen

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

TSPEC-Status und -Statistik

Auf der Seite „TSPEC-Status und -Statistik“ werden die folgenden Informationen angezeigt:

- Zusammenfassende Informationen zu TSPEC-Sitzungen nach Funkmodulen
- Zusammenfassende Informationen zu TSPEC-Sitzungen nach VAPs
- Sende- und Empfangsstatistiken in Echtzeit für die Funkschnittstelle und die Netzwerkschnittstellen

Alle angezeigten Sende- und Empfangsstatistiken werden als Gesamtmengen seit dem letzten Start des WAP-Geräts angezeigt. Wenn Sie das WAP-Gerät neu starten, gehen aus diesen Zahlen die insgesamt gesendeten und empfangenen Mengen seit dem Neustart hervor.

Zum Anzeigen des TSPEC-Status und der TSPEC-Statistiken wählen Sie im Navigationsbereich **Status und Statistiken > TSPEC-Status und -Statistik** aus.

Auf der Seite „TSPEC-Status und -Statistik“ werden die folgenden Statusinformationen für die WLAN-Schnittstellen (Funk) und VAP-Schnittstellen angezeigt:

- **Netzwerkschnittstelle**: Der Name der Funkschnittstelle oder VAP-Schnittstelle. WLAN0 steht für Radio 1 und WLAN1 für Radio 2.
- **Zugriffskategorie**: Die aktuelle Zugriffskategorie, die diesem Verkehrsstrom zugeordnet ist (Sprache oder Video)
- **Status**: Gibt an, ob die TSPEC-Sitzung für die entsprechende Zugriffskategorie aktiviert (aktiv) oder nicht aktiviert (nicht aktiv) ist.

HINWEIS Beim Status handelt es sich um einen Konfigurationsstatus, der nicht zwangsläufig die aktuellen Sitzungsaktivitäten darstellt.

- **Aktiver Verkehrsstrom**: Die Anzahl der zurzeit aktiven TSPEC-Verkehrsströme für dieses Funkmodul und diese Zugriffskategorie
- **Verkehrsstromclients**: Die Anzahl der TS-Clients, die diesem Funkmodul und dieser Zugriffskategorie zugeordnet sind
- **Mittlere zugeteilte Zeit**: Die Zeit, die dieser Zugriffskategorie für die Übertragung von Daten über das Übertragungsmedium zugewiesen ist. Dieser Wert sollte kleiner oder gleich der maximalen Bandbreite sein, die für diesen Verkehrsstrom über dieses Medium zulässig ist.
- **Mittlere nicht zugewiesene Zeit**: Die Zeit für die nicht verwendete Bandbreite für diese Zugriffskategorie

Diese Statistiken werden für die Sende- und Empfangspfade der WLAN-Funkschnittstelle separat angezeigt:

- **Zugriffskategorie**: Die Zugriffskategorie, die diesem Verkehrsstrom zugeordnet ist (Sprache oder Video)
- **Pakete gesamt**: Die Gesamtanzahl der von diesem Funkmodul gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) TS-Pakete für die angegebene Zugriffskategorie
- **Bytes gesamt**: Die Gesamtanzahl der in der angegebenen Zugriffskategorie empfangenen Bytes

Diese Statistiken werden für die Sende- und Empfangspfade der Netzwerkschnittstellen (VAPs) separat angezeigt:

- **Sprachpaket gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle „Übertragen“) oder empfangenen (in der Tabelle „Empfangen“) TS-Sprachpakete
- **Sprachbyte gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) TS-Sprachbytes
- **Videopakete gesamt**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) TS-Videopakete
- **Videobyte gesamz**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle „Senden“) oder empfangenen (in der Tabelle „Empfangen“) TS-Videobytes

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

TSPEC-AP-Statistik

Auf der Seite „TSPEC-AP-Statistik“ werden Informationen zu den vom WAP-Gerät akzeptierten und abgelehnten Sprach- und Videoverkehrsströmen angezeigt. Zum Anzeigen der Seite „TSPEC-AP-Statistik“ wählen Sie im Navigationsbereich **Status und Statistiken > TSPEC-AP-Statistik** aus.

- **TSPEC Statistics Summary for Voice ACM**: Die Gesamtanzahl der akzeptierten und abgelehnten Sprachverkehrsströme
- **Zusammenfassung der TSPEC-Statistik für Video-ACM**: Die Gesamtanzahl der akzeptierten und abgelehnten Videoverkehrsströme

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

Funkstatistik

Auf der Seite „Funkstatisitik“ können Sie Statistiken auf Paketebene und auf Byte-Ebene für die einzelnen Funkschnittstellen anzeigen. Zum Anzeigen der Seite „Funkstatistik“ wählen Sie im Navigationsbereich **Status und Statistiken > Funkstatistik** aus.

Beim WAP571/E-Gerät wählen Sie das Funkmodul aus, für das Sie Statistiken anzeigen möchten.

- **Empfangene Pakete**: Die Gesamtanzahl der vom WAP-Gerät empfangenen Pakete
- **Gesendete Pakete**: Die Gesamtanzahl der vom WAP-Gerät gesendeten Pakete
- **Empfangene Bytes**: Die Gesamtanzahl der vom WAP-Gerät empfangenen Bytes
- **Gesendete Bytes**: Die Anzahl der vom WAP-Gerät empfangenen Pakete, die gelöscht wurden

- **Gelöschte empfangene Pakete**: Die Anzahl der vom WAP-Gerät empfangenen Pakete, die gelöscht wurden
- **Gelöschte gesendete Pakete**: Die Anzahl der vom WAP-Gerät gesendeten Pakete, die gelöscht wurden
- **Gelöschte empfangene Bytes**: Die Anzahl der vom WAP-Gerät empfangenen Bytes, die gelöscht wurden
- **Gelöschte gesendete Bytes**: Die Anzahl der vom WAP-Gerät gesendeten Bytes, die gelöscht wurden
- **Empfangene Fragmente**: Die Anzahl der vom WAP-Gerät empfangenen fragmentierten Frames
- **Gesendete Fragmente**: Die Anzahl der vom WAP-Gerät gesendeten fragmentierten Frames
- **Empfangene Multicast-Frames**: Die Anzahl der empfangenen MSDU-Frames, bei denen das Multicast-Bit in der MAC-Zieladresse festgelegt war
- **Gesendete Multicast-Frames**: Die Anzahl der erfolgreich gesendeten MSDU-Frames, bei denen das Multicast-Bit in der MAC-Zieladresse festgelegt war
- **Anzahl doppelte Frames**: Gibt an, wie oft ein Frame empfangen wurde, bei dem aus dem Feld „Sequenzkontrolle“ hervorging, dass es sich um ein Duplikat handelte.
- **Anzahl fehlgeschlagene Sendevorgänge**: Gibt an, wie oft ein MSDU nicht erfolgreich gesendet wurde, da bei den Sendeversuchen der kurze oder lange Wiederholungsgrenzwert überschritten wurde.
- **Anzahl FCS-Fehler**: Die Anzahl der in einem empfangenen MPDU-Frame erkannten Fehler
- **Anzahl Sendewiederholungen**: Gibt an, wie oft ein MSDU nach mindestens einer Wiederholung erfolgreich gesendet wurde.
- **Anzahl ACK-Fehler**: Die Anzahl der ACK-Frames, die nicht wie erwartet empfangen wurden
- **Anzahl RTS-Fehler**: Die Anzahl der CTS-Frames, die nicht als Antwort auf einen RTS-Frame empfangen wurden
- **Anzahl nicht entschlüsselbare WEP-Frames**: Die Anzahl der Frames, die verworfen wurden, da sie vom Funkmodul nicht entschlüsselt werden konnten. Frames können verworfen werden, da der Frame nicht oder mit einer vom WAP-Gerät nicht unterstützten Datenschutzoption verschlüsselt war.

- **Anzahl erfolgreiche RTS**: Die Anzahl der CTS-Frames, die als Antwort auf einen RTS-Frame empfangen wurden
- **Anzahl mehrere Wiederholungen**: Gibt an, wie oft ein MSDU nach mehreren Wiederholungen erfolgreich gesendet wurde.
- **Anzahl gesendete Frames**: Die Anzahl der erfolgreich gesendeten MSDUs

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

E-Mail-Warnungsstatus

Auf der Seite „E-Mail-Warnungsstatus“ werden Informationen zu den E-Mail-Alarmen angezeigt, die basierend auf den im WAP-Gerät generierten Syslog-Nachrichten gesendet wurden. Zum Anzeigen der Seite „E-Mail-Warnungsstatus“ wählen Sie im Navigationsbereich **Status und Statistiken > E-Mail-Warnungstatus** aus.

- **Email Alert Status**: Der konfigurierte Status für E-Mail-Alarme. Als Status ist „Aktiviert“ oder „Deaktiviert“ möglich. Die Standardeinstellung ist „Deaktiviert“.
- **Anzahl gesendete E-Mails**: Die Gesamtanzahl der gesendeten E-Mails. Möglich ist eine vorzeichenlose 32-Bit-Ganzzahl. Die Standardeinstellung ist 0.
- **Anzahl fehlgeschlagene E-Mails**: Die Gesamtanzahl der E-Mail-Fehler. Möglich ist eine vorzeichenlose 32-Bit-Ganzzahl. Die Standardeinstellung ist 0.
- **Letzter E-Mail-Sendezeitpunkt**: Tag, Datum und Uhrzeit der letzten gesendeten E-Mail

Sie können auf **Aktualisieren** klicken, um die aktuellen Informationen anzuzeigen.

Protokoll

Auf der Seite „Protokoll“ wird eine Liste mit Systemereignissen angezeigt, durch die ein Protokolleintrag generiert wurde, beispielsweise Anmeldeversuche und Konfigurationsänderungen. Das Protokoll wird beim Neustart gelöscht und kann von einem Administrator gelöscht werden. Es können bis zu 512 Ereignisse angezeigt werden. Ältere Einträge werden nach Bedarf aus der Liste entfernt, um Platz für neue Ereignisse freizugeben.

Zum Anzeigen der Seite „Protokoll“ wählen Sie im Navigationsbereich **Status und Statistiken > Protokoll** aus.

- **Time Stamp**: Der Zeitpunkt, zu dem das Ereignis aufgetreten ist
- **Schweregrad**: Gibt an, ob das Ereignis auf einen Fehler („err“) zurückzuführen ist oder ob es sich um eine Information („info“) handelt.
- **Service**: Die dem Ereignis zugeordnete Softwarekomponente
- **Beschreibung**: Eine Beschreibung des Ereignisses

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

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

3

Administration

In diesem Abschnitt wird das Konfigurieren globaler Systemeinstellungen und das Ausführen von Diagnosen beschrieben.

Folgende Themen werden behandelt:

- **Systemeinstellungen**
- **Benutzerkonten**
- **Zeiteinstellungen**
- **Protokolleinstellungen**
- **E-Mail-Warnung**
- **LED-Anzeige**
- **HTTP-/HTTPS-Service**
- **Verwaltungszugangskontrolle**
- **Firmware verwalten**
- **Konfigurationsdatei herunterladen/sichern**
- **Konfigurationsdateieigenschaften**
- **Konfiguration kopieren/speichern**
- **Neu starten**
- **Discovery - Bonjour**
- **Paketerfassung**
- **Supportinformationen**
- **Spanning Tree-Einstellungen**

Systemeinstellungen

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

Konfigurieren von Systemeinstellungen

So konfigurieren Sie die Systemeinstellungen:

SCHRITT 1 Wählen Sie **Verwaltung** > **Systemeinstellungen** aus.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

- **Hostname**: Der administrativ zugewiesene Name des WAP-Geräts. Konventionsgemäß handelt es sich dabei um den vollständigen Hostnamen des Knotens. Der Standardhostname setzt sich aus dem Wort **wap** und den sechs letzten Hexadezimalstellen der MAC-Adresse des WAP-Geräts zusammen. Labels für Hostnamen können nur Buchstaben, Ziffern und Bindestriche enthalten. Labels für Hostnamen können 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**: Eine Kontaktperson für das WAP-Gerät. Der Systemkontakt kann aus 0 bis 255 Zeichen bestehen und Leerzeichen und Sonderzeichen enthalten.
- **Systemstandort**: Eine Beschreibung des physischen Standorts des WAP-Geräts. 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.

Benutzerkonten

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

So fügen Sie einen neuen Benutzer hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **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 über Lesezugriff, aber nicht über Lese- und Schreibzugriff verfügen.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. Daraufhin wird eine neue Zeile mit Textfeldern angezeigt.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen für den neuen Benutzer, und wählen Sie **Bearbeiten** aus.

SCHRITT 4 Geben Sie in **Benutzername** einen Benutzernamen mit 1 bis 32 alphanumerischen Zeichen ein. Für Benutzernamen sind nur die Zahlen 0 bis 9 und die Buchstaben a bis z (Groß- oder Kleinbuchstaben) zulässig.

SCHRITT 5 Geben Sie in **Neues Passwort** ein neues Kennwort mit 1 und 64 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld **Neues Passwort bestätigen** ein.

Wenn Sie ein Kennwort eingeben, ändert sich die Anzahl und Farbe der vertikalen Balken. Damit wird wie folgt die Kennwortstärke angegeben:

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

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Löschen eines Benutzers aktivieren Sie das Kontrollkästchen neben dem Benutzernamen, und wählen Sie **Löschen** aus. Wählen Sie anschließend **Speichern** aus, um die Löschung dauerhaft zu speichern.

Ändern eines Benutzerkennworts

So ändern Sie ein Benutzerkennwort:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **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 in **Neues Passwort** ein neues Kennwort mit 1 und 64 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld **Neues Passwort bestätigen** ein.

Wenn Sie ein Kennwort eingeben, ändert sich die Anzahl und Farbe der vertikalen Balken. Damit wird wie folgt die Kennwortstärke angegeben:

- **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.

Zeiteinstellungen

Über eine Systemuhr wird ein mit dem Netzwerk synchronisierter Zeitstempeldienst für Softwareereignisse wie beispielsweise Nachrichtenprotokolle bereitgestellt. Sie können die Systemuhr manuell konfigurieren oder das WAP-Gerät als NTP-Client (Network Time Protocol) konfigurieren, der die Uhrzeitdaten von einem Server bezieht.

Auf der Seite „Time Settings“ können Sie die Systemzeit manuell festlegen oder das System so konfigurieren, dass die Zeiteinstellungen von einem vorkonfigurierten NTP-Server bezogen werden. Der AP 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.

So legen Sie fest, dass die Zeiteinstellungen für das WAP-Gerät automatisch über NTP bezogen werden:

Automatisches Beziehen der Zeiteinstellungen über NTP

So beziehen Sie die Zeiteinstellungen automatisch über NTP:

SCHRITT 1 Wählen Sie für das Feld „Systemuhrzeitquelle“ **Netzwerkzeitprotokoll** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **IPv4-Adresse/IPv6-Adresse/Name des NTP-Servers**: Geben Sie die IPv4-Adresse, die IPv6-Adresse oder den Hostnamen eines NTP-Servers an. Ein Standard-NTP-Server wird aufgeführt.

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

- **Zeitzone**: Wählen Sie die Zeitzone für den Standort aus.

SCHRITT 3 Wählen Sie **Zeit an Sommerzeit anpassen** aus, wenn die Sommerzeit für die Zeitzone gilt. Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die folgenden Felder:

- **Beginn der Sommerzeit**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
- **Ende der Sommerzeit**: 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 für das Feld „Systemuhrzeitquelle“ die Option **Manuell** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **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, beispielsweise 22:00:00 Uhr.

HINWEIS Es wird ein Pfeil neben der Systemzeit angezeigt, um die Zeit vom aktuellen Computer zu übertragen, falls Sie Zeit und Datum Ihres Computers verwenden möchten.

- **Zeitzone**: Wählen Sie die Zeitzone für den Standort aus.

SCHRITT 3 Wählen Sie **Zeit an Sommerzeit anpassen** aus, wenn die Sommerzeit für die Zeitzone gilt. Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die folgenden Felder:

- **Beginn der Sommerzeit**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
- **Ende der Sommerzeit**: 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.

Protokolleinstellungen

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

Konfigurieren des dauerhaften Protokolls

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 Verringerung des verfügbaren (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 einer dauerhaften Protokollierung

So konfigurieren Sie die dauerhafte Protokollierung:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Protkolleinstellungen** 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 im nichtflüchtigen Datenspeicher bis zu 128 Protokollnachrichten speichern. Wenn das Limit von 128 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**: Der Mindestschweregrad, den ein Ereignis aufweisen muss, damit es in den nichtflüchtigen Datenspeicher geschrieben wird. Wenn Sie beispielsweise „2“ (kritisch) angeben, werden kritische Ereignisse, Alarmereignisse und Notfallereignisse im nichtflüchtigen Datenspeicher protokolliert. Fehlermeldungen mit dem Schweregrad 3 bis 7 werden in den flüchtigen Datenspeicher geschrieben.
- **Tiefe**: Die maximale Anzahl von Nachrichten (512), 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. Im nichtflüchtigen Datenspeicher können maximal 128 Protokollnachrichten gespeichert werden (dauerhaftes Protokoll). Diese Anzahl kann nicht konfiguriert werden.

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

Remoteprotokollserver

Beim Kernel-Protokoll handelt es sich um eine umfassende Liste mit (im Systemprotokoll angezeigten) Systemereignissen und Kernel-Nachrichten wie beispielsweise Fehlerbedingungen.

Sie können Kernel-Protokollnachrichten nicht direkt über die Weboberfläche anzeigen. Zuerst müssen Sie einen Remoteprotokollserver zum Empfangen und Erfassen von Protokollen einrichten. Dann 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 des WAP-Geräts durch den Remoteprotokollserver bietet die folgenden Funktionen:

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

Spezifizieren eines Hosts as Remoteprotokollserver

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Protkolleinstellungen** aus.

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

- **Remoteprotokollserver**: 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 diese Option, um diesen 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**: Die Nummer des logischen Ports für den Syslog-Prozess auf dem Remotehost. Möglich sind Werte im Bereich von 1 bis 65535. Der Standardport lautet „514“.

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

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

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

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

E-Mail-Warnung

Verwenden Sie die Funktion für E-Mail-Alarme, um beim Auftreten bestimmter Systemereignisse Nachrichten an die konfigurierten E-Mail-Adressen zu senden.

Die Funktion unterstützt die Konfiguration von Mailservern und Nachrichtenschweregraden sowie von drei E-Mail-Adressen zum Senden dringender und nicht dringender Alarme.

TIPP Verwenden Sie nicht Ihre persönliche E-Mail-Adresse, um persönliche E-Mail-Anmeldeinformationen nicht unnötig preiszugeben. 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. Überprüfen Sie die E-Mail-Einstellungen, um sicherzustellen, dass sie den Datenschutzrichtlinien Ihres Unternehmens entsprechen.

Konfigurieren des AP zum Senden von E-Mail-Alarmen

So konfigurieren Sie den AP zum Senden von E-Mail-Alarmen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **E-Mail-Warnung** aus.

SCHRITT 2 Konfigurieren Sie im Bereich „Globale Konfiguration“ die folgenden Parameter:

- **Administrativer Modus**: Wählen Sie diese Option aus, um die Funktion für E-Mail-Alarme global zu aktivieren.
- **Von-E-Mail-Adresse**: Geben Sie die Adresse ein, die als Absender der E-Mail angezeigt werden soll. Bei der Adresse handelt es sich um eine aus 255 Zeichen bestehende Zeichenfolge, die nur druckbare Zeichen enthält. Standardmäßig ist keine Adresse konfiguriert.

- **Protokollierungsdauer**: Wählen Sie die Häufigkeit aus, mit der geplante Nachrichten gesendet werden. Möglich sind Werte im Bereich von 30 bis 1440 Minuten. Die Standardeinstellung beträgt 30 Minuten.
- **Meldungsschweregrad (geplant)**: Protokollnachrichten mit diesem oder einem höheren Schweregrad werden gruppiert und mit der über die Option „Log Duration“ angegebenen Häufigkeit an die konfigurierte E-Mail-Adresse gesendet. Wählen Sie einen dieser Werte aus: „Keine“, „Notfall“, „Warnung, „Kritisch“, „Fehler“, „Warnung“, „Hinweis“, „Info“ und „Debugging“. Wenn Sie „Keine“ festlegen, werden keine geplanten Schweregradnachrichten gesendet. Der Standardschweregrad lautet „Warning“.
- **Meldungsschweregrad Dringend**: Protokollnachrichten mit diesem oder einem höheren Schweregrad werden sofort an die konfigurierte E-Mail-Adresse gesendet. Wählen Sie einen dieser Werte aus: „Keine“, „Notfall“, „Warnung, „Kritisch“, „Fehler“, „Warnung“, „Hinweis“, „Info“ und „Debugging“. Wenn Sie „None“ festlegen, werden keine dringenden Schweregradnachrichten gesendet. Der Standardwert lautet „Alert“.

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. (Den Hostnamen erhalten Sie vom E-Mail-Anbieter.) 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, das heißt einer Gruppe aus bis zu 63 alphanumerischen Zeichen, bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Beschriftungen durch einen Punkt (.) getrennt. Die gesamte Zeichenfolge aus Labels und Punkten kann bis zu 253 Zeichen umfassen.
- **Datenverschlüsselung**: Geben Sie den Sicherheitsmodus für den ausgehenden E-Mail-Alarm ein. Der Alarm kann mit dem sicheren TLS-Protokoll oder dem Standardprotokoll (Open) gesendet werden. Mit dem sicheren TLSv1-Protokoll können Sie Abhören und Manipulationen während der Kommunikation über das öffentliche Netzwerk verhindern.
- **Port**: Geben Sie die Nummer des SMTP-Ports ein, der für ausgehende E-Mails verwendet werden soll. Gültig sind Portnummern im Bereich von 0 bis 65535. Der Standardport lautet „465“. Im Allgemeinen ist entscheidend, welchen Port der E-Mail-Anbieter verwendet.

- **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 Benutzername kann aus 1 bis 64 alphanumerischen Zeichen bestehen.
- **Kennwort**: 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 die E-Mail-Adressen und die Betreffzeile.

- **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 **Test-E-Mail**, um durch Senden einer Test-E-Mail das konfigurierte E-Mail-Konto zu überprüfen.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Beispiele für E-Mail-Alarme

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

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Die vollständige E-Mail-Adresse, mit der Sie sich bei dem E-Mail-
Konto anmelden können, das dem oben genannten Server zugeordnet ist
Password = xxxxxxxx ist ein gültiges Kennwort für das gültige E-Mail-Konto
To Email Address 1 = meine-e-mail@gmail.com

Windows Live Hotmail
Für Windows Live Hotmail werden die folgenden Einstellungen empfohlen:
Data Encryption: TLSv1
SMTP-Server: smtp.live.com
SMTP-Port: 587
Benutzername: Ihre vollständige E-Mail-Adresse, beispielsweise
meinName@hotmail.com oder meinName@meineDomäne.com
Kennwort: Das Kennwort für Ihr Windows Live-Konto

Yahoo! Mail
Bei Yahoo benötigen Sie für diesen Dienst ein kostenpflichtiges Konto.
Für Yahoo werden die folgenden Einstellungen empfohlen:
Data Encryption: TLSv1
SMTP-Server: plus.smtp.mail.yahoo.com
SMTP-Port: 465 oder 587
Benutzername: Ihre E-Mail-Adresse ohne den Domänennamen, beispielsweise
meinName (ohne @yahoo.com)
Kennwort: Das Kennwort für Ihr Yahoo-Konto
```

Im folgenden Beispiel wird ein Format einer allgemeinen Protokoll-E-Mail gezeigt:

```
Von: AP-192.168.2.10@mailserver.com
Gesendet: Mittwoch, 09. September 2009, 11:16 Uhr
Bis: administrator@mailserver.com
Thema: Protokollnachricht vom AP

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

LED-Anzeige

Das WAP-Gerät verfügt über eine Kontrollleuchte: Verwenden Sie die Seite „LED-Anzeige“, um die LED zu aktivieren oder zu deaktivieren und der LED ein konfiguriertes Planungsmodulprofil zuzuordnen.

Die Option „LED-Anzeige“ ist standardmäßig **aktiviert**. Wenn die Option „LED-Anzeige“ **deaktiviert** ist, ist die Kontrollleuchte ausgeschaltet. Wenn der Wert für „LED-Anzeige“ **Planungsmodul zuordnen** ist, wird ein Dropdownfeld angezeigt, in dem Sie ein Planungsmodulprofil auswählen können. Ist die Option aktiviert, zeigt die Leuchte den entsprechenden Status und die Aktivität des WAP-Geräts an.

So ändern Sie die Option „LED-Anzeige“:

So ändern Sie die Option „LED-Anzeige“:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung > LED-**Anzeige aus.

SCHRITT 2 Wählen Sie im Dropdownfeldl **Planungsmodul aktivieren/deaktivieren/ zuordnen** aus.

SCHRITT 3 Wählen Sie den Profilnamen aus der Dropdown-Auswahl für „Planungsmodul-LED-Anzeige zuordnen“ aus. Den LEDs ist standardmäßig kein Profil zugeordnet. Die Dropdown-Auswahl zeigt die konfigurierten Planungsmodul-Profilnamen wie auf der Seite **WLAN > Planungsmodul** an.

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**. Die Änderungen werden in der Startkonfiguration gespeichert.

HTTP-/HTTPS-Service

Auf der Seite „HTTP/HTTPS Service“ können Sie webbasierte Verwaltungsverbindungen aktivieren und konfigurieren. Wenn HTTPS für sichere Verwaltungssitzungen verwendet wird, können Sie auf der Seite „HTTP/HTTPS Service“ außerdem die erforderlichen SSL-Zertifikate verwalten.

Konfigurieren von HTTP- und HTTPS-Diensten

So konfigurieren Sie HTTP- und HTTP-Dienste:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **HTTP-/HTTPS-Service** aus.

SCHRITT 2 Konfigurieren Sie die folgenden globalen Einstellungen:

- **Maximale Sitzungen**: Die Anzahl der Websitzungen, einschließlich HTTP und HTTPS, 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. Der Standardwert lautet „5“. Wenn die maximale Sitzungsanzahl erreicht ist, wird dem nächsten Benutzer, der sich beim Konfigurationsdienstprogramm anzumelden versucht, eine Fehlermeldung bezüglich des Sitzungslimits angezeigt.

- **Sitzungstimeout**: Die maximale Dauer (in Minuten), während der inaktive Benutzer beim Konfigurationsdienstprogramm für das WAP-Gerät angemeldet bleiben. Wenn das konfigurierte Timeout erreicht ist, werden die Benutzer automatisch abgemeldet. Möglich sind Werte im Bereich von 1 bis 60 Minuten. Die Standardeinstellung beträgt 10 Minuten.

SCHRITT 3 Konfigurieren Sie die HTTP- und HTTPS-Dienste:

- **HTTP-Server**: Aktiviert den Zugriff über HTTP. Standardmäßig ist der HTTP-Zugriff aktiviert. Wenn Sie diese Option deaktivieren, werden alle aktuellen über dieses Protokoll hergestellten Verbindungen getrennt.

- **HTTP Port**: Die Nummer des logischen Ports (von 1025 bis 65535), der für HTTP-Verbindungen verwendet werden soll. Die Standardportnummer für HTTP-Verbindungen ist die allgemein bekannte IANA-Portnummer 80.

- **HTTPS-Server**: Aktiviert den Zugriff über Secure HTTP. Standardmäßig ist der HTTPS-Zugriff aktiviert. Wenn Sie diese Option deaktivieren, werden alle aktuellen über dieses Protokoll hergestellten Verbindungen getrennt.

- **HTTPS Port**: Die Nummer des logischen Ports (von 1025 bis 65535), der für HTTP-Verbindungen verwendet werden soll. Die Standardportnummer für HTTP-Verbindungen ist die allgemein bekannte IANA-Portnummer 443.
- **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.

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

Verwalten von SSL-Zertifikaten

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

Zum Generieren des Zertifikats über das WAP-Gerät klicken Sie auf **SSL-Zertifikat generieren**. Dies sollte geschehen, nachdem der AP eine IP-Adresse bezogen hat. Dadurch wird sichergestellt, dass der allgemeine Name für das Zertifikat der IP-Adresse für den AP entspricht. 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 „Certificate File Status“ können Sie anzeigen, ob auf dem WAP-Gerät zurzeit ein Zertifikat vorhanden ist, und die folgenden Informationen zum Zertifikat anzeigen:

- 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** oder **TFTP** als **Downloadmethode** aus und klicken Sie auf **Herunterladen**.

- Wenn Sie HTTP auswählen, werden Sie aufgefordert, den Download zu bestätigen und dann zu dem Speicherort im Netzwerk zu wechseln, an dem Sie die Datei speichern möchten.

- Wenn Sie TFTP auswählen, werden zusätzliche Felder angezeigt, in die Sie den Dateinamen, den Sie der heruntergeladenen Datei zuweisen möchten, und die TFTP-Serveradresse, von der Sie die Datei herunterladen möchten, eingeben können.

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

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

Nach dem erfolgreichen Upload wird eine Bestätigung angezeigt.

Verwaltungszugangskontrolle

Sie können eine Zugangskontrollliste (Access Control List, ACL) mit bis zu fünf IPv4-Hosts und fünf IPv6-Hosts erstellen, die autorisiert sind, auf das Konfigurationsdienstprogramm für das WAP-Gerät zuzugreifen. 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.

Wenn die Verwaltungs-ACL aktiviert ist, ist der Zugriff über das Web und über SNMP auf die angegebenen IP-Hosts beschränkt.

VORSICHT 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.

Erstellen einer Zugriffsliste

So erstellen Sie eine Zugangsliste:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **„Administration“** > **„Management Access Control“** aus.

SCHRITT 2 Wählen Sie für **Management ACL Mode** die Option **Enable** aus.

SCHRITT 3 Geben Sie bis zu fünf IPv4-Adressen und fünf IPv6-Adressen ein, denen Sie den Zugriff gewähren möchten.

SCHRITT 4 Vergewissern Sie sich, dass die IP-Adressen richtig sind.

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

Firmware verwalten

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 den AP zur Verfügung stehen, können Sie die Firmware der Geräte aktualisieren, um von neuen Funktionen und Verbesserungen zu profitieren. Der AP verwendet für Firmwareupgrades einen TFTP- oder HTTP-Client.

Wenn Sie neue Firmware hochgeladen und das System neu gestartet haben, wird die neue Firmware zum primären Image. Wenn beim Upgrade ein Fehler auftritt, wird die ursprüngliche Firmware weiter als primäres Image verwendet.

HINWEIS Beim Aktualisieren der Firmware werden die vorhandenen Konfigurationsinformationen des Access Points beibehalten.

So tauschen Sie das im AP ausgeführte Firmware-Image aus:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **„Administration“** > **„Manage Firmware“** aus.

SCHRITT 2 Klicken Sie auf **„Swap Active Image“**.

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 der Access Point nicht verfügbar. Schalten Sie den Access Point während des Image-Wechsels nicht aus. Nach Abschluss des Image-Wechsels wird der Access Point neu gestartet. Der AP nimmt den Normalbetrieb wieder auf. Dabei werden die gleichen Konfigurationseinstellungen wie vor dem Upgrade verwendet.

TFTP-Aktualisierung

So aktualisieren Sie die Firmware eines Access Points über TFTP:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **„Administration“** > **„Manage Firmware“** aus.

Die Produkt-ID (PID-VID) sowie die aktive und die inaktive Firmwareversion werden angezeigt.

SCHRITT 2 Wählen Sie **TFTP als Transfermethode**.

SCHRITT 3 Geben Sie in das Feld **Quelldateiname** einen Namen (1 bis 128 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 4 Geben Sie in **„TFTP Server IPv4 Address“** die IPv4-Adresse des TFTP-Servers ein, und klicken Sie auf **„Upgrade“**.

Das Hochladen der neuen Software kann mehrere Minuten dauern. Beim Hochladen der neuen Software dürfen Sie nicht die Seite aktualisieren oder zu einer anderen Seite navigieren, da sonst der Software-Upload abgebrochen wird. Nach Abschluss des Vorgangs wird der Access Point neu gestartet und nimmt den Normalbetrieb wieder auf.

SCHRITT 5 Vergewissern Sie sich, dass das Firmware-Upgrade erfolgreich abgeschlossen wurde, indem Sie sich auf der Benutzeroberfläche anmelden und auf der Seite „Upgrade Firmware“ die aktive Firmwareversion anzeigen.

HTTP-Aktualisierung

So führen Sie das Upgrade über HTTP durch:

SCHRITT 1 Wählen **HTTP als Transfermethode**.

SCHRITT 2 Wenn Sie den Namen und den Pfad der neuen Datei kennen, geben Sie diese Informationen in das Feld **„Source File Name“** 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.

SCHRITT 3 Klicken Sie auf **„Upgrade“**, um das neue Firmware-Image zu übernehmen.

Das Hochladen der neuen Software kann mehrere Minuten dauern. Beim Hochladen der neuen Software dürfen Sie nicht die Seite aktualisieren oder zu einer anderen Seite navigieren, da sonst der Software-Upload abgebrochen wird. Nach Abschluss des Vorgangs wird der Access Point neu gestartet und nimmt den Normalbetrieb wieder auf.

SCHRITT 4 Vergewissern Sie sich, dass das Firmware-Upgrade erfolgreich abgeschlossen wurde, indem Sie sich auf der Benutzeroberfläche anmelden und auf der Seite Upgrade Firmware die aktive Firmwareversion anzeigen.

Konfigurationsdatei herunterladen/sichern

Die Konfigurationsdateien für den AP 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. Wenn Sie eine gesicherte Konfigurationsdatei bearbeitet haben, können Sie die Datei in den Access Point herunterladen, um die Konfiguration zu ändern.

Die folgenden Konfigurationsdateien sind im AP 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 stellt eine Momentaufnahme einer ehemaligen Startkonfiguration dar. 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 die Dateien auch in andere Dateitypen im WAP-Gerät kopieren. Informationen hierzu finden Sie unter **Konfiguration kopieren/speichern**.

Sichern einer Konfigurationsdatei

So sichern Sie die Konfigurationsdatei auf einem Netzwerk-Host oder TFTP-Server (bzw. laden sie hoch):

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Konfigurationsdatei herunterladen/sichern** aus.

SCHRITT 2 Wählen Sie für **Transfer Method** die Option **Via TFTP** oder **Via HTTP/HTTPS** aus.

SCHRITT 3 Wählen Sie als **Speicheraktion Sichern (von AP auf PC)** aus.

SCHRITT 4 Bei einer reinen TFTP-Sicherung geben Sie in **Zieldateiname** den Zieldateinamen mit der Erweiterung „.xml“ ein. Geben Sie dabei auch den Pfad an, in 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 reinen TFTP-Sicherung geben Sie die **IPv4-Adresse des TFTP-Servers** ein.

SCHRITT 6 Wählen Sie die zu sichernde Konfigurationsdatei aus:

- **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 Spiegelkonfigurationsdatei stellt eine Momentaufnahme einer ehemaligen Startkonfiguration dar. 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-Sicherungen wird ein Fenster angezeigt, in dem Sie zum gewünschten Speicherort für die Datei wechseln können.

Sie können eine Datei in den AP herunterladen, um die Konfiguration zu aktualisieren oder eine zuvor gesicherte Konfiguration im AP wiederherzustellen.

Herunterladen einer Konfigurationsdatei

So laden Sie eine Konfigurationsdatei in das WAP-Gerät herunter:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Konfigurationsdatei herunterladen/sichern** aus.

SCHRITT 2 Wählen Sie für**Übertragungsmethode Über TFTP** oder **Über HTTP/HTTPS** aus

SCHRITT 3 Wählen Sie für **Aktion speichern Herunterladen (von PC auf AP)** aus.

SCHRITT 4 Bei einem reinen TFTP-Download geben Sie in **Quelldateiname** den Quelldateinamen mit der Erweiterung „.xml“ ein. Geben Sie dabei auch den Pfad der Datei auf dem Server an. 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 die Konfigurationsdatei im AP aus, die Sie durch die heruntergeladene Datei ersetzen möchten: **„Startup Configuration“** oder **„Backup Configuration“**.

Wenn die Startkonfigurationsdatei mit der heruntergeladenen Datei überschrieben und die Gültigkeit der Datei erfolgreich überprüft wurde, wird die heruntergeladene Konfiguration beim nächsten Neustart des APs wirksam.

SCHRITT 6 Klicken Sie auf **Speichern**, um das Upgrade bzw. die Sicherung zu starten. Bei HTTP-Downloads wird ein Fenster angezeigt, in dem Sie die herunterzuladende Datei auswählen können. Nach Abschluss des Downloads wird der erfolgreiche Vorgang in einem Fenster bestätigt.

VORSICHT Die Stromversorgung für den AP 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.

Konfigurationsdateieigenschaften

Auf der Seite „Configuration Files Properties“ können Sie die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei löschen. Wenn Sie die Startkonfigurationsdatei löschen, wird die Backup-Konfigurationsdatei beim nächsten Starten des APs aktiv.

Wenn der Access Point aktiv wird, versucht er, die Startkonfiguration anzuwenden. Ist mit der Startkonfiguration ein Problem zu erkennen, versucht der Access Point, die Spiegelkonfiguration anzuwenden. Kann die Spiegelkonfiguration aus irgendeinem Grunde nicht angewendet werden, versucht der Access Point eine Backup-Konfiguration.

Löschen der Startkonfigurationsdatei oder Backup-Konfigurationsdatei

So löschen Sie die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Konfigurationsdateieigenschaften** aus

SCHRITT 2 Wählen Sie den Dateityp **Startup Configuration** oder **Backup Configuration** aus.

SCHRITT 3 Klicken Sie auf **Dateien löschen**.

Konfiguration kopieren/speichern

Auf der Seite „Konfiguration kopieren/speichern“ können Sie Dateien innerhalb des Dateisystems des AP kopieren. Sie können beispielsweise die Backup-Konfigurationsdatei in die Startkonfigurationsdatei kopieren, damit sie beim nächsten Start des WAP-Geräts verwendet wird.

Kopieren einer Datei in einen anderen Dateityp

So kopieren Sie eine Datei in einen anderen Dateityp:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Konfiguration kopieren/speichern** aus.

SCHRITT 2 Wählen Sie unter **Source File Name** den Namen der Quelldatei aus:

- **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 Spiegelkonfigurationsdatei stellt eine Momentaufnahme einer ehemaligen Startkonfiguration dar. 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 für **Zieldateiname** den Dateityp aus, den Sie durch die kopierte Datei ersetzen möchten.

SCHRITT 4 Klicken Sie auf **Speichern**, um den Kopiervorgang zu starten.

Nach Abschluss des Vorgangs wird in einem Fenster die Meldung „Copy Operation Successful“ angezeigt.

Neu starten

Neustarten des AP

Über die Seite „Neustart“ können Sie den AP neu starten.

SCHRITT 1 Zum Neustarten des WAP-Geräts wählen Sie im Navigationsbereich die Option **Verwaltung** > **Neustart** aus.

SCHRITT 2 Wählen Sie eine der folgenden Optionen aus:

- **Neustart**: Das WAP-Gerät wird mit der Startkonfiguration neu gestartet.
- **Neustart mit Werkseinstellungen**: Das WAP-Gerät wird mit der Standardkonfigurationsdatei mit den Werkseinstellungen neu gestartet. Alle angepassten Einstellungen gehen verloren.

Es wird ein Fenster angezeigt, in dem Sie den Neustart bestätigen oder abbrechen können. Die aktuelle Verwaltungssitzung wird möglicherweise beendet.

SCHRITT 3 Klicken Sie auf **OK**, um das Gerät neu zu starten.

Discovery - Bonjour

Bonjour ermöglicht die Erkennung des APs und der zugehörigen Dienste mithilfe von Multicast-DNS (mDNS). Bonjour kündigt Dienste im Netzwerk an und beantwortet Anfragen für die unterstützten Diensttypen. Dadurch wird die Netzwerkkonfiguration in den Umgebungen kleiner und mittlerer Unternehmen vereinfacht.

Der AP kündigt die folgenden Diensttypen an:

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

Sie können Bonjour in IPv4- und IPv6-Netzwerken verwenden.

Bonjour ist standardmäßig aktiviert.

Ändern des administrativen Status

So ändern Sie den administrativen Status:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Verwaltung** > **Discovery – Bonjour** aus.

SCHRITT 2 Klicken Sie auf **Enable**, um Bonjour zu aktivieren, oder löschen Sie die Auswahl von **Enable**, um Bonjour zu deaktivieren.

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

Paketerfassung

Mit der Funktion für die 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 Erfassung**: Die erfassten Pakete werden in einer Datei im WAP-Gerät gespeichert. Das WAP-Gerät kann die Datei an einen TFTP-Server übertragen oder sie über HTTP(S) auf einen Computer herunterladen. Die Datei liegt im PCAP-Format vor und kann mit Tools wie beispielsweise Wireshark und OmniPeek untersucht werden.
- **Remoteerfassung**: Die erfassten Pakete werden in Echtzeit an einen externen Computer umgeleitet, auf dem das Wireshark-Tool ausgeführt wird.
- **CloudShark-Erfassung**: Die Erfassten Pakete werden in Echtzeit in die CloudShark-Appliance hochgeladen. Die CloudShark-Appliance ordnet die Erfassungen, sodass sie benannt, getaggt und gesucht werden können.

HINWEIS CloudShark ist ein Netzwerkanalysetool für das Internet, auf das jeder Webbrowser ohne zusätzliche Dienstprogramme, Plug-Ins oder Downloads zugreifen kann.

Die folgenden Pakettypen können im WAP-Gerät erfasst werden:

- An Funkschnittstellen empfangene und gesendete 802.11-Pakete. An Funkschnittstellen erfasste Pakete enthalten den 802.11-Header.
- An der Ethernet-Schnittstelle empfangene und gesendete 802.3-Pakete.
- An den internen logischen Schnittstellen wie beispielsweise VAPs und WDS-Schnittstellen empfangene und gesendete 802.3-Pakete.

Wählen Sie **Verwaltung > Paketerfassung** aus, um die Seite „Paketerfassung“ anzuzeigen. Auf der Seite „Packet Capture“ haben Sie folgende Möglichkeiten:

- Konfigurieren der Parameter für die Paketerfassung
- Starten einer lokalen Paketerfassung oder Remotepaketerfassung
- Anzeigen des aktuellen Status der Paketerfassung
- Herunterladen einer Paketerfassungsdatei

Im Bereich „Paketerfassungskonfiguration“ können Sie Parameter konfigurieren und eine Paketerfassung initiieren.

Konfigurieren der Paketerfassung

So konfigurieren Sie die Paketerfassungseinstellungen:

SCHRITT 1 Konfigurieren Sie die folgenden Parameter:

- **Beacons erfassen**: Aktiviert oder deaktiviert die Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder gesendet wurden.
- **Promiscuous-Erfassung**: Aktiviert oder deaktiviert den Promiscuous-Modus, wenn die Erfassung aktiv ist.

  Im Promiscuous-Modus empfängt das Funkmodul den gesamten Verkehr im Kanal, einschließlich des nicht an dieses WAP-Gerät gerichteten Verkehrs. Wenn das Funkmodul im Promiscuous-Modus betrieben wird, stellt sie weiterhin Dienste für die zugeordneten Clients bereit. Nicht an das WAP-Gerät gerichtete Pakete werden nicht weitergeleitet.

  Nach Abschluss der Erfassung nimmt das Funkmodul den Betrieb im Non-Promiscuous-Modus wieder auf.
- **WLAN-Clientfilter**: Aktiviert oder deaktiviert den WLAN-Clientfilter, um nur Frames zu erfassen, die an einen WLAN-Client mit einer angegebenen MAC-Adresse gesendet bzw. von diesem empfangen wurden.
- **Clientfilter-MAC-Adresse**: Gibt die MAC-Adresse für die WLAN-Clientfilterung an.

HINWEIS Der MAC-Filter ist nur aktiv, wenn eine Erfassung an einer 802.11-Schnittstelle ausgeführt wird.

- **Paketerfassungsmethode**: Wählen Sie eine der folgenden Optionen aus:
  - **Lokale Datei**: Die erfassten Pakete werden in einer Datei im WAP-Gerät gespeichert.
  - **Remote**: Die erfassten Pakete werden in Echtzeit an einen externen Computer umgeleitet, auf dem das Wireshark-Tool ausgeführt wird.
  - **CloudShark**: Die Erfassten Pakete werden in Echtzeit in die CloudShark-Appliance hochgeladen.

SCHRITT 2 Fahren Sie abhängig von der ausgewählten Methode mit den Schritten im Abschnitt „Lokale Paketerfassung“ oder „Remotepaketerfassung“ fort.

HINWEIS Änderungen an Konfigurationsparametern für die Paketerfassung werden nach dem Neustart der Paketerfassung wirksam. Wenn Sie die Parameter während einer ausgeführten Paketerfassung ändern, hat dies keine Auswirkung auf die aktuelle Paketerfassungssitzung. Sie müssen die vorhandene Paketerfassungssitzung beenden und neu starten, damit die neuen Parameterwerte verwendet werden.

Lokale Paketerfassung

So initiieren Sie eine lokale Paketerfassung:

SCHRITT 1 Stellen Sie sicher, dass für **Paketerfassungsmethode** die Option **Lokale Datei** ausgewählt ist.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Erfassungsschnittstelle**: Geben Sie einen Erfassungsschnittstellentyp für die Paketerfassung ein:
  - **radio1**: 802.11-Verkehr an der Funkschnittstelle Radio1.
  - **radio2**: 802.11-Verkehr an Funkschnittstelle 2.
  - **eth0**: 802.3-Verkehr am Ethernet-Port.
  - **wlan0**: VAP0-Verkehr an Funkschnittstelle 1.
  - **wlan1**: VAP0-Verkehr an Funkschnittstelle 2.
  - **Wlan0vap1** bis **wlan0vap7**: Verkehr am angegebenen VAP an Funkschnittstelle .1
  - **Wlan1vap1** bis **wlan1vap 7**: Verkehr am angegebenen VAP an Funkschnittstelle 2.
  - **Wlan0wds0** bis **wlan0wds3**: Verkehr an der angegebenen WDS-Schnittstelle.
  - **brtrunk:**: Linux-Bridge-Schnittstelle im WAP-Gerät.
- **Erfassungsdauer**: Geben Sie die Dauer der Erfassung in Sekunden ein. Möglich sind Werte im Bereich von 10 bis 3600. Der Standardwert lautet „60“. Bei der unbegrenzten Paketerfassungsmethode unter Verwendung von CloudShark kann dieser Wert null Sekunden betragen.

- **Maximale Größe der Erfassungsdatei.**: Geben Sie die maximal zulässige Größe für die Erfassungsdatei in KB ein. Möglich sind Werte im Bereich von 64 bis 4096. Die Standardeinstellung ist 1024. Diese Option ist für die Paketerfassungsmethode unter Verwendung von CloudShark nicht aktiviert.

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

SCHRITT 4 Klicken Sie auf **Erfassung starten**.

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.

Im Bereich „Packet Capture Status“ der Seite wird der Status einer im WAP-Gerät aktiven Paketerfassung angezeigt.

- **Aktueller Erfassungsstatus**: Gibt an, ob die Paketerfassung ausgeführt wird oder beendet wurde.
- **Paketerfsassungszeit**: Die verstrichene Dauer der Erfassung.
- **Größe der Paketerfassungsdatei**: Die aktuelle Größe der Erfassungsdatei. Die Größe ist für gewöhnlich höher als die Erfassungsgröße in CloudShark, wenn Sie ein kostenloses CloudShark-Konto mit begrenzter Erfassungsgröße verwenden.
- **Upload-Status der CloudShark-Erfassungsdatei:** Zeigt einen Hyperlink an, wenn die ausgewählte CloudShark-Paketerfassung erfolgreich hochgeladen wurde. Sie können auf den Hyperlink **Erfassung auf CloudShark ansehen** klicken, um ein Browserfenster zu öffnen und die erfassten Pakete in der CloudShark-Appliance anzusehen.

HINWEIS Wenn der Upload fehlschlägt, wird eine Fehlermeldung angezeigt.

Klicken Sie auf **Aktualisieren**, um die neuesten Daten des WAP-Geräts anzuzeigen.

HINWEIS Zum Beenden einer Paketdateierfassung klicken Sie auf **Erfassung stoppen**.

Remotepaketerfassung

Mit der Funktion für die Remoteerfassung können Sie einen Remoteanschluss 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 http://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.

Bei Verwendung des 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.

Initiieren einer Remoteerfassung in einem WAP-Gerät

So initiieren Sie eine Remoteerfassung in einem WAP-Gerät:

SCHRITT 1 Wählen Sie**Verwaltung** > **Paketerfassung** aus.

SCHRITT 2 Aktivieren Sie **Promiscuous-Erfassung**.

SCHRITT 3 Wählen Sie für **Paketerfassunsmethode Remote** aus.

SCHRITT 4 Verwenden Sie für **Remoterfassungsport** den Standardport (2002), oder geben Sie, wenn Sie einen anderen als den Standardport verwenden, die gewünschte Portnummer für die Verbindung zwischen Wireshark und dem WAP-Gerät ein. Möglich sind Ports im Bereich von 1025 bis 65530.

SCHRITT 5 Wenn Sie die Einstellungen zur späteren Verwendung speichern möchten, klicken Sie auf **Speichern**.

SCHRITT 6 Klicken Sie auf **Erfassung starten**.

Initiieren des Netzwerkanalysetools

So initiieren Sie das Wireshark-Netzwerkanalysetool für Microsoft Windows:

SCHRITT 1 Initiieren Sie auf dem gleichen Computer das Wireshark-Tool.

SCHRITT 2 Wählen Sie im Menü die Option **Erfassung** > **Optionen** aus. Daraufhin wird ein Popup-Fenster angezeigt.

SCHRITT 3 Wählen Sie für **Schnittstelle Remote** aus. Daraufhin wird ein Popup-Fenster angezeigt.

SCHRITT 4 Geben Sie unter **Host** die IP-Adresse des WAP-Geräts ein.

SCHRITT 5 Geben Sie unter **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 Pakete erfassen möchten. Das Wireshark-Popup-Fenster enthält neben der IP-Adresse eine Pulldown-Liste, in der Sie die Schnittstellen auswählen können. Folgende Schnittstellen sind möglich:

Linux-Bridge-Schnittstelle im WAP-Gerät
`--rpcap://[192.168.1.220]:2002/brtrunk`
Kabelgebundene LAN-Schnittstelle
`-- rpcap://[192.168.1.220]:2002/eth0`
VAP0-Verkehr an Funkschnittstelle 1
`-- rpcap://[192.168.1.220]:2002/wlan0`
802.11-Verkehr
`-- rpcap://[192.168.1.220]:2002/radio1`
Bei WAP571/E, VAP1 ~ VAP7-Verkehr für Funkschnittstelle 1
`-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
Bei WAP371/E, VAP1 ~ VAP7-Verkehr für Funkschnittstelle 2
`-- rpcap://[192.168.1.220]:2002/wlan1vap1 ~ wlan1vap7`

Sie können jeweils bis zu vier Schnittstellen im WAP-Gerät verfolgen. Sie müssen jedoch für jede Schnittstelle eine separate Wireshark-Sitzung starten. Wenn Sie weitere Remoteerfassungssitzungen initiieren möchten, wiederholen Sie die Schritte für die Wireshark-Konfiguration. Im 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 portrange 58000-58004

Aufgrund von Leistungs- und Sicherheitsproblemen wird der Paketerfassungsmodus nicht im NVRAM des WAP-Geräts gespeichert. Wenn das WAP-Gerät zurückgesetzt wird, wird der Erfassungsmodus deaktiviert und muss von Ihnen wieder aktiviert werden, um die Erfassung des Verkehrs fortzusetzen. 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.

Sie können eine Erfassungsdatei über TFTP auf einen konfigurierten TFTP-Server oder über HTTP(S) auf einen Computer herunterladen. Da sich die Erfassungsdatei im RAM-Dateisystem befindet, wird sie beim Zurücksetzen des WAP-Geräts gelöscht.

Herunterladen einer Paketerfassungsdatei über TFTP:

So laden Sie eine Paketerfassungsdatei über TFTP herunter:

SCHRITT 1 Wählen Sie **Erfassungsdatei über TFTP herunterladen** aus.

SCHRITT 2 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 3 Geben Sie in das Feld die **IPv4-Adresse des TFTP-Servers** ein.

SCHRITT 4 Klicken Sie auf **Herunterladen**.

Herunterladen einer Paketerfassungsdatei über HTTP

So laden Sie eine Paketerfassungsdatei über HTTP herunter:

SCHRITT 1 Löschen Sie **Erfassungsdatei über TFTP herunterladen**.

SCHRITT 2 Klicken Sie auf **Herunterladen**. Daraufhin wird ein Bestätigungsfenster angezeigt.

SCHRITT 3 Klicken Sie auf **OK**. Es wird ein Dialogfeld angezeigt, in dem Sie einen Netzwerkspeicherort zum Speichern der Datei auswählen können.

Supportinformationen

Auf der Seite „Supportinformationen“ können Sie eine Textdatei mit detaillierten Konfigurationsinformationen zum AP herunterladen. Die Datei enthält Informationen zur Software- und Hardwareversion, MAC- und IP-Adressen, den administrativen Status und den Betriebsstatus von Funktionen, von Benutzern konfigurierte Einstellungen, Verkehrsstatistiken usw. Sie können die Textdatei Mitarbeitern des technisches Supports als Unterstützung bei der Fehlerbehebung zur Verfügung stellen.

Wählen Sie im Navigationsbereich die Option **Verwaltung > Supportinformationen** aus, um die Seite „Supportinformationen“ anzuzeigen.

Klicken Sie auf **Download**, um die Datei auf der Grundlage der aktuellen Systemeinstellungen zu generieren. Nach einer kurzen Pause wird ein Fenster angezeigt, in dem Sie die Datei auf dem Computer speichern können.

Spanning Tree-Einstellungen

Verwenden Sie die Seite „Spanning Tree-Einstellungen“, um die STP-Einstellungen auf dem Cisco WAP571/E zu konfigurieren.

Konfigurieren der STP-Einstellungen auf dem Cisco WAP571

So konfigurieren Sie die erweiterten STP-Einstellungen auf dem Cisco WAP571/E:

SCHRITT 1 Wählen Sie **Verwaltung > Spanning Tree-Einstellungen** aus.

SCHRITT 2 Konfigurieren Sie die Parameter:

STP-Status: Aktiviert oder deaktiviert STP global auf dem Cisco WAP571/E. STP ist standardmäßig aktiviert.

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

4

LAN

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

Das Kapitel enthält die folgenden Themen:

- **Porteinstellungen**
- **VLAN-Konfiguration**
- **IPv4-Einstellung**
- **IPv6-Einstellung**
- **IPv6-Tunnel**
- **LLDP**

Porteinstellungen

Auf der Seite „Porteinstellungen“ können Sie Einstellungen für den Anschluss anzeigen und konfigurieren, über den das WAP-Gerät physisch mit einem LAN verbunden wird.

So konfigurieren Sie PoE-Porteinstellungen:

SCHRITT 1 Wählen Sie **LAN** > **Porteinstellungen** aus.

Die Tabelle mit den Porteinstellungen beinhaltet die folgenden Status und Konfigurationen für zwei Schnittstellen (Eth0 bis Eth1):

- **Linkstatus**: Zeigt den aktuellen Leistungsstatus 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. Die Geschwindigkeit 1.000 Mbit/s wird nur bei aktivierter automatischer Aushandlung unterstützt.
- Duplexmodus: Im Überprüfungsmodus wird hier der aktuelle Duplex-Modus des Ports angezeigt. Wählen Sie, sofern die automatische Aushandlung deaktiviert ist, entweder Halb-Duplex oder Voll-Duplex 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 kann nur verwendet werden, wenn für den Port automatische Aushandlung 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 Energie erkannt wird. Der EEE-Modus unterstützt RUHIGE Zeiten während niedriger Verbindungsauslastung und ermöglicht es so beiden Seiten einer Verbindung, Komponenten der PHY-Platine zu deaktivieren, um so Strom zu sparen.

- **Green Ethernet-Status** – Zeigt den aktuellen EEE-Status an.

SCHRITT 2 Prüfen Sie die Schnittstellen, die Sie bearbeiten möchten, und klicken Sie anschließend auf die Schaltfläche „Bearbeiten“, um in den Bearbeitungsmodus zu wechseln. Geben Sie dann Ihre Einstellungen ein.

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

HINWEIS WAP571/E bündelt Eth0 und Eth1 zu einer Link-Aggregation. Der Link-Partner muss ebenfalls Link-Aggregation unterstützen. Eth1 folgt immer den Eth0-Konfigurationen.

VLAN-Konfiguration

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

So konfigurieren Sie die Einstellungen für ein VLAN:

SCHRITT 1 Wählen Sie **LAN** > **VLAN-Konfiguration**.

SCHRITT 2 In der Tabelle mit den VLAN-Einstellungen umfasst jeder VLAN-Datensatz die folgenden Felder:

- **VLAN-ID**: Identifikator des VLANs. Jede VLAN-ID liegt im Bereich zwischen 1 und 4094 und sollte sich von anderen VLAN-IDs unterscheiden.
- **Beschreibung**: Beschreibung des verbundenen VLAN. Die Länge sollte weniger als 64 Zeichen betragen und es dürfen A-Z, a-z und 0-9 sowie der Unterstrich (_) verwendet werden.

SCHRITT 3 **Management-VLAN**: Unter dem Management-VLAN versteht man das VLAN, das für den Zugriff auf das WAP-Gerät über die Web-GUI verwendet wird. Es darf nur ein einziges VLAN als das Management-VLAN fungieren. Wenn keine Schnittstelle (kabelgebunden oder Wireless) zum Management-VLAN gehört, existiert keine Schnittstelle, die der Benutzer für den Zugriff auf das Konfigurationsdienstprogramm verwenden kann.

- **Eth0 – Eth1**: Jeder Port sollte maximal ein unmarkiertes VLAN besitzen. Folgende Optionen sind verfügbar:
  - **Ohne Tag**: Der Port gehört dem VLAN als Mitglied an. Ein Paket des VLAN, das vom Port gesendet wird, ist unmarkiert. Ein beim Port eingehendes unmarkiertes Paket wird als VLAN klassifiziert (markiert).
  - **Markiert**: Der Port gehört zum VLAN. Ein vom Port abgesendetes Paket des VLAN wird mit dem VLAN-Header markiert.
  - **Ausgeschlossen**: Der Port gehört nicht zum VLAN.

HINWEIS Die VLAN-ID 1 kann nicht gelöscht werden. Wenn ein mit dem VLAN verbundener Port (kabelgebunden oder Wireless) gelöscht wurde, setzt das WAP-Gerät dessen VLAN-ID automatisch auf 1.

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Dabei werden die Verbindungen des WAP-Geräts möglicherweise unterbrochen. Es wird empfohlen, die Einstellungen des WAP-Geräts zu einem Zeitpunkt zu ändern, zu dem ein Konnektivitätsverlust die geringsten Auswirkungen auf die WLAN-Clients hat.

IPv4-Einstellung

Verwenden Sie die Seite „IPv4-Einstellung“, um die statische oder dynamische IPv4-Adresszuordnung zu konfigurieren.

So konfigurieren Sie die IPv4-Adresseinstellungen:

SCHRITT 1 Wählen Sie **LAN > IPv4-Einstellung** 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 dieser Optionen:

  - **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 (192.0.2.10) ein.

- Statische-IP-Adresse, Subnetzmaske, und Standardgateway: Wenn Sie die Zuweisung einer statischen IP-Adresse ausgewählt haben, geben Sie die IP-Informationen ein.
- **Domänen-Nameserver**: Wählen Sie eine der folgenden Optionen:
  - **Dynamisch**: Das WAP-Gerät bezieht DNS-Serveradressen von einem DHCP-Server im LAN.

- **Manuell**: Sie können manuell eine oder mehrere DNS-Serveradressen konfigurieren. Geben sie bis zu zwei IP-Adressen in die bereitgestellten Felder ein.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen für die automatische IPv4-DCHP-Konfiguration:

- **Optionen für automatische DHCP-Konfiguration**: Diese Option ist standardmäßig aktiviert. Wenn der Access Point mit Werkseinstellungen aktiv wird, versucht er zunächst die automatische Konfiguration mit den DHCP-Optionen.

  Während der automatischen Konfiguration:

  - Der Access Point wird nur 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 im WAP-Gerät 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 Durch Hochladen einer Konfiguration durch den Benutzer/Administrator wird die automatische Konfiguration außer Kraft gesetzt, sodass die ausgewählte Konfigurationsdatei Vorrang erhält. Bei jedem anderen Neustart des Access Points (Firmware-Upgrade/Neustartvorgänge usw.) wird die vorhandene automatische Konfigurationseinstellung beibehalten.

- **IPv4-Adresse/Hostname des Backup-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 den

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 Konfiguration des Access Points 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.

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

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Dabei werden die Verbindungen des WAP-Geräts möglicherweise unterbrochen. Es wird empfohlen, die Einstellungen des WAP-Geräts zu einem Zeitpunkt zu ändern, zu dem ein Konnektivitätsverlust die geringsten Auswirkungen auf die WLAN-Clients hat.

IPv6-Einstellung

Auf der Seite „IPv6-Adressen“ können Sie das WAP-Gerät für die Verwendung von IPv6-Adressen konfigurieren.

So konfigurieren Sie IPv6-Adresseinstellungen:

SCHRITT 1 Wählen Sie **LAN** > **IPv6-Einstellung**.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **IPv6-Verbindungstyp**: Wählen Sie aus, auf welche Weise das WAP-Gerät eine IPv6-Adresse bezieht:
  - **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 (200 1:DB8::CAD5:7D9 1) ein.

HINWEIS Wenn die statische IPv6-Adresse konfiguriert ist, fällt DHCPv6 aus. Wenn DHCPv6 konfiguriert ist, kann die IPv6-Adresse eingesetzt werden, sofern eine Konfiguration vorhanden ist.

- **IPv6-Administrationsmodus**: Aktiviert oder deaktiviert den IPv6-Verwaltungszugriff.
- **IPv6-Administrationsmodus – Automatische Konfiguration**: Aktiviert die automatische Konfiguration von IPv6-Adressen für das WAP-Gerät.

  Wenn diese Option aktiviert ist, lernt das WAP-Gerät die IPv6-Adressen und das Gateway durch Verarbeiten der am LAN-Anschluss empfangenen Routerankündigungen. Das WAP-Gerät kann mehrere automatisch konfigurierte IPv6-Adressen haben.
- **Statische-IPv6-Adresse**: Die statische IPv6-Adresse. Das WAP-Gerät kann auch dann eine statische IPv6-Adresse haben, wenn die Adressen automatisch konfiguriert wurden.
- **Static IPv6 Address Prefix Length**: Die Präfixlänge der statischen Adresse, bei der es sich um eine Ganzzahl im Bereich von 0 bis 128 handelt. Der Standardwert lautet „0“.
- **Status der statischen IPv6-Adresse**: Wählen Sie eine der folgenden Optionen:
  - **Einsatzbereit**: Die Eindeutigkeit der IP-Adresse im LAN wurde überprüft. Die IP-Adresse kann an der 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. Eine IPv6-Adresse gilt mit Vorbehalt, während ihre Eindeutigkeit im Netzwerk überprüft wird. Mit diesem Status kann die IPv6-Adresse nicht zum Senden oder Empfangen von regulärem Verkehr verwendet werden.

  - **Leer (kein Wert)**: Es ist keine IP-Adresse zugewiesen, oder die zugewiesene IP-Adresse ist nicht funktionsfähig.

- **Automatisch konfigurierte globale IPv6-Adressen**: Wenn dem WAP-Gerät automatisch eine oder mehrere IPv6-Adressen zugewiesen wurde, werden die Adressen aufgeführt.
- **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-Nameserver werden dynamisch über DHCPv6 vermittelt.
  - **Manuell**: Sie können bis zu zwei IPv6-DNS-Nameserver manuell in die entsprechenden Felder ein.

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

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Dabei werden die Verbindungen des WAP-Geräts möglicherweise unterbrochen. Es wird empfohlen, die Einstellungen des WAP-Geräts zu einem Zeitpunkt zu ändern, zu dem ein Konnektivitätsverlust die geringsten Auswirkungen auf die WLAN-Clients hat.

IPv6-Tunnel

Die WAP571/E-Geräte unterstützen ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Mithilfe von 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.

So konfigurieren Sie einen IPv6-Tunnel mit ISATAP:

SCHRITT 1 Wählen Sie im Navigationsbereich **LAN** > **IPv6-Tunnel** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **ISATAP-Status**: Aktiviert oder deaktiviert den administrativen ISATAP-Modus im WAP-Gerät.
- **ISATAP-fühiger Host**: Die IP-Adresse oder der DNS-Name des ISATAP-Routers. Der Standardwert lautet „isatap“.
- **ISATAP-Abfrageintervall**: Gibt an, wie oft der AP beim Versuch, den ISATAP-Hostnamen in eine IP-Adresse aufzulösen, Abfragen an den DNS-Server senden soll. Das WAP-Gerät sendet nur dann DNS-Abfragen, wenn die Adresse eines ISATAP-Routers nicht bekannt ist. Gültig sind Werte im Bereich von 120 bis 3600 Sekunden. Der Standardwert liegt bei 120 Sekunden.
- **ISATAP-Anfrageintervall**: Gibt an, wie oft das WAP-Gerät Routeranfragenachrichten an die ISATAP-Router senden soll, von denen es durch die DNS-Abfragenachrichten erfährt. Das WAP sendet nur dann Solicitation-Mitteilungen, wenn es keinen aktiven ISATAP-Router gibt. Gültig sind Werte im Bereich von 120 bis 3600 Sekunden. Der Standardwert liegt bei 120 Sekunden.

SCHRITT 3 Klicken Sie auf **Speichern**. Die Einstellungen werden in der Startkonfiguration gespeichert.

Wenn der Tunnel aufgebaut wurde, werden **ISATAP-IPv6-Link Local-Adresse** und **Globale ISATAP-Pv6-Adresse** auf der Seite angezeigt. Dabei handelt es sich um die virtuellen IPv6-Schnittstellenadressen für das IPv4-Netzwerk.

LLDP

LLDP (Link Layer Discovery Protocol) ist durch den IEEE 802.1AB-Standard definiert und ermöglicht dem UAP, Informationen zum eigenen Systemnamen, zu Systemfunktionen und Leistungsbedarf auszugeben. Diese Informationen können Ihnen dabei helfen, die Topologie des Systems zu ermitteln und fehlerhafte Konfigurationen auf dem LAN zu erkennen. Der Access Point 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.

So konfigurieren Sie LLDP-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich **LAN > LLDP** aus

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **LLDP-Modus**: Der administrative Modus des LLDP auf dem Access Point. Wenn LLDP aktiviert ist, überträgt der Access Point LLDP-Protokolldateneinheiten an benachbarte Geräte.
- **TX-Intervall** – Die Anzahl der Sekunden zwischen den Übertragungen von LLDP-Mitteilungen. Gültig sind Werte im Bereich von 5 bis 32.768 Sekunden. Der Standardwert liegt bei 30 Sekunden.
- **POE-Priorität**: Der vom AP übertragene Prioritätslevel im Extended Power-Informationselement. Der PoE-Prioritätslevel unterstützt das PSE (Power Sourcing Equipment), beispielsweise einen Switch, dabei, festzulegen, welchen strombetriebenen Geräten Priorität bei der Leistungszuweisung eingeräumt werden soll, wenn das PSE nicht über ausreichend Kapazität verfügt, um die angeschlossenen Geräte mit Energie zu versorgen. Folgende PoE-Prioritäten sind möglich:
  - Kritisch
  - Hoch
  - Niedrig

- Unbekannt

SCHRITT 3 Klicken Sie auf **Speichern**. Die Einstellungen werden im System gespeichert.

5

Wireless

In diesem Abschnitt wird beschrieben, wie Sie die Eigenschaften für den Funkbetrieb konfigurieren.

Das Kapitel enthält die folgenden Themen:

- **Funk**
- **Rogue-AP-Erkennung**
- **Netzwerke**
- **Wireless Multicast Forwarding (WMF)**
- **Planungsmodul**
- **Planungsmodulzuordnung**
- **MAC-Filterung**
- **Bridge**
- **QoS**

Funk

Die Funkeinstellungen steuern direkt das Verhalten des Funkmoduls im WAP-Gerät sowie dessen Interaktionen mit dem physischen Medium. Das heißt, sie steuern, welchen Signaltyp das WAP-Gerät auf welche Weise ausgibt.

Konfigurieren der Funkeinstellungen

So konfigurieren Sie die Funkeinstellungen:

SCHRITT 1 Wählen sie im Navigationsbereich **Wireless** > **Funk** aus.

SCHRITT 2 Konfigurieren Sie im Bereich „Globale Einstellungen“ das **TSPEC-Verletzungsintervall**, bei dem es sich um das Zeitintervall in Sekunden handelt,

in dem das WAP-Gerät zugeordnete Clients meldet, die sich nicht an die verpflichtenden Zugangskontrollverfahren halten. 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.

SCHRITT 3 Wählen Sie die **Funkschnittstelle** aus, die Sie konfigurieren möchten (Funkmodul 1 oder Funkmodul 2).

SCHRITT 4 Konfigurieren Sie im Bereich „Basiseinstellungen“ die folgenden Einstellungen:

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

- **Funk**: Schaltet die Funkschnittstelle ein oder ab. Der Funk ist standardmäßig eingeschaltet.

HINWEIS Wenn Sie die Funkmodule mit 5 GHz und 80 MHz Bandbreite aktivieren und das Datenverkehrsaufkommen hoch ist, wird die vom WAP-Gerät benötigte Leistung durch den IEEE 802.3af PoE-Standard (12,95 W) nicht gedeckt. Es wird dringend empfohlen, das WAP-Gerät mit einem 802.3at-PSE mit Strom zu versorgen, wenn ein 80-MHz-Kanal verwendet wird. Wenn die vom WAP-Gerät benötigte Leistung die Maximalleistung des PSE übersteigt, wird das WAP-Gerät möglicherweise neu gestartet.

- **MAC-Adresse**: Die Media Access Control (MAC)-Adresse für die Schnittstelle. Die MAC-Adresse wird vom Hersteller zugewiesen und kann nicht geändert werden.
- **Modus**: IEEE 802.11-Standard und Frequenz, die vom Funk verwendet werden. Der Standardwert für Mode ist 802.11a/n/ac für Radio 1 und 802.11b/g/n für Radio 2. Wählen Sie für jede Funkschnittstelle einen der verfügbaren Modi.

  Funkmodul 1 unterstützt die folgenden Funkmodi:

  - **802.11a**: Nur 802.11a-Clients können sich mit dem WAP-Gerät verbinden.
  - 802.11a/n/ac – 802.11a-Clients, 802.11n und 802.11ac-Clients, die mit der 5-GHz-Frequenz betrieben werden, können sich mit dem WAP-Gerät verbinden.
  - 802.11n/ac – 802.11n-Clients und 802.11ac-Clients, die mit der 5-GHz-Frequenz betrieben werden, können sich mit dem WAP-Gerät verbinden.

  Funkmodul 2 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, die mit der 2,4-GHz-Frequenz betrieben werden, können sich mit dem WAP-Gerät verbinden.
- 802.11n 2.4-GHz: Nur 802.11n-Clients, die mit der 2,4-GHz-Frequenz betrieben werden, können sich mit dem WAP-Gerät verbinden.

- **Kanalbandbreite** (nur 802.11n- und 802.11ac-Modi): Die 802.11n-Spezifizierung erlaubt neben dem älteren 20-MHz-Kanal, der in anderen Modi verfügbar ist, einen 40-MHz-breiten Kanal. Der 40-MHz-Kanal ermöglicht höhere Datenraten, lässt jedoch weniger verfügbare Kanäle übrig, die von anderen 2,4-GHz- und 5-GHz-Geräten verwendet werden können.

  Die 802.11ac-Spezifizierung erlaubt neben den 20-MHz- und 40-MHz-Kanälen einen 80-MHz-breiten Kanal.

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

- **Primärer Kanal** (Nur 802.11n-Modi mit 20 oder 40 MHz Bandbreite): Ein 40-MHz-Kanal besteht normalerweise aus zwei 20-MHz-Kanälen, die in der Frequenzdomäne aneinander angrenzen. Diese beiden 20-MHz-Kanäle werden häufig als die primären und sekundären Kanäle bezeichnet. Der primäre Kanal wird für 802.11n-Clients verwendet, die nur eine Kanalbandbreite von 20 MHz unterstützen und für ältere Clients.

  Wählen Sie eine der folgenden Optionen aus:

  - **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 der Funk für Übertragung und Empfang verwendet.

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

- **Spektrumanalysemodus**: Der Status des Spektrumanalysemodus. Der Spektrumanalysemodus kann „Deaktiviert“, „Dedizierte Spektrumanalyse“ oder „Hybridspektrumanalyse“ sein. Die Standardeinstellung ist „Deaktiviert“.

SCHRITT 5 Konfigurieren Sie im Bereich „Advanced Settings“ die folgenden Einstellungen:

- **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 eine Funktion, mit der 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 funktioniert nur für das 5-GHz-Frequenzband. 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 **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 ergibt sich eine Steigerung des Datendurchsatzes um 10 Prozent.

  Das kurze Guard Interval muss auch von dem Client unterstützt werden, mit dem das WAP-Gerät kommuniziert.

  Wählen Sie eine der folgenden Optionen aus:

  - **Ja**: Das WAP-Gerät überträgt Daten mithilfe eines 400-Nanosekunden-Schutzintervalls, wenn es mit Clients kommuniziert, die auch das kurze Schutzintervall unterstützen. Die Standardauswahl lautet „Yes“.
  - **Neiin**: Das WAP-Gerät überträgt Daten mithilfe eines 800-Nanosekunden-Schutzintervalls.

- **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“). Jedoch können 802.11n-Übertragungen dann Auswirkungen auf ältere Clients oder WAP-Geräte innerhalb der Reichweite haben. Der Schutz ist auch verfügbar, wenn der 802.11b/g-Modus ausgewählt ist. 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 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.

  Aus dem angegebenen DTIM-Zeitraum geht hervor, wie oft die Clients, für die das WAP-Gerät zuständig ist, überprüfen sollen, ob im WAP-Gerät auf den Abruf wartende zwischengespeicherte Daten vorhanden sind.

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

- **Fragmentierungsschwelle**: Die Schwelle für Framegrößen in Byte. Gültig ist eine gerade Ganzzahl im Bereich von 256 bis 2346. Der Standardwert lautet „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 Fragmentierungsfunktion aktiviert, und das Paket wird in Form mehrerer 802.11-Frames gesendet.

  Wenn das zu sendende Paket maximal der Schwelle entspricht, wird keine Fragmentierung verwendet. Wenn Sie die Schwelle auf den höchsten Wert (den Standardwert „2.346 Byte“) festlegen, deaktivieren Sie die Fragmentierung damit effektiv.

  Durch die Fragmentierung ergibt sich ein höherer Aufwand, da die Frames aufgeteilt und erneut zusammengesetzt werden müssen und sich der Nachrichtenverkehr im Netzwerk erhöht. Wenn die Fragmentierung richtig konfiguriert ist, kann sie jedoch zur Verbesserung der Netzwerkleistung und -zuverlässigkeit beitragen.

Durch das Senden kleinerer Frames (mithilfe einer niedrigeren Fragmentierungsschwelle) können Sie möglicherweise manche Interferenzprobleme vermeiden, beispielsweise im Zusammenhang mit Mikrowellenherden.

Aggregierte 802.11n- oder 802.11ac-Frames (AMPDUs) können nicht fragmentiert werden. Die Fragmentierung kann nur für ältere Funkmodi wie 802.11a oder 802.11b/g angewendet werden.

Die Fragmentierung ist standardmäßig deaktiviert. Es wird empfohlen, Fragmentierung nur zu verwenden, 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. Gültig ist eine Ganzzahl im Bereich von 0 bis 65535. Der Standardwert lautet „65535 Oktette“.

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

  Durch Ändern der RTS-Schwelle können Sie insbesondere bei WAP-Geräten mit zahlreichen Clients den Verkehrsfluss durch das WAP-Gerät steuern. Wenn Sie eine niedrigere Schwelle 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.

  Die RTS-Schwelle wird nur für ältere 802.11-Daten-Frames verwendet (d.h. nicht für 802.11n oder 802.11ac). Bei 802.11n und 802.11ac werden AMPDU-Übertragungen unabhängig von der Frame-Länge durch einen RTS/CTS-Austausch geschützt.

- **Bandbreitennutzung**: **Wie viel der Funkbandbreite kann verwendet werden, bis das WAP-Gerät keine neuen Clientzuordnungen mehr zulässt. Gültig sind Ganzzahlen von 0 bis 100 Prozent. Ist dieser Wert auf 0 eingestellt, werden alle neuen Zuordnungen, unabhängig von ihrer Nutzungsrate, zugelassen. Die Standardeinstellung ist 0.**

- **Maximal zugeordnete Clients**: Die maximale Anzahl der Stationen, die gleichzeitig auf jedes Funkmodul dieses WAP-Geräts zugreifen dürfen. Sie können eine Ganzzahl zwischen 0 und 200 eingeben. Der Standartwert lautet 200 Stationen. Das Dualfunk-Gerät WAP571/E kann im Ganzen bis zu 400 Clients unterstützen.
- **Übertragungsleistung**: Ein Prozentwert für die Leistungsstufe der Übertragung für dieses 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. Dadurch 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 verügen.
- **Frame-Burst-Unterstützung**: **Die generelle Aktivierung von Frame-Burst-Unterstützung verbessert die Funkleistung im Downstream.**
- **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 Sekunden ausgedrückt.

  Unter „Supported Rate Sets“ werden die vom WAP-Gerät unterstützten Raten angegeben. Sie können durch Aktivieren einzelner Kontrollkästchen mehrere Raten aktivieren. Das WAP-Gerät wählt auf der Grundlage bestimmter Faktoren wie beispielsweise Fehlerraten und der Entfernung der Clientstationen zum WAP-Gerät automatisch die effizienteste Rate aus.

Unter „Basic Rate Sets“ 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.

  Standardmäßig ist die Option „Multicast/Broadcast Rate Limiting“ deaktiviert. Die folgenden Felder werden erst aktiviert, wenn Sie „Multicast/Broadcast Rate Limiting“ 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.

- **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. Verwenden Sie diese Einstellung, wenn das WAP-Gerät Verkehr von QoS-fähigen Geräten wie beispielsweise Wi-Fi-zertifizierten Telefonen verarbeitet.

  - **Aus**: Das WAP-Gerät ignoriert TSPEC-Anfragen von Clientstationen. Verwenden Sie diese Einstellung, wenn Sie TSPEC nicht verwenden möchten, um QoS-fähigen Geräten Priorität für zeitkritischen Verkehr zuzuweisen.

- **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 Verkehr 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.

- **TurboQAM**: Der Zweck dieser Funktion besteht in der Aktivierung/Deaktivierung von Broadcom-spezifischen Erweiterungen in VHT für Broadcom-zu-Broadcom-Verbindungen. Die VHT-Funktion ermöglicht Support für 256QAM-VHT-Raten, die nicht durch den 802.11ac-Entwurf spezifiziert wurden. Bei allen Raten handelt es sich um den VHT-LDPC-Modus: MCS 9 Nss 1 20Mhz, MCS 9 Nss 2 20Mhz, MCS 6 Nss 3 80Mhz. Die VHT-Funktion wird für 802.11ac PHY unterstützt.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

VORSICHT Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

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 einen kostengünstigen Wireless-AP installieren können, der möglicherweise nicht autorisierten Personen den Zugriff auf das Netzwerk ermöglicht.

Der AP führt in jedem Funkmodul 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 zu „Known AP List“ hinzufügen.

HINWEIS „Detected Rogue AP List“ und „Trusted AP List“ enthalten Informationen, die Sie für weitere Maßnahmen verwenden können. Der AP hat keine Kontrolle über Rogue-APs in den Listen und kann auf die beim RF-Scan erkannten APs keine Sicherheitsrichtlinien anwenden.

Zum Anzeigen weiterer Informationen zu Rogue-APs wählen Sie im Hauptnavigationsbereich die Option „Wireless“ > „-RogueAP -Erkennung“ aus.

Zum Anzeigen weiterer Informationen zu Rogue-APs wählen Sie die Option **Wireless > Rogue-AP-Erkennung** aus.

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

Anzeigen der Rogue-AP-Liste

Sie können die Rogue-AP-Erkennung aktivieren und deaktivieren. Zum Aktivieren der Erfassung von Informationen zu Rogue-APs durch das Funkmodul klicken Sie auf **Aktivieren** neben **AP-Erkennung** (für Funkmodul 1 oder Funkmodul 2) und dann auf **Speichern**.

Die Rogue-AP-Erkennung verfügt über keine Aktualisierungmethode und die SSID wird nach der Erkennung in der Datenbank gespeichert.

Daraufhin werden Informationen zu erkannten und vertrauenswürdigen Rogue-Access Points angezeigt. Sie können auf **Aktualisieren** klicken, um den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

- **Aktion**: Wenn der AP in der Liste erkannter Rogue-APs enthalten ist, können Sie auf **Vertrauenswürdig** klicken, um den AP in die Liste vertrauenswürdiger APs zu verschieben.

  Wenn der AP in der Liste vertrauenswürdiger Rogue-APs enthalten ist, können Sie auf **Nicht vertrauenswürdig** klicken, um den AP in die Liste erkannter Rogue-APs zu verschieben.

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.

- **MAC-Adresse**: Die MAC-Adresse des Rogue-APs
- **Funk**: Zeigt an, ob der Rogue-AP auf Funkmodul 1 (wlan0) oder Funkmodul 2 (wlan1) erkannt wird.
- **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).

HINWEIS Das Beacon-Intervall legen Sie auf der Seite **Funk** fest.

- **Typ**: Der Typ des Geräts:

- „AP“ bedeutet, dass es sich beim Rogue-Gerät um einen AP handelt, der das IEEE 802.11 Wireless Networking Framework im Infrastrukturmodus verwendet.
- „Ad hoc“ weist auf eine Rogue-Station im Ad-hoc-Modus hin. Auf den Ad-hoc-Modus festgelegte Stationen kommunizieren direkt miteinander, ohne einen herkömmlichen AP zu verwenden. 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

  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.

- **Datenschutz**: Gibt an, ob Sicherheit für das Rogue-Gerät festgelegt ist:
  - „Off“ bedeutet, dass der Sicherheitsmodus des Rogue-Geräts auf „None“ (keine Sicherheit) festgelegt ist.
  - „On“ bedeutet, dass bestimmte Sicherheitsfunktionen für das Rogue-Gerät festgelegt sind.

HINWEIS Auf der Seite **Netzwerke** können Sie die Sicherheit für den AP konfigurieren.

- **WPA**: Gibt an, ob WPA-Sicherheit für den Rogue-AP aktiviert oder deaktiviert ist.
- **Band**: Der vom Rogue-AP verwendete IEEE 802.11-Modus (Beispiele: IEEE 802.11a, IEEE 802.11b, 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 802.11, 802.11n oder 802.11ac (oder eine Kombination dieser Modi).
- **Kanal**: Der Kanal, über den der Rogue-AP zurzeit sendet

  Der Kanal definiert den Teil des Funkspektrums, den das Funkmodul zum Senden und Empfangen verwendet.

HINWEIS Auf der Seite **Funk** können Sie den Kanal festlegen.

HINWEIS Wenn der AP im DFS-Kanal ausgeführt wird, ist Scanning untersagt. Daher werden keine Rogue-APs erkannt.

- **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 „Supported Rates“ angezeigten Raten.

  Die gemeldete Rate entspricht der Geschwindigkeit des letzten Pakets, das vom Access Point an den Client übertragen wurde. Dieser Wert kann innerhalb des angezeigten Ratensatzes auf Basis der Signalqualität zwischen AP und Client und der Geschwindigkeit, mit der Broadcast- oder Multicast-Frames gesendet werden, variieren. Wenn der AP mithilfe der Standardraten einen Broadcast-Frame an eine WLAN-Station sendet, zeigt das Feld 1 Mbit/s für 2,4-Ghz-Funkmodule und 6 Mbit/s für 5-Ghz-Funkmodule an. Clients, die inaktiv sind, übertragen mit hoher Wahrscheinlichkeit die niedrigen Standardraten.

- **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**.

Erstellen und Speichern einer „Vertrauenswürdige-AP-Liste“

So erstellen Sie eine „Vertrauenswürdige-AP-Liste“ und speichern diese in einer Datei:

SCHRITT 1 Klicken Sie in der Liste erkannter Rogue-APs neben den Ihnen bekannten APs auf **Vertrauenswürdig**. Die vertrauenswürdigen APs werden in „Trusted AP List“ verschoben.

SCHRITT 2 Wählen Sie in „Liste vertrauenswürdiger APs herunterladen/sichern“ **Sichern (AP auf PC)** aus.

SCHRITT 3 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 „Vertrauenswürdige-AP-Liste“

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

Gehen Sie wie folgt vor, um eine AP-Liste aus einer Datei zu importieren:

SCHRITT 1 Wählen Sie im Bereich „Liste vertrauenswürdiger APs herunterladen/sichern“ die Option **Herunterladen (PC auf AP)**.

SCHRITT 2 Klicken Sie auf **Durchsuchen** und wählen Sie die zu importierende Datei aus.

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 3 Wählen Sie aus, ob die vorhandene „Trusted AP List“ ersetzt werden soll oder ob die Einträge in der importierten Datei der „Trusted AP List“ hinzugefügt werden sollen.

a. Wählen Sie **Ersetzen** aus, um die Liste zu importieren und den Inhalt von „Liste bekannter APs“ zu ersetzen.

b. Wählen Sie **Zusammenführen** aus, um die Liste zu importieren und die APs in der importierten Datei den zurzeit in „Liste bekannter APs“ angezeigten APs hinzuzufügen.

SCHRITT 4 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.

Netzwerke

Durch virtuelle Access Points (VAPs) wird das WLAN in mehrere Broadcast-Domänen segmentiert, die das WLAN-Äquivalent von Ethernet-VLANs darstellen. VAPs simulieren in einem physischen WAP-Gerät mehrere Access Points. Der AP unterstützt bis zu 16 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. Zum Deaktivieren des Betriebs von VAP0 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 2bis 32Zeichen sein, bei dem zwischen Groß- und Kleinschreibung unterschieden wird. Zulässig sind druckbare Zeichen sowie Leerzeichen (ASCII 0x20).

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 WAP571/E-Gerät unterstützt 33 aktive VLANs (32 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 im Navigationsbereich **Wireless** > **Netzwerke** aus.

SCHRITT 2 Wählen Sie die **Funk**schnittstelle aus, auf der Sie VAPs konfigurieren möchten (**Funkmodul 1** oder **Funkmodul 2**).

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **Aktiviert** für den zu konfigurierenden VAP.

Oder

Wenn es sich bei VAP0 um den einzigen im System konfigurierten VAP handelt und Sie einen VAP hinzufügen möchten, klicken Sie auf **Hinzufügen**. Wählen Sie den VAP aus, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die Parameter:

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

VORSICHT Die eingegebene VLAN-ID muss im Netzwerk richtig konfiguriert sein. Wenn der VAP WLAN-Clients einen nicht richtig konfigurierten VLAN zuordnet, kann es zu Netzwerkproblemen kommen.
Wenn ein WLAN-Client über diesen VAP eine Verbindung mit dem WAP-Gerät herstellt, kennzeichnet das WAP-Gerät den gesamten Verkehr vom WLAN-Client mit der in dieses Feld eingegebenen VLAN-ID, es sei denn, Sie geben die VLAN-ID ein oder weisen einen WLAN-Client mithilfe eines RADIUS-Servers einem VLAN zu. Für die VLAN-ID sind Werte im Bereich von 1 bis 4094 gültig.

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

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

HINWEIS 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 die Verbindung mit der neuen SSID wiederherstellen.

- **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.

- **Sicherheit**: Der Typ der für den Zugriff auf den VAP erforderlichen Authentifizierung:
  - Ohne
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

Wenn Sie einen anderen Sicherheitsmodus als „None“ auswählen, werden zusätzliche Felder angezeigt. Es wird empfohlen, den Authentifizierungstyp „WPA Personal“ oder „WPA Enterprise“ zu verwenden, da diese mehr Schutz bieten. Verwenden Sie „Static WEP“ oder „Dynamic WEP“ nur für ältere WLAN-Computer oder -Geräte ohne Unterstützung für „WPA Personal„ bzw. „WPA Enterprise“. Wenn Sie den Sicherheitsmodus „Static WEP“ oder „Dynamic WEP“ festlegen möchten, konfigurieren Sie für das Funkmodul den 802.11a- oder 802.11b/g-Modus (siehe **Funk**). Im 802.11n-Modus können Sie die Sicherheitsmodi „Static WEP“ oder „Dynamic WEP“ nicht verwenden.

- **MAC-Filterung**: Gibt an, ob die Stationen, die auf diesen VAP zugreifen können, auf eine konfigurierte globale Liste von MAC-Adressen beschränkt sind (siehe **MAC-Filterung**). Sie können für die MAC-Filterung die folgenden Typen auswählen:
  - **Deaktiviert**: Die MAC-Filterung wird nicht verwendet.
  - **Lokal**: Die auf der Seite **MAC-Filterung** konfigurierte MAC-Authentifizierungsliste wird verwendet.
  - **RADIUS**: Die MAC-Authentifizierungsliste auf einem externen RADIUS-Server wird verwendet.
- **Kanalisolierung**: Aktiviert und deaktiviert die Isolierung von Stationen.
- Wenn diese Option deaktiviert ist, können WLAN-Clients normal miteinander kommunizieren, indem sie Verkehr durch das WAP-Gerät senden.
  - Wenn die Option aktiviert ist, blockiert das WAP-Gerät die Kommunikation zwischen WLAN-Clients des gleichen VAPs. Das WAP-Gerät lässt dennoch Datenverkehr zwischen den WLAN-Clients und drahtgebundenen Geräten im Netzwerk über eine WDS-Verbindung sowie zu anderen einem anderen VAP zugeordneten WLAN-Clients zu. Verbindungen zwischen WLAN-Clients sind jedoch nicht zulässig.

HINWEIS Channel Isolation ist auf Clients anwendbar, die mit demselben VAP eines einzelnen AP verbunden sind, aber nicht auf Clients, die mit demselben VAP verschiedener APs verbunden sind. Clients, die also mit demselben VAP eines einzelnen AP verbunden sind, können einander nicht anpingen. Clients, die mit demselben VAP von verschiedenen APs verbunden sind können dies aber sehr wohl.

- **Band Steering**: Ermöglicht Band Steering, wenn beide Funkmodule aktiv sind. Die n-Bandbreite des Funk wird nicht für Band Steering berücksichtigt. Selbst wenn der 5-GHz-Funk zufällig die 20-MHz-Bandbreite verwendet, versucht der AP, sobald Band Steering konfiguriert wurde, Clients auf den 5-GHz-Funk zu verschieben.

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

VORSICHT Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

HINWEIS Zum Löschen eines VAPs wählen Sie den VAP aus, und klicken Sie auf **Löschen**. Klicken Sie anschließend auf **Speichern**, um die Löschung dauerhaft zu speichern.

Konfigurieren von Sicherheitseinstellungen

In diesen Abschnitten werden die Sicherheitseinstellungen beschrieben, die Sie abhängig von der Auswahl in der Liste „Sicherheit“ auf der Seite „Netzwerke“ konfigurieren.

Keine (Unverschlüsselt)

Wenn Sie den Sicherheitsmodus **Keine** auswählen, können Sie keine zusätzlichen Sicherheitseinstellungen für den AP konfigurieren. In diesem Modus werden die zum und vom AP 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. (Bei dem Verschlüsselungsalgorithmus handelt es sich um eine Stream-Verschlüsselung, die als RC4 bezeichnet wird.)

Sie konfigurieren „Static WEP“ mit den folgenden Parametern:

- **Übertragungsschlüsselindex**: Eine Liste der Schlüsselindizes Zur Verfügung stehen die Schlüsselindizes 1 bis 4. Der Standardwert lautet „1“.

  Aus dem „Transferschlüsselindex“ geht hervor, welchen WEP-Schlüssel das WAP-Gerät zum Verschlüsseln der übertragenen Daten verwendet.

- **Schlüssellänge**: Die Länge des Schlüssels Wählen Sie eine Option aus:

  - 64 Bit
  - 128 Bit

- **Schlüsseltyp**: Der Schlüsseltyp Wählen Sie eine Option aus:

  - ASCII
  - Hexadezimal

- **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: Enthält Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen wie @ und #.
  - Hex: Enthält 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 „Characters Required“. 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.

- **Erforderliche Zeichen**: Die Anzahl der Zeichen, die Sie in die Felder unter „WEP Key“ eingeben, hängt von der ausgewählten Schlüssellänge und dem ausgewählten Schlüsseltyp ab. Wenn Sie beispielsweise 128-Bit-ASCII-Schlüssel verwenden, müssen Sie für den WEP-Schlüssel 26 Zeichen eingeben. Die erforderliche Zeichenanzahl wird abhängig von den Angaben für Schlüssellänge und Schlüsseltyp automatisch aktualisiert.

- **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:

- **Offenes System**: Bei dieser Authentifizierung 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 Verkehr 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**: Bei dieser Authentifizierung 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-Schlüssel3 definiert sein.
- 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.)
- Bei manchen WLAN-Clientsoftwareanwendungen 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.

Dynamic WEP

Dynamic WEP ist eine Kombination aus 802.1x-Technologie und dem EAP-Protokoll (Extensible Authentication Protocol). Bei der Dynamic WEP-Sicherheit werden WEP-Schlüssel dynamisch geändert.

EAP-Nachrichten werden mithilfe des EAPOL-Protokolls (EAP Encapsulation Over LANs) über ein IEEE 802.11-WLAN gesendet. IEEE 802.1X stellt dynamisch generierte Schlüssel bereit, die regelmäßig aktualisiert werden. Der Textkörper des Frames wird mit RC4-Stream-Verschlüsselung verschlüsselt, und für die einzelnen 802.11-Frames wird eine CRC-Überprüfung (Cyclic Redundancy Checking) ausgeführt.

In diesem Modus müssen Benutzer mithilfe eines externen RADIUS-Servers authentifiziert werden. Für das WAP-Gerät ist ein RADIUS-Server mit EAP-Unterstützung erforderlich, beispielsweise Microsoft Internet Authentication Server. Für die Verwendung mit Microsoft Windows-Clients muss der Authentifizierungsserver PEAP (Protected EAP) und MSCHAP V2 unterstützen.

Sie können beliebige vom IEEE 802.1X-Modus unterstützte Authentifizierungsmethoden verwenden, beispielsweise Zertifikate, Kerberos und Authentifizierung durch öffentliche Schlüssel. Sie müssen die Clientstationen so konfigurieren, dass das gleiche Authentifizierungsverfahren wie für das WAP-Gerät verwendet wird.

Sie konfigurieren „Dynamic WEP“ mit den folgenden Parametern:

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

  Wenn Sie die globalen RADIUS-Servereinstellungen verwenden möchten, muss das Kontrollkästchen aktiviert sein.

  Wenn Sie für den VAP einen separaten RADIUS-Server verwenden möchten, deaktivieren Sie das Kontrollkästchen, und geben Sie die IP-Adresse des RADIUS-Servers sowie den Schlüssel in die folgenden 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-Addresse 1** oder **Server-IPv6-Addresse 1**: Die Adresse des primären RADIUS-Servers für diesen VAP.

  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 angegebene Adresse gesendet.

  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.

- **Server-IP-Addresse 2** bis **4** oder **Server-IPv6-Adresse 2** bis **4**: Bis zu drei IPv4- oder IPv6-Adressen für RADIUS-Backup-Server

  Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird der Reihe nach jeder konfigurierte Backup-Server ausprobiert.

- **Schlüssel**: Der gemeinsame geheime Schlüssel, den das WAP-Gerät für die Authentifizierung gegenüber dem 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** bis **Schlüssel 4**: Der RADIUS-Schlüssel, der den konfigurierten RADIUS-Backup-Servern zugeordnet ist. Der Server an Server-IP-Adresse (IPv6) 2 verwendet „Schlüssel 2“, der Server an Server-IP-Adresse (IPv6) 3 verwendet „Schlüssel 3“ usw.
- **RADIUS-Prüfung 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.
- **Aktiver Server**: Aktiviert die administrative Auswahl des aktiven RADIUS-Servers. Ist die Option deaktiviert, versucht das WAP-Gerät der Reihe nach eine Verbindung mit den einzelnen konfigurierten Servern herzustellen und wählt den ersten aktiven Server aus.
- **Aktualisierungsrate für Broadcast-Schlüssel**: Das Intervall, in dem der Broadcast-Schlüssel (Gruppenschlüssel) für diesem VAP zugeordnete Clients aktualisiert wird.

  Der Standardwert lautet „300“. 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.

WPA Personal

WPA Personal ist ein IEEE 802.11i-Standard der Wi-Fi Alliance, der AES-CCMP- und TKIP-Verschlüsselung umfasst. Bei der Personal-Version von WPA wird anstelle von IEEE 802.1X ein vorher vereinbarter Schlüssel (Pre-Shared Key, PSK) verwendet, 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.

Sie konfigurieren „WPA Personal“ mit den folgenden Parametern:

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

  Wenn im Netzwerk eine Mischung aus Clients vorhanden ist, das heißt einige Clients mit Unterstützung für WPA2 und andere nur mit Unterstützung für den ursprünglichen WPA-Modus, aktivieren Sie beide Kontrollkästchen. 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

- **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 #.
- **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**.
- **Aktualisierungsrate für Broadcast-Schlüssel**: Das Intervall, in dem der Broadcast-Schlüssel (Gruppenschlüssel) für diesem VAP zugeordnete Clients aktualisiert wird.

  Der Standardwert beträgt 300 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 mithilfe eines RADIUS-Servers authentifiziert werden.

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

Sie konfigurieren „WPA Enterprise“ mit den folgenden Parametern:

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

- **MFP (Management Frame Protection)** : Stellt Sicherheit für die andernfalls ungeschützten und unverschlüsselten 802.11-Management-Frames bereit. Dieses Feld ist nur sichtbar, wenn die Felder „WPA2-Sicherheit“ und „CCMP“ aktiviert sind. Hierzu können die folgenden drei Kontrollkästchenwerte konfiguriert werden. Der Standardwert laute „Wird unterstützt“.
  - Nicht erforderlich
  - Fähig
  - Erforderlich
- **Vorauthentifizierung aktivieren**: Wenn Sie unter „WPA Versions“ nur „WPA2“ oder „WPA and WPA2“ auswählen, können Sie die Vorauthentifizierung für WPA2-Clients aktivieren.

  Klicken Sie auf „Enable pre-authentication“, wenn WPA2-WLAN-Clients Vorauthentifizierungspakete senden sollen. Die Vorauthentifizierungsinformationen werden von dem zurzeit vom Client verwendeten WAP-Gerät an das WAP-Zielgerät weitergeleitet. Durch Aktivieren dieser Funktion können Sie die Authentifizierung für Roaming-Clients beschleunigen, die Verbindungen mit mehreren APs herstellen.

  Diese Option gilt nicht, wenn Sie unter „WPA Versions“ 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 einen RADIUS-Schlüssel
  - Eine gültige CCMP (AES)-RADIUS-IP-Adresse und einen RADIUS-Schlüssel
- **Globale RADIUS-Servereinstellungen verwenden**: Standardmäßig verwenden alle VAPs die für das WAP-Gerät definierten globalen RADIUS-Einstellungen (siehe **RADIUS-Server**). Sie können jedoch für jeden VAP andere RADIUS-Server konfigurieren.

  Wenn Sie die globalen RADIUS-Servereinstellungen verwenden möchten, muss das Kontrollkästchen aktiviert sein.

  Wenn Sie für den VAP einen separaten RADIUS-Server verwenden möchten, deaktivieren Sie das Kontrollkästchen, und geben Sie die IP-Adresse des RADIUS-Servers sowie den Schlüssel in die folgenden 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-Addresse 1** oder **Server-IPv6-Addresse 1**: Die Adresse des primären RADIUS-Servers für diesen VAP.

  Wenn **IPv4** als Option für **Server-IP-Adresstype** ausgewählt ist, geben Sie die IP-Adresse des von allen VAPs standardmäßig verwendeten RADIUS-Servers ein (beispielsweise 192.168.10.23). Wenn **IPv6** ausgewählt ist, geben Sie die IPv6-Adresse des primären globalen RADIUS-Servers ein (beispielsweise 2001:DB8:1234::abcd).

- **Server-IP-Adresse 2** bis **4** oder **Server-IPv6-Adresse 2** bis **4**: 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** bis **Schlüssel 4**: Der RADIUS-Schlüssel, der den konfigurierten RADIUS-Backup-Servern zugeordnet ist. Der Server an **„Server IP (IPv6) Address 2“** verwendet **„Key 2“**, der Server an **„Server IP (IPv6) Address 3“** verwendet **„Key 3“** usw.

- **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 300 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.

Wireless Multicast Forwarding (WMF)

Wireless Multicast Forwarding bietet eine effiziente Möglichkeit, den Multicast-Datenverkehr auf dem WLAN-Medium weiterzuleiten und die Multicast-Übertragungsprobleme im WLAN zu beseitigen, indem es den wiederholten Unicast von Multicast-Frames verwendet.

Es werden IGMP-Frames verwendet, um teilnehmende Gruppenmitglieder zu verfolgen. Multicast-Pakete werden nach der Unicast-MAC-Umwandlung nur an interessierte Mitglieder übertragen.

Mit WMF ist die Datenübertragung zuverlässiger, das die Frames als Unicast gesendet werden und eine stabile Übertragung möglich ist, da die dynamische Kontrolle pro Station basierend auf Link-Fehlern und Lärm durchgeführt werden kann.

Die Multicast-Gruppenmitglieder können eine STA-Emdgerät sein. Streaming zwischen STA-Geräten wird ebenfalls unterstützt. Der Multicast-Streaming-Server kann mit jedem LAN-Anschluss verbunden werden.

Konfigurieren von Wireless Multicast Forwarding-Einstellungen

So konfigurieren Sie Wireless Multicast Forwarding-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Optionen **Wireless > Wireless Multicast Forwarding** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter.

- **Wireless Multicast Forwarding (WMF)**: Wireless Multicast-Weiterleitung wird global auf dem Cisco WAP571/E aktiviert oder deaktiviert.

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

Planungsmodul

Mit dem Planungsmodul für Funkmodule und VAPs können Sie eine Regel mit einem konkreten Zeitintervall konfigurieren, in dem VAPs oder Funkmodule betriebsbereit sind. Auf diese Weise können Sie das Aktivieren bzw. Deaktivieren der VAPs und Funkmodule automatisieren.

So können Sie mit dieser Funktion beispielsweise den Betrieb des Funkmoduls nur während der Arbeitszeit planen, um die Sicherheit zu erhöhen und den Stromverbrauch zu verringern. Darüber hinaus können Sie das Planungsmodul verwenden, um WLAN-Clients den Zugriff auf VAPs nur zu bestimmten Tageszeiten zu ermöglichen.

Der AP 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.

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

Hinzufügen von Planungsmodulprofilen

So zeigen Sie den Planungsmodulstatus an und fügen ein Planungsmodulprofil hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless** > **Planungsmodul** aus

SCHRITT 2 Stellen Sie sicher, dass **Administrativer Modus** aktiviert ist. Standardmäßig ist die Option deaktiviert.

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

- **Status**: Der Betriebsstatus des Planungsmoduls. Der Bereich ist „Enabled“ oder „Disabled“. Die Standardeinstellung ist „Deaktiviert“.

- **Grund**: Der Grund für den Betriebsstatus des Planungsmoduls. Folgende Werte sind möglich:
  - **Aktiv**: Das Planungsmodul ist administrativ aktiviert.
  - **Administrationsmodus ist deaktiviert**: Der Betriebsstatus entspricht „Down“, da die globale Konfiguration deaktiviert ist.
  - **Systemzeit ist veraltet**: Die Systemzeit ist nicht synchronisiert.

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.

Konfigurieren von Planungsmodulregeln

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 alle 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.

Konfigurieren einer Regel für ein Profil

So konfigurieren Sie eine Regel für ein Profil:

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

SCHRITT 2 Klicken Sie auf **Regel hinzufügen**.

Die neue Regel wird in der Regeltabelle 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 der Betrieb des Funkmoduls oder des VAPs 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.
- End Time: Der Zeitpunkt, zu dem der Betrieb des Funkmoduls oder des VAPs 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**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Ein Planungsmodulprofil wird erst wirksam, wenn es einer Funkschnittstelle oder VAP-Schnittstelle zugeordnet ist. Weitere Informationen finden Sie auf der Seite: **Planungsmodulzuordnung**.

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

Gültigkeit von Planungsmodulregeln

Die Gültigkeit von Planungsmodulregeln wird hier beschrieben.

- Eine Regel, die nur für einen spezifischen Tag festgelegt wird, gilt nicht für andere Tage.
- Eine Regel, die Gruppen wie „Täglich“, „Wochentag“ oder „Wochenende“ verwendet, gilt für mehrere Tage.
- Eine Regel, die für „Wochenende“ festgelegt wurde, gilt nur für Samstag und Sonntag. Die anderen Tage sind davon nicht betroffen. Standardmäßig verhält sich das Planungsmodul so, dass das Funkmodul aktiviert ist, wenn für einen bestimmten Tag keine explizite Regel festgelegt ist, die besagt, wie lange das Funkmodul aktiv sein sollte.
- Das Planungsmodul ist so ausgelegt, dass jede Regel Bedingungen für die Aktivierung von Funkmodulen oder VAPs festlegt.

- Der Eintrag „Tag der Woche“ legt die Gültigkeit für die Regeln fest. Die Regel gilt NUR für den festgelegten Gültigkeitsbereich. Die Regel „Wochenende“ gilt nur für Sonntag und Samstag. „Täglich“ bedeutet jeden Tag usw. Bei der Festlegung der Regeln legt der GUI-Eintrag „Tag der Woche“ den Gültigkeitsbereich fest: Wochenende, Täglich, Wochentag, Sonntag, Montag usw.
- Die Definition detaillierterer Regeln wird möglich. Es gibt keine Regel, die implizit alles verweigert, wenn die Gültigkeit nicht jeden einzelnen Tag der Woche umfasst. Erstellen Sie eine Regel „deny“ oder „disable“, indem Sie die angemessene Gültigkeit nur eine Minute lang aktivieren. Damit Funkmodul oder VAP AUSSER für explizit vorgegebene Zeiten dauerhaft deaktivert bleiben, muss eine Regel für „Daily“ eingerichtet werden, die von Mitternacht bis 12:01 Uhr eine Minute lang aktiv ist. Das bedeutet, dass das Funkmodul nur eine Minute pro Tag läuft. Danach können Ausnahmen für jeden Zeitraum hinzugefügt werden, in dem das Funkmodul laufen soll.

Ein typisches Beispiel:

- Funkmodul aktivieren von 9:00 Uhr bis 17:00 Uhr von Montag bis Freitag
- Kein Funkmodul aktiviert am Wochenende.

Erstellen eines Profils mit zwei Regeln:

Wochentag: Startzeit: 09:00:00 Endzeit: 17:00

Wochenende Startzeit: 00:00 Endzeit: 00:01

Planungsmodulzuordnung

Planungsmodulprofile werden erst wirksam, wenn sie der WLAN-Schnittstelle oder VAP-Schnittstelle zugeordnet sind. Standardmäßig werden keine Planungsmodulprofile erstellt, und den Funkmodulen oder VAPs sind keine Profile zugeordnet.

Sie können der WLAN-Schnittstelle oder den einzelnen VAPs nur jeweils ein Planungsmodulprofil zuordnen. Ein einzelnes Profil kann mehreren VAPs zugeordnet sein. Wenn Sie das einem VAP oder der WLAN-Schnittstelle zugeordnete Planungsmodulprofil löschen, wird die Zuordnung entfernt.

Zuordnen eines Planungsmodulprofils zur WLAN-Schnittstelle oder einem VAP

So ordnen Sie ein Planungsmodulprofil der WLAN-Schnittstelle oder einem VAP zu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Optionen **Wireless** > **Planungsmodulzuordnung** aus. Wählen Sie die **Funk**schnittstelle aus, der Sie ein Planungsmodulprofil zuordnen möchten (**Funkmodul 1** oder **Funkmodul 2**).

SCHRITT 2 Für die WLAN-Schnittstelle oder einen VAP wählen Sie das Profil in der Liste **Profilname** aus.

In der Spalte **Schnittstellenbetriebsstatus** wird angezeigt, ob die Schnittstelle zurzeit aktiviert oder deaktiviert ist.

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

MAC-Filterung

Mithilfe der MAC-Filterung (Media Access Control, Medienzugriffssteuerung) können Sie nur für die aufgeführten Clientstationen die Authentifizierung gegenüber dem Access Point ausschließen oder zulassen. Die MAC-Authentifizierung können Sie auf der Seite **Netzwerke** pro VAP aktivieren und deaktivieren. Abhängig von der Konfiguration des VAPs verwendet das WAP-Gerät möglicherweise eine auf einem externen RADIUS-Server oder lokal im WAP-Gerät gespeicherte MAC-Filterliste.

Konfigurieren einer lokalen MAC-Filterliste im WAP-Gerät

Das WAP-Gerät unterstützt nur eine einzige lokale MAC-Filterliste. Das heißt, für alle VAPs, die für die Verwendung der lokalen Liste aktiviert sind, gilt die gleiche Liste. Sie können den Filter so konfigurieren, dass der Zugriff nur den MAC-Adressen in der Liste gewährt oder verweigert wird.

Sie können der Filterliste bis zu 512 MAC-Adressen hinzufügen.

Konfigurieren der MAC-Filterung

So konfigurieren Sie die MAC-Filterung:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless** > **MAC-Filterung** aus.

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

- **Nur Stationen in Liste zulassen**: Allen nicht in der Stationsliste enthaltenen Stationen wird der Zugriff auf das Netzwerk über das WAP-Gerät verweigert.
- **Alle Stationen 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 MAC-Filterliste.

SCHRITT 3 Geben Sie in das Feld **MAC-Adresse** die zuzulassende oder zu blockierende MAC-Adresse ein, und klicken Sie auf **Hinzufügen**.

Die MAC-Adresse wird in der **Stationsliste** angezeigt.

SCHRITT 4 Geben Sie weitere MAC-Adressen ein, bis die Liste vollständig ist, und klicken Sie dann auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Entfernen einer MAC-Adresse aus der Stationsliste wählen Sie die MAC-Adresse aus, und klicken Sie dann auf **Entfernen**.

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

Konfigurieren der MAC-Authentifizierung auf dem RADIUS-Server

Wenn mindestens ein VAP für die Verwendung eines auf einem RADIUS-Authentifizierungsserver gespeicherten MAC-Filters konfiguriert ist, 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

Bridge

In diesem Abschnitt werden die zwei Typen von Bridges beschrieben. Das Kapitel enthält die folgenden Themen:

WDS-Bridge

Mithilfe von WDS (Wireless Distribution System) können Sie mehrere WAP571/E-Geräte verbinden. Bei WDS kommunizieren Access Points ohne Kabel miteinander. Diese Möglichkeit spielt bei der nahtlosen Verwendung durch Roamingclients und bei der Verwaltung mehrerer WLANs eine wichtige Rolle. Außerdem können Sie dadurch die Netzwerkinfrastruktur vereinfachen, da weniger Kabel verlegt werden müssen. 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 und anderen Repeatern. 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 Clientzuordnungen 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 AP kann auch als Repeater fungieren. In diesem Modus dient der AP als Verbindung zwischen zwei APs, die möglicherweise zu weit voneinander entfernt sind, um das Funksignal zu empfangen. Wenn der AP als Repeater fungiert, ist keine Kabelverbindung mit dem LAN erforderlich, und die Signale werden über die WLAN-Verbindung weitergesendet. Sie müssen keine besonderen Einstellungen konfigurieren, um den AP als Repeater zu verwenden, und es gibt keine Einstellungen für den Repeater-Modus. 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:

- Für einen reinen Bridging-Modus, der keine Clientzuordnungen zulässt, empfehlen wir die Verwendung eines WPA-Schlüssels, der nicht als Klartext übermittelt wird, für VAP0 oder die Deaktivierung der SSID-Übertragung.

- 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.)

HINWEIS 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.

Weitere Informationen zum Konfigurieren dieser Einstellungen finden Sie unter **Funk** (Basiseinstellungen).

- 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.

So konfigurieren Sie eine WDS-Bridge:

SCHRITT 1 Wählen Sie im Navigationsbereich **Wireless** > **Bridge** aus.

SCHRITT 2 Wählen Sie im Dropdownmenü die WDS-Bridge aus.

SCHRITT 3 **Klicken Sie auf „Aktivieren“** für die **WDS-Schnittstelle**, die Sie konfigurieren möchten

SCHRITT 4 Konfigurieren Sie die übrigen Parameter:

- **Remote-MAC-Adresse**: Gibt die MAC-Adresse des WAP-Zielgeräts an, das heißt, des WAP-Geräts am anderen Ende der WDS-Verbindung, an das Daten gesendet oder übergeben werden und von dem Daten empfangen werden.

TIPP Die MAC-Adresse finden Sie auf der Seite „Status and Statistics“ > „Network Interface“.

- **Verschlüsselung**: Der für die WDS-Verbindung zu verwendende Verschlüsselungstyp, der nicht mit dem überbrückten VAP übereinstimmen muss. Die WDS-Verschlüsselungseinstellungen gelten nur für diese WDS-Bridge. Folgende Optionen sind möglich: „None“, „WEP“ und „WPA Personal“. WPA2-PSK ist eine Option für die Verschlüsselung von WDS-Verbindungen und die VAP-Sicherheit. Der Administrator muss eine der Optionen auswählen, um sie durchzusetzen.

  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 Informationen zu Verschlüsselungsoptionen finden Sie im Anschluss an dieses Verfahren unter **WEP für WDS-Verbindungen** oder **WPA/PSK für WDS-Verbindungen**.

HINWEIS Static WEP kann nur für Funkmodule verwendet werden, die mit älteren Modi arbeiten: 802.11a für 5-GHz-Funkmodule und 802.11b/g für 2,4-GHz-Funkmodule.

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

SCHRITT 6 Wiederholen Sie das Verfahren für die anderen Geräte, die Verbindungen mit der Bridge herstellen.

TIPP Sie können überprüfen, ob die Bridge-Verbindung aktiv ist, indem Sie die Seite „Status and Statistics“ > „Network Interface“ anzeigen. In der Tabelle „Interface Status“ sollte für WLAN0:WDS(x) der Status „Up“ angezeigt werden.

HINWEIS Der Partner WDS AP im Remote-Netzwerk speichert die vom mit dem WDS AP im Hauptnetzwerk verbundenen DHCP-Server erhaltene IP-Verwaltungsadresse selbst dann, wenn die WDS-Verbindung unterbrochen ist. Die IP-Adresse wird freigegeben, wenn die WDS-Schnittstelle administrativ deaktiviert wird.

VORSICHT Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

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, geben Sie den Typ des WEP-Schlüssels an: **ASCII** oder **Hex**.
- **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 geeigneten 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 #.

WorkGroup-Bridge

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

Die WorkGroup-Bridge-Funktion ermöglicht die Unterstützung des STA-Modus. Das WAP-Gerät kann in einem BSS (Basic Service Set) als STA-Gerät betrieben werden. Ist der WorkGroup-Bridge-Modus aktiviert, unterstützt der AP nur ein BSS, mit dem der AP als Wireless-Client zugeordnet wird

Es wird empfohlen, den WorkGroup-Bridge-Modus nur zu verwenden, wenn die WDS-Bridge-Funktion nicht mit einem Peer-AP verwendet werden kann. WDS ist als bessere Lösung der WorkGroup-Bridge-Lösung vorzuziehen. Verwenden Sie WDS, wenn Sie Cisco WAP571/E-Geräte überbrücken. Ziehen Sie anderenfalls den WorkGroup-Bridge-Modus in Betracht. Wenn die WorkGroup-Bridge-Funktion aktiviert ist, wird anstelle der VAP-Konfigurationen nur die WorkGroup-Bridge-Konfiguration angewendet.

HINWEIS Die WDS-Funktion kann nicht verwendet werden, wenn der WorkGroup-Bridge-Modus für den AP aktiviert ist.

Im WorkGroup-Bridge-Modus wird der vom WAP-Gerät (dem WAP-Gerät, dem das WAP-Gerät als STA zugeordnet wird) verwaltete BSS als Infrastrukturclient-Schnittstelle bezeichnet, und das andere WAP-Gerät wird als Upstream-AP bezeichnet.

Die mit der kabelgebundenen Schnittstelle des WAP-Geräts verbundenen Geräte können auf das Netzwerk zugreifen, das über die Infrastrukturclient-Schnittstelle verbunden ist.

Beachten Sie beim Konfigurieren der WorkGroup-Bridge-Funktion im WAP-Gerät die folgenden Richtlinien:

- Alle an der WorkGroup-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** (Basiseinstellungen).

- Im WorkGroup-Bridge-Modus wird zurzeit nur IPv4-Verkehr unterstützt.
- In einem Single Point Setup wird der WorkGroup-Bridge-Modus nicht unterstützt.

So konfigurieren Sie den WorkGroup-Bridge-Modus:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless > Bridge** aus.

SCHRITT 2 Wählen Sie aus der Dropdown-Liste „WorkGroup-Bridge-Modus“ aus.

SCHRITT 3 Wählen Sie für **WorkGroup Bridge Mode** die Option **Enable** aus.

SCHRITT 4 Wählen Sie die Funkschnittstelle aus, für die Sie den WorkGroup-Bridge-Modus konfigurieren möchten (**Funkmodul 1** oder **Funkmodul 2**).

SCHRITT 5 Konfigurieren Sie für die Infrastrukturclient-Schnittstelle (Upstream) die folgenden Parameter:

- **SSID**: Die SSID des BSS.

HINWEIS Unter SSID Scanning befindet sich ein Pfeil neben SSID. Diese Funktion ist standardmäßig deaktiviert und wird nur aktiviert, wenn unter „Rogue-AP-Erkennung“ die (ebenfalls standardmäßig deaktivierte) Option „AP-Erkennung“ aktiviert ist.

- **Sicherheit**: Der Typ der Sicherheit, die für die Authentifizierung als Clientstation für das Upstream-WAP-Gerät verwendet werden soll. Zur Auswahl stehen die folgenden Optionen:
  - **Ohne**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise**

- **VLAN ID**: Das dem BSS zugeordnete VLAN.

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. Das Feld „Connection Status“ gibt an, ob der WAP mit dem Upstream-WAP-Gerät verbunden ist. Sie können auf die Schaltfläche „Aktualisieren“ klicken, um den aktuellen Verbindungsstatus anzuzeigen.

WGB-AP (der AP, der als Client für den Upstream-AP fungiert) behält seine Management-IP-Adresse, die von einem Upstream-DHCP-Server bezogen wurde, selbst wenn er vom Upstream-AP getrennt wird.

HINWEIS Static WEP kann nur für Funkmodule verwendet werden, die mit älteren Modi arbeiten: 802.11a für 5-GHz-Funkmodule und 802.11b/g für 2,4-GHz-Funkmodule.

QoS

Mithilfe der QoS-Einstellungen (Quality of Service) können Sie Übertragungswarteschlangen im Hinblick auf optimierten Durchsatz und bessere Leistung konfigurieren, wenn differenzierter WLAN-Verkehr wie beispielsweise VoIP (Voice-over-IP), andere Arten von Audio und Video, Streaming-Medien und herkömmliche IP-Daten verarbeitet wird.

Zum Konfigurieren von QoS für den AP legen Sie Parameter für die Übertragungswarteschlangen für verschiedene WLAN-Verkehrstypen fest und geben (mithilfe von Konfliktfenstern) minimale und maximale Wartezeiten für die Übertragung an.

EDCA-Parameter (Enhanced Distributed Channel Access) für WAPs beeinflussen den Verkehrsfluss vom WAP-Gerät zur Clientstation.

EDCA-Parameter für Stationen beeinflussen den Verkehrsfluss von der Clientstation zum WAP-Gerät.

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

Konfigurieren von EDCA-Parametern für das WAP-Gerät und für die Stationen

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless** > **QoS**Wählen Sie die Funkschnittstelle aus, für die Sie QoS-Einstellungen konfigurieren möchten (**Funkmodul 1** oder **Funkmodul 2**).

SCHRITT 2 Wählen Sie in der Liste **EDCA-Vorlage** eine Option aus:

- **WFA-Standards**: Füllt die EDCA-Parameter für das WAP-Gerät und die Stationen mit Standardwerten der WiFi Alliance, die sich für allgemeinen gemischten Verkehr am besten eignen.
- **Optimiert für Sprache**: Füllt die EDCA-Parameter für das WAP-Gerät und die Stationen mit für Sprachverkehr am besten geeigneten Werten.
- **Benutzerdefiniert**: Ermöglicht die Auswahl benutzerdefinierter EDCA-Parameter.

Diese vier Warteschlangen definieren Sie für verschiedene Datentypen, 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 (Sprach)**: 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 (Background)**: 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 3 Konfigurieren Sie die folgenden EDCA-Parameter und EDCA-Stationsparameter:

HINWEIS Diese Parameter können Sie nur konfigurieren, wenn Sie im vorherigen Schritt die Option „Custom“ ausgewählt haben.

- **Arbitration Inter-Frame Space**: Eine 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 einer Übertragung 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.

  Gültig sind die Werte 1, 3, 7, 15, 31, 63, 127, 255, 511 oder 1023. Der Wert muss niedriger sein als der Wert für „Maximum Contention Window“.

- **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.

  Gültig sind die Werte 1, 3, 7, 15, 31, 63, 127, 255, 511 oder 1023. Der Wert muss höher sein als der Wert für „Minimum Contention Window“.

- **Maximale Burst-Länge** (nur WAP): 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.

- **Wi-Fi-MultiMedia (WMM)**: Wählen Sie **Aktivieren** aus, um WMM-Erweiterungen (Wi-Fi Multimedia) zu aktivieren. 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 den AP 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.

- **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 4 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.
- **Unscheduled Automatic Power Save Delivery**: Wählen Sie**Aktivieren** aus, um die Energieverwaltungsmethode APSD zu aktivieren. APSD wird empfohlen, wenn VoIP-Telefone über das WAP-Gerät auf das Netzwerk zugreifen.

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

VORSICHT Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

6

Spektrumanalyseprogramm

In diesem Abschnitt wird die Spektrumanalysator-Funktion auf dem AP-Gerät erläutert.

Spektrumanalyseprogramm

Die Spektrumanalyse-Funktion bietet eine umfassende Überwachung der Funkfrequenzumgebung und ermöglicht so Echtzeitmanagement eines Wireless-Netzwerks. Die Funktion ermöglicht es dem Administrator eines Wireless-Netzwerks, sowohl Echtzeit- als auch Verlaufsinformationen über die Funkfrequenzumgebung anzuzeigen.

Die Spektrumanalyse kann sämtliche IEEE 802.11-Kanäle in den 2,4-GHz- und 5-GHz-Frequenzbändern auf Nicht-Wi-Fi-Interferenzen überprüfen, die Interferenz klassifizieren und die Interferenzereignisse in lokalen Ereignisprotokollen am Netzwerk-Edge speichern.

HINWEIS Der Spektrumanalysator kann die folgenden Interferenzen aufzeichnen: analoges schnurloses Telefon, kabellose Videokamera, Mikrowelle, S-Band-Bewegungsmelder, Schmalband-Störsender, Breitband-Störsender und unbekannte Störungen.

Die Seite „Spektrumanalysator“ zeigt den Status der Spektrumanalysator-Funktion an und stellt den Link zum Anzeigen der Spektrumdaten bereit.

Konfigurieren des Spektrumanalyseprogramm

So konfigurieren Sie den Spektrumanalysator:

SCHRITT 1 Wählen Sie im Navigationsbereich **Spektrumanalysator** aus.

SCHRITT 2 Der Status des Spektrumanalysemodus. Der Status lautet „Dedizierte Spektrumanalyse“, „Hybridspektrumanalyse“ oder „Deaktiviert“. Die Standardeinstellung ist „Deaktiviert“. Der Spektrumanalysator unterstützt nur eine Frequenz zur selben Zeit.

HINWEIS 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. Im Hybridmodus werden Clientverbindungen garantiert, aber ein geringerer Durchsatz wird erwartet.

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

SCHRITT 4 Klicken Sie auf die Schaltfläche **Spektrumdaten anzeigen**, um die Spektrumanzeige zu starten, wenn der Scanmodus auf „Dedizierte Spektrumanalyse“ oder „Hybridspektrumanalyse“ eingestellt ist.

HINWEIS Der Zugriff auf die Spektrumanzeige kann nur über eine IPv4-Adresse erfolgen.

7

Systemsicherheit

In diesem Abschnitt wird die Konfiguration der Sicherheitseinstellungen auf dem AP-Gerät erläutert.

Folgende Themen werden behandelt:

- **RADIUS-Server**
- **802.1X-Supplicant**
- **Kennwortkomplexität**
- **WPA-PSK-Komplexität**

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, die WLAN-Zugriff kontrollieren (siehe Seite **Funk**). Die Sicherheitsmethoden „Dynamisches WEP“ und „WPA Enterprise“ verwenden 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 IP-v6-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. Weitere Informationen finden Sie auf der Seite: **Netzwerke**.

So konfigurieren Sie globale RADIUS-Server:

SCHRITT 1 Wählen Sie im Navigationsbereich **Systemsicherheit** > **RADIUS-Server** aus.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

- **Server-IP-Adresstyp**: Die IP-Version, die der RADIUS-Server verwendet.

  Sie können zwischen den Adresstypen zur Konfiguration von globalen IPv4- und IPv6-RADIUS-Adresseinstellungen wechseln, das WAP-Gerät kontaktiert jedoch nur den RADIUS-Server oder Server des Adresstyps, den Sie in diesem Feld auswählen.

- **Server-IP-Adresse 1** oder **Server-IPv6-Adresse 1**: Die Adressen für den primären, globalen RADIUS-Server.

  Wenn der erste Wireless-Client versucht, sich mit dem WAP-Gerät zu authentifizieren, 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** bis **4)** oder **Server-IPv6-Adresse (2** bis **4)**: Bis zu vier Backup-IPv4- oder IPv6-RADIUS-Serveradressen.

  Wenn die Authentifizierung mit dem primären Server fehlschlägt, wird der Reihe nach jeder konfigurierte Backup-Server ausprobiert.

- **Schlüssel1**: Der freigegebene geheime Schlüssel, den das WAP-Gerät verwendet, um den primären RADIUS-Server zu authentifizieren.

  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 von Ihnen eingegebene Text wird mit Sternchen versehen angezeigt.

- **Schlüssel (2** bis **4)**: Der den konfigurierten Backup-RADIUS-Servern zugeordnete RADIUS-Schlüssel. Der Server unter der **Server-IP-(IPv6)-Adresse 2** verwendet **Schlüssel 2**, der Server unter **Server-IP-(IPv6)-Adresse 3** verwendet **Schlüssel 3** und so weiter.

- **RADIUS-Prüfung 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**. Die Änderungen werden in der Startkonfiguration gespeichert.

802.1X-Supplicant

Die IEEE 802.1X-Authentifizierung ermöglicht es dem Access Point, Zugriff auf ein gesichertes kabelgebundenes Netzwerk zu erhalten. Sie können den Access Point als 802.1X-Supplicant (Client) im kabelgebundenen Netzwerk aktivieren. Ein Benutzername und Passwort, die mithilfe des MD5-Algorithmus verschlüsselt werden, können so konfiguriert werden, dass dem Access Point die Authentifizierung über 802.1X erlaubt wird.

In Netzwerken, die eine IEEE-802.1X-Port-basierte Netzwerkzugriffskontrolle verwenden, kann ein Supplicant keinen Zugriff auf das Netzwerk erhalten, bis der 802.1X-Authenticator Zugriff gewährt. Wenn Ihr Netzwerk 802.1X verwendet, müssen Sie 802.1X-Authentifizierungsinformationen auf dem WAP-Gerät konfigurieren, damit es diese dem Authenticator bereitstellen kann.

Die Seite 802.1X Supplicant ist in drei Bereiche unterteilt: Supplicant-Konfiguration, Zertifikatsdatei-Status und Zertifikatsdatei-Upload.

Im Bereich „Supplicant-Konfiguration“ können Sie den Betriebsstatus und grundlegende Einstellungen von 802.1X konfigurieren.

So konfigurieren Sie den 802.1X Supplicant:

SCHRITT 1 Wählen Sie im Navigationsbereich **Systemsicherheit** > **802.1X-Supplicant** aus.

SCHRITT 2 Klicken Sie auf **Aktualisieren**, um den Zertifikatsdatei-Status zu aktualisieren.

SCHRITT 3 Geben Sie folgende Parameter ein:

- **Verwaltungsmodus**: Aktiviert die Funktion „802.1X-Supplicant“.

- **EAP-Methode**: Der Algorithmus, der für die Verschlüsselung von Authentifizierungsbenutzernamen und -Passwörtern verwendet wird.
  - **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**: Das WAP-Gerät verwendet diesen Benutzernamen, wenn es auf Anfragen von einem 802.1X-Authenticator antwortet. Der Benutzername kann zwischen 1 und 64 Zeichen lang sein. ASCII-druckbare Zeichen sind zulässig. Hierzu zählen große und kleine alphabetische Zeichen, Ziffern und sämtliche Sonderzeichen außer Anführungszeichen.
- **Passwort**: Das WAP-Gerät verwendet dieses MD5-Passwort, wenn es auf Anfragen von einem 802.1X-Authenticator antwortet. Das Passwort kann zwischen 1 und 64 Zeichen lang sein. ASCII-druckbare Zeichen sind zulässig. Hierzu zählen große und kleine alphabetische Zeichen, Ziffern und sämtliche Sonderzeichen außer Anführungszeichen.

HINWEIS Im EAP-TLS-Modus verwendet das WAP-Gerät diese Identität, wenn es auf Anfragen von einem 802.1X-Authenticator antwortet. Das WAP-Gerät unterstützt Zertifikatsdateien im PEM-Format. Die Zertifikatsdatei muss einen privaten Schlüssel und Root-Zertifikate enthalten. Das WAP-Gerät geht davon aus, dass es sich bei der Zertifikatsdatei um eine passwortgeschützte Datei handelt. Das WAP-Gerät verwendet ein Passwort für privaten Schlüssel, um die Zertifikatsdatei zu entsperren.

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

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

Der Zertifikatsdatei-Status zeigt an, ob ein aktuelles Zertifikat existiert:

- **Zertifikatsdatei vorhanden**: Gibt an, ob die HTTP SSL-Zertifikatsdatei vorhanden ist Im Feld wird „Ja“ angezeigt, wenn es vorhanden ist. Die Standardeinstellung ist „Nein“.
- **Zertifikatsablaufdatum**: Gibt an, wann die HTTP-SSL-Zertifikatsdatei abläuft. Der Bereich ist ein gültiges Datum.

Im Bereich „Zertifikatsdatei-Upload“ können Sie eine Zertifikatsdatei auf den AP hochladen:

SCHRITT 1 Wählen Sie entweder**HTTP** oder **TFTP** als **Übertragungsmethode** aus.

SCHRITT 2 Wenn Sie HTTP ausgewählt haben, klicken Sie auf **Durchsuchen**, um die Datei auszuwählen

HINWEIS Informationen zur Konfiguration von HTTP- und HTTPS-Servereinstellungen finden Sie unter **HTTP-/HTTPS-Service**.

Wenn Sie TFTP ausgewählt haben, geben Sie den **Dateinamen** und die **TFTP-Server-IPv4-Adresse** ein. Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * sowie zwei oder mehr aufeinanderfolgende Punkte.

SCHRITT 3 Klicken Sie auf **Hochladen**.

Es wird ein Bestätigungsfenster angezeigt, gefolgt von einem Fortschrittsbalken, der den Status des Uploads angibt.

Kennwortkomplexität

Sie können Komplexitätsanforderungen für Passwörter konfigurieren, die für den Zugriff auf das Konfigurationsdienstprogramm des WAP-Geräts verwendet werden. Durch komplexe Passwörter wird die Sicherheit erhöht.

So konfigurieren Sie Passwortkomplexitätsanforderungen:

SCHRITT 1 Wählen Sie im Navigationsbereich **Systemsicherheit** > **Passwortkomplexität** aus.

SCHRITT 2 Wählen Sie für die Einstellung **Password Complexity** die Option **Enable** aus.

SCHRITT 3 Konfigurieren Sie die Parameter:

- **Mindestanzahl der Passwort-Zeichenklassen** – Die Mindestanzahl der Zeichenklassen, die im Passwort vertreten sein müssen. Die vier möglichen Zeichenklassen sind Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen auf einer Standardtastatur.
- **Passwort unterscheidet sich vom aktuellen** – Auswählen, damit Benutzer ein anderes Passwort eingeben müssen, wenn ihr aktuelles abläuft. Ist diese Funktion nicht ausgewählt, können Benutzer dasselbe Passwort eingeben, wenn es abläuft.
- **Maximum Password Length**: Kennwörter können aus maximal 64 bis 80 Zeichen bestehen. Der Standardwert lautet „64„.
- **Minimum Password Length**: Kennwörter müssen aus mindestens 0 bis 32 Zeichen bestehen. Der Standardwert lautet „8“.
- **Passwortablauf-Support** – Auswählen, damit Passwörter nach einer festgelegten Zeit ablaufen.
- **Password Aging Time**: Die Anzahl der Tage bis zum Ablauf eines neu erstellten Kennworts (1 bis 365). Die Standardeinstellung sieht 180 Tage vor.

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

WPA-PSK-Komplexität

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

So konfigurieren Sie die WPA-PSK-Komplexität:

SCHRITT 1 Wählen Sie im Navigationsbereich **Systemsicherheit** > **WPA-PSK-Komplexität** aus.

SCHRITT 2 Klicken Sie für die Einstellung **WPA-PSK Complexity** auf **Enable**, damit das WAP-Gerät WPA-PSK-Schlüssel anhand der konfigurierten Kriterien überprüft. Wenn Sie das Kästchen deaktivieren, wird keine dieser Einstellungen verwendet. Die WPA-PSK-Komplexität ist standardmäßig deaktiviert.

SCHRITT 3 Konfigurieren Sie die Parameter:

- **Minimale WPA-PSK-Zeichenklasse** – Die Mindestanzahl der Zeichenklassen, die in einer Zeichenkette vorhanden sein müssen. Die vier möglichen Zeichenklassen sind Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen auf einer Standardtastatur. Drei ist die Standardeinstellung.
- **WPA-PSK unterscheidet sich vom aktuellen** – Wählen Sie eine dieser Optionen aus:
  - **Aktivieren** – Benutzer müssen einen anderen Schlüssel konfigurieren, wenn ihr aktuelles abläuft.
  - **Deaktivieren** – Benutzer können den alten oder vorherigen Schlüssel verwenden, nachdem ihr aktueller abgelaufen ist.
- **Maximum WPA-PSK Length**: Der Schlüssel kann aus maximal 32 bis 63 Zeichen bestehen. Der Standardwert lautet „63“.
- **Minimum WPA-PSK Length**: Der Schlüssel muss aus mindestens 8 bis 16 Zeichen bestehen. Der Standardwert lautet „8“. Aktivieren Sie das Kontrollkästchen, damit Sie das Feld bearbeiten und diese Anforderung aktivieren können.

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

8

Client-QoS

Dieser Abschnitt bietet eine Übersicht der Client-Servicequalität (QoS). Außerdem werden die im Client-QoS-Menü verfügbaren Funktionen erläutert. Folgende Themen werden behandelt:

- **Globale Einstellungen**
- **Klassenzuordnung**
- **Richtlinienzuordnung**
- **Client-QoS-Zuordnung**
- **Client-QoS-Status**

Globale Einstellungen

Auf der Seite „Globale Einstellungen“ können Sie die Funktion für die Servicequalität des WAP-Geräts aktivieren oder deaktivieren.

Wenn Sie **Client QoS** deaktivieren, werden die Ratenbegrenzung und DiffServ-Konfigurationen global deaktiviert.

Wenn Sie diesen Modus aktivieren, können Sie auch den Modus „Servicequalität für Clients“ für bestimmte VAPs oder Ethernet aktivieren oder deaktivieren. Weitere Informationen finden in der Einstellung **Client-QoS-Mode** auf der Seite **Client-QoS-Zuordnung**.

Klassenzuordnung

Die QoS-Funktion enthält Unterstützung für DiffServ (Differentiated Services), die die Klassifizierung von Verkehr in Streams und eine bestimmte QoS-Behandlung gemäß definierten Verhaltensweisen pro Hop ermöglicht.

Standardmäßige 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, die zeitkritischen Verkehr enthalten, können Richtlinienzuordnungen zugewiesen werden, die diesen Klassen den Vorrang vor anderem Verkehr geben.

Sie können die Klassenzuordnung verwenden, um Verkehrsklassen zu definieren. Auf der Seite **Richtlinienzuordnung** können Sie Richtlinien definieren und ihnen Klassenzuordnungen zuordnen.

Konfigurieren einer IPv4-Klassenzuordnung

So können Sie eine IPv4-Klassenzuordnung hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie **Client-QoS > Klassenzuordnung**.

SCHRITT 2 Geben Sie im Feld „Klassenzuordnungsname“ den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

SCHRITT 3 Wählen Sie aus der Liste der ACL-Klassenzuordnungsypen „IPv4“ als ACL-Typ aus. Die IPv4-Klassenzuordnung gilt nur für IPv4-Verkehr im WAP-Gerät.

SCHRITT 4 Konfigurieren Sie im Bereich „Kriterienkonfiguration abstimmen“ diese Parameter, um die Pakete einer Klasse zuzuordnen:

- **Klassenzuordnungsname**: Wählen Sie die IPv4-Klassenzuordnung aus der Liste.

- **Übereinstimmung mit allen Paketen**: Die Übereinstimmungsbedingung gilt für alle Parameter in einem Layer-3-Paket. Wenn diese Option aktiviert ist, entsprechen alle Layer-3-Pakete der Bedingung.
- **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.
  - **Aus Liste auswählen**: Das ausgewählte Protokoll wird abgeglichen: IP, ICMP, IGMP, TCP oder UDP.
  - **Mit Wert abgleichen**: 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-IP**: Erfordert die Quell-Ipv4-Adress eines Pakets, um die in den entsprechenen Felder definierte IPv4-Adresse abzustimmen.
  - **Quell-IP-Adresse**: Geben Sie die IP-Adresse ein, um dieses Kriterium anzuwenden.
  - **Quell-IP-Maske**: Geben Sie die Quell-IPv4-Maske 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.

- **Quell-Port**: Umfasst einen Quell-Port in der Abgleichbedingung für die Regel. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Select From List**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.

- **Mit Port abgleichen**: 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

- **Maske**: Die Portmaske. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 1 bedeutet, dass der Bit wichtig ist, 0 bedeutet, dass dieser Bit ignoriert werden sollte.

- **Ziel-IP**: Erfordert die Ziel-IPv6-Adresse eines Pakets, um die in den entsprechenden Feldern definierte IPv6-Adresse abzugleichen.

  - **Ziel-IP Adresse**: Geben Sie eine IPv4-Adresse an, um dieses Kriterium anzuwenden.

  - **Ziel-IP-Maske**: Geben Sie die Ziel-IP-Adressmaske ein.

- **Ziel-Port**: Wenn diese Option gewählt wird, werden die Abgleichbedingungen für die Regel um eine Ziel-Port-Bedingung erweitert. Der Ziel-Port wird im Datagramm-Header identifiziert.

  - **Select From List**: Gleicht die Zielportnummer im Datagramm-Header mit dem ausgewählten Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.

  - **Mit Port abgleichen**: Gleicht den Zielport 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

  - **Maske**: Die Portmaske. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 1 bedeutet, dass der Bit wichtig ist, 0 bedeutet, dass dieser Bit ignoriert werden sollte.

- **Servicetyp**: Gibt einen Servicetyp an, der für den Abgleich von Paketen mit Klassenkriterien verwendet werden soll.
  - **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.

    Beim IP-ToS-Maskenwert handelt es sich um eine zweistellige Hexadezimalzahl von 00 bis FF, die eine umgekehrte (d. h. Wildcard-) 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 5 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Löschen einer Klassenzuordnung wählen Sie diese in der Liste „Klassenzuordnungsname“ aus, und klicken Sie auf „Löschen“. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Konfigurieren einer IPv6-Klassenzuordnung

So fügen Sie eine IPv4-Klassenzuordnung hinzu und konfigurieren sie:

SCHRITT 1 Wählen Sie **Client-QoS > Klassenzuordnung**.

SCHRITT 2 Geben Sie im Feld „Klassenzuordnungsname“ den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

SCHRITT 3 Wählen Sie aus der Liste der ACL-Klassenzuordnungsypen „IPv6“ als ACL-Typ aus. Die IPv6-Klassenzuordnung gilt nur für IPv6-Verkehr im WAP-Gerät.

SCHRITT 4 Konfigurieren Sie im Bereich „Kriterienkonfiguration abstimmen“ diese Parameter, um die Pakete einer Klasse zuzuordnen:

- **Klassenzuordnungsname**: Wählen Sie die IPv6-Klassenzuordnung aus der Liste.
- **Übereinstimmung mit allen Paketen**: Die Übereinstimmungsbedingung gilt für alle Parameter in einem Layer-3-Paket. Wenn diese Option aktiviert ist, entsprechen alle Layer-3-Pakete der Bedingung.
- **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.
  - **Aus Liste auswählen**: Das ausgewählte Protokoll wird abgeglichen: IPv6, ICMPv6, TCP, UDP.
  - **Mit Wert abgleichen**: 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-IPv6**– Erfordert die Quell-IPv6-Adresse eines Pakets, um die in den entsprechenden Feldern definierte IPv6-Adresse abzugleichen.
  - **Quell-IPv6-Adresse**: Geben Sie die IPv6-Adresse ein, um dieses Kriterium anzuwenden.
  - **Quell-IPv6-Präfixlänge**: Geben Sie die Präfixlänge der Quell-IPv6-Adresse ein.
- **Quell-Port**: Umfasst einen Quell-Port in der Abgleichbedingung für die Regel. Der Quell-Port wird im Datagramm-Header identifiziert.

- **Select From List**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
- **Mit Port abgleichen**: 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
- **Maske**: Die Portmaske. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die hexadezimale Ziffer (0 bis 0xFFFF) ist zulässig. 1 bedeutet, dass der Bit wichtig ist, 0 bedeutet, dass dieser Bit ignoriert werden sollte.

- **Ziel-IPv6**: Erfordert die Ziel-IPv6-Adresse eines Pakets, um die in den entsprechenden Feldern definierte IPv6-Adresse abzugleichen.
  - **Ziel-IPv6-Adresse**: Geben Sie eine IPv6-Adresse ein, um dieses Kriterium anzuwenden.
  - **Quell-IPv6-Präfixlänge**: Geben Sie die Präfixlänge der Ziel-IPv6-Adresse ein.
- **Ziel-Port**: Wenn diese Option gewählt wird, werden die Abgleichbedingungen für die Regel um eine Ziel-Port-Bedingung erweitert. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Select From List**: Gleicht die Zielportnummer im Datagramm-Header mit dem ausgewählten Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Mit Port abgleichen**: Gleicht den Zielport 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

- **Maske**: Die Portmaske. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die hexadezimale Ziffer (0 bis 0xFFFF) ist zulässig. 1 bedeutet, dass der Bit wichtig ist, 0 bedeutet, dass dieser Bit ignoriert werden sollte.

- **IPv6-Flusskennzeichnung**: Geben Sie eine für ein IPv6-Paket eindeutige 20-Bit-Zahl ein. Es wird von Endgeräten verwendet, um die QoS-Behandlung in Routern zu kennzeichnen (Bereich 0 bis 1048575).
- **IP-DSCP**: Verwendet den DSCP-Wert als Abgleichkriterium.
  - **Aus Liste auswählen**: Wählen Sie den DSCP-Typ aus der Liste aus.
  - **Mit Wert abgleichen**: Geben Sie einen benutzerdefinierten DSCP-Wert von 0 bis 63 ein.

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

HINWEIS Zum Löschen einer Klassenzuordnung wählen Sie diese in der Liste „Klassenzuordnungsname“ aus, und klicken Sie auf „Löschen“. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Konfigurieren einer MAC-Klassenzuordnung

So konfigurieren Sie eine MAC-Klassenzuordnung:

SCHRITT 1 Wählen Sie **Client-QoS** > **Klassenzuordnung**.

SCHRITT 2 Geben Sie im Feld „Klassenzuordnungsname“ den Namen der neuen Klassenzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

SCHRITT 3 Wählen Sie aus der Liste der Klassenzuordnungstypen „MAC“ als Klassenzuordnungstyp aus. Die MAC-Klasse gilt für Layer 2-Kriterien.

SCHRITT 4 Konfigurieren Sie im Bereich „Kriterienkonfiguration abstimmen“ diese Parameter, um die Pakete einer Klasse zuzuordnen:

- **Klassenzuordnungsname**: Wählen Sie die MAC-Klassenzuordnung aus der Liste.
- **Übereinstimmung mit allen Paketen**: Wenn diese Option aktiviert ist, entsprechen alle Layer-2-Pakete der Bedingung.

- **Ethernettyp**: 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.
  - **Select from List**: Gleicht den Ethertype im Datagramm-Header mit den ausgewählten Protokolltypen ab: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.
  - **Mit Wert abgleichen**: 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.
- **Class of Service**: Legt einen Wert für die Class of Service-802.1p-Benutzerpriorität fest, der für die Pakete abgeglichen werden soll. Der gültige Bereich reicht von 0 bis 7.
- **Quell-MAC**: Schließt einen Quellport in die Übereinstimmungsbedingungen für die Regel ein.
  - **MAC-Quelladresse**: Geben Sie die MAC-Quelladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **MAC-Quellmaske**: 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 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 00:00:00:00:00:00 wird verwendet, um alle Adressbits zu überprüfen und eine einzelne

MAC-Adresse abzugleichen.

- **Ziel-MAC**: Schließt einen Zielport in die Übereinstimmungsbedingung für die Regel ein.
  - **Ziel-MAC-Adresse**: Geben Sie die Ziel-MAC-Adresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **Ziel-MAC-Maske**: Geben Sie die MAC-Zieladressmaske ein, um anzugeben, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.
- **VLAN-ID**: Legt die VLAN-ID fest, die für Pakete abgeglichen werden soll. Der gültige VLAN-ID-Bereich reicht von 0 bis 4095.

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

HINWEIS Zum Löschen einer Klassenzuordnung wählen Sie diese in der Liste „Klassenzuordnungsname“ aus, und klicken Sie auf „Löschen“. Eine bereits an eine Richtlinie angefügte Klassenzuordnung kann nicht gelöscht werden.

Richtlinienzuordnung

Pakete werden anhand definierter Kriterien klassifiziert und verarbeitet. Die Klassifizierungskriterien definieren Sie anhand einer Klasse auf der Seite **Klassenzuordnung**. 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 unterstützt bis zu 50 Richtlinienzuordnungen. Eine Richtlinienzuordnung kann bis zu zehn Klassenzuordnungen enthalten.

Hinzufügen und Konfigurieren einer Richtlinienzuordnung

So können Sie eine Richtlinienzuordnung hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie **Client-QoS** > **Richtlinienzuordnung**.

SCHRITT 2 Geben Sie im Feld „Richtlinienzuordnungsname“ einen Namen für die Richtlinienzuordnung ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

SCHRITT 3 Klicken Sie auf **Richtlinienzuordnung hinzufügen**.

SCHRITT 4 Konfigurieren Sie im Bereich „Richtlinienklassendefinition“ die folgenden Parameter:

- **Richtlinienzuordnungsname**: Wählen Sie die Richtlinienzuordnung aus, die Sie konfigurieren möchten.
- **Klassenzuordnungsname**: Wählen Sie die Klassenzuordnung aus, um diese Richtlinien anzuwenden.
- **Richtlinie einfach**: Legt den Traffic-Policing-Typ für die Klasse fest. Bei der einfachen Form des Policing-Typs wird eine einfache Datenrate und Burst-Größe verwendet, die zu zwei Ergebnissen führt: konform und nicht konform.

Wenn Sie diese Funktion aktivieren, konfigurieren Sie eines der folgenden Felder:

- **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 204800000 Byte.

- **Senden**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom weitergeleitet werden sollen, wenn das Klassenzuordnungskriterium erfüllt ist.
- **Löschen**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom gelöscht werden sollen, wenn das Klassenzuordnungskriterium erfüllt ist.
- **Serviceklasse 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.
- **IP-DSCP markieren**: Markiert alle Pakete für den zugeordneten Verkehrsstrom mit dem IP-DSCP-Wert, den Sie in der Liste auswählen oder angeben.
  - **Aus Liste auswählen**: Eine Liste mit DSCP-Typen
- **IP-Priorisierung 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.
- **Klassenzuordnung aufheben**: Entfernt die in der Liste „Klassenzuordnungsname“ ausgewählte Klasse aus der in der Liste „Richtlinienzuordnungsname“ ausgewählten Richtlinie.
- **Mitgliedsklassen**: Listet alle DiffServ-Klassen auf, die zurzeit als Mitglieder der ausgewählten Richtlinie definiert sind. Das Feld ist leer, wenn der Richtlinie keine Klasse zugeordnet ist.

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

HINWEIS Zum Löschen einer Richtlinienzuordnung wählen Sie diese in der Liste „Richtlinienzuordnungsname“ aus, und klicken Sie auf „Löschen“.

HINWEIS Eine Richtlinienzuordnung kann nur gelöscht werden, wenn sie keinem VAP zugewiesen ist.

HINWEIS Die Kennzeichnungsparameter für Richtlinien wie „Class of Service“, „IP-DSCP markieren“ und „IP-Priorisierung markieren“ werden für die IPV6-Klassenzuordnung nicht unterstützt.

Client-QoS-Zuordnung

Die Seite „QoS-Zuordnung“ bietet zusätzliche Kontrolle über bestimmte QoS-Aspekte der Wireless- und Ethernet-Schnittstelle. Sie ermöglicht außerdem Kontrolle über die Menge an Bandbreite, die ein einzelner Client senden und empfangen darf.

Neben der Steuerung der allgemeinen Verkehrskategorien können Sie mit QoS die Abstimmung verschiedener Mikrodatenflüsse auf einzelne Clients durch DiffServ (Differentiated Services) konfigurieren. DiffServ-Richtlinien eignen sich zum Festlegen einer allgemeinen Definition für ein- und ausgehende Mikrodatenflüsse und für Behandlungsmerkmale, die bei der Authentifizierung im Netzwerk auf die einzelnen WLAN-Clients angewendet werden können.

Konfigurieren der Parameter für die QoS-Zuordnung

So konfigurieren Sie die Parameter für die QoS-Zuordnung:

SCHRITT 1 Wählen Sie **Client-QoS** > **Client-QoS-Zuordnung**.

SCHRITT 2 Klicken Sie im Feld „Schnittstelle“ auf die Funk- oder Ethernet-Schnittstelle, auf der sie die QoS-Parameter konfigurieren möchten.

SCHRITT 3 Wählen Sie **Aktiviert** für die **ausgewählte Schnittstelle** aus.

SCHRITT 4 Konfigurieren Sie diese Parameter für die ausgewählte Schnittstelle:

- **Bandbreitenuntergrenze**: Geben Sie die maximal zulässige Übertragungsrate vom WAP-Gerät zum Client in Bit pro Sekunde (Bit/s) ein. Gültig sind Werte im Bereich von 0 bis 1300 MBit/s.
- **Bandbreitenobergrenze**: Geben Sie die maximal zulässige Übertragungsrate vom Client zum WAP-Gerät in Bit pro Sekunde (Bit/s) an. Gültig sind Werte im Bereich von 0 bis 1300 MBit/s.
- **DiffServ-Richtlinie**: Wählen Sie eine DiffServ-Richtlinie aus, die auf an das WAP-Gerät gesendeten Datenverkehr für die ausgewählte Schnittstelle angewendet werden soll.

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

Client-QoS-Status

Die Seite „Client-QoS-Status“ zeigt Details zur Richtlinienzuordnung und Klassenzuordnung an, wie beispielsweise welche Klasse eine Richtlinienzuordnunug enthält und an welche Schnittstellen diese Richtlinienzuordnung gebunden ist.

Die Tabellen „IPv4-QoS“, IPv6-QoS“ und „MAC-QoS“, zeigen Informationen zu den auf der Seite „Klassenzuordnund“ definierten Klassenzuordnungen an.

- **Mitgliedsklasse**: Der Name der Klassenzuordnung
- **Alle abgleichen**: Zeigt, ob diese Zuordnung alle Pakete abgleicht.

Regelfeld: Zeigt die detaillierte Definition dieser Klassenzuordnung an. Weitere Informationen finden Sie unter **Klassenzuordnung**.

Die Tabelle „Richtlinienzuordnung“ zeigt Informationen zu den auf der Seite „Richtlinienzuordnung“ definierten Richtlinienzuordnungen an.

- **Richtlinienzuordnungsname**: Richtlinienzuordnungsname
- **Schnittstellen-Bound**: Zeigt an, welcher Schnittstelle diese Richtlinienzuordnung zugeordnet wurde.
- **Klassenzuordnungsname**: Listet die Klassenzuordnungen auf, die diese Richtlinienzuordnung enthält.

Richtlinie: Zeigt die Richtliniendetails dieser Klassenzuordnung an. Weitere Informationen finden Sie unter **Richtlinienzuordnung**.

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

9

ACL

In diesem Abschnitt wird die Konfiguration der ACL-Funktion auf dem WAP-Gerät erläutert. Folgende Themen werden behandelt.

- **ACL-Regel**
- **ACL-Zuordnung**
- **ACL-Status**

ACL-Regel

Unter ACLs (Access Control Lists, Zugriffssteuerungslisten) versteht man eine Sammlung an Zulassungs- und Verweigerungsbedingungen, Regeln genannt, die für Sicherheit sorgen, indem unautorisierte 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-ACL-Regeln.

IPv4- und IPv6-ACLs

IP-ACLs klassifizieren Datenverkehr für die Layer 3 und 4.

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.

HINWEIS Am Ende jeder erstellten Regel gibt es eine implizite Verweigerung. Um eine allgemeine Verweigerung zu vermeiden, wird empfohlen, in der ACL eine Zulassungsregel hinzuzufügen, 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 Seite „ACL-Regel“, um die ACLs und Regeln zu konfigurieren, und wenden Sie die Regeln dann auf eine festgelegte Schnittstelle an.

Konfigurieren von ACLs

So konfigurieren Sie ACLs:

SCHRITT 1 Wählen Sie **ACL > ACL-Regel**.

SCHRITT 2 Legen Sie einen Namen für die ACL fest.

SCHRITT 3 Wählen Sie die Art von ACL, die Sie hinzufügen möchten.

SCHRITT 4 Fügen Sie die ACL hinzu.

SCHRITT 5 Fügen Sie der ACL neue Regeln hinzu.

SCHRITT 6 Konfigurieren Sie die Abgleichkriterien für die Regeln.

SCHRITT 7 Verwenden Sie die Seite „ACL-Zuordnung“, um die ACL auf eine oder mehrere Schnittstellen anzuwenden.

Konfiguration von IPv4-ACLs

Konfigurieren einer IPv4-ACL

So konfigureren Sie eine IPv4-ACL:

SCHRITT 1 Wählen Sie **ACL > ACL-Regel**.

SCHRITT 2 Geben Sie im Feld „ACL-Name“ den Namen zur Kennzeichnung der ACL ein. Der Name kann zwischen 1 und 31 alphanumerische Zeichen sowie Sonderzeichen enthalten. Leerzeichen sind nicht zulässig.

SCHRITT 3 Wählen Sie aus der Liste der ACL-Typen „IPv4“ als ACL-Typ aus. IPv4-ACLs kontrollieren den Zugriff auf Netzwerkressourcen auf der Grundlage von Layer-3- und Layer-4-Kriterien.

SCHRITT 4 Klicken Sie auf „ACL hinzufügen“.

SCHRITT 5 Konfigurieren Sie im Bereich „ACL-Regelkonfiguration“ die folgenden ACL-Regelparameter:

- **ACL Name/ACL Typ**: Wählen Sie die ACL aus, die mit der neuen Regel konfiguriert werden soll.
- **Regel**: Wählen Sie „Neue Regel“ aus, um eine neue Regel für die ausgewählte ACL zu konfigurieren. Wenn für eine ACL mehrere Regeln existieren, werden die Regeln auf das Paket oder den Frame in der Reihenfolge angewendet, in der Sie diese zur ACL hinzufügen. Als finale Regel existiert eine implizite „Alle Ablehnen“-Regel.
- **Aktion**: Wählen Sie, ob die ACL-Regel eine Aktion zulassen oder ablehnen soll.
- 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.
- **Jedes Paket abgleichen**: Ist diese Funktion aktiviert, gleicht die Regel, die entweder eine Zulassen- oder eine Verweigern-Aktion bezeichnet, den Frame oder das Paket unabhängig vom jeweiligen Inhalt ab. Wenn Sie diese Funktion aktivieren, können Sie keine zusätzlichen Abgleichkriterien konfigurieren. Bei neuen Regeln ist diese Option standardmäßig ausgewählt. Sie müssen die Option deaktivieren, um andere Abgleichfelder zu konfigurieren.
- **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. Sie können eine dieser Optionen oder „Alle“ wählen:
  - **Aus Liste auswählen**: Wählen Sie eines dieser Protokolle: IP, ICMP, IGMP, TCP oder UDP.

- **An Wert anpassen**: Geben Sie eine von IANA zugewiesene Standardprotokoll-ID von 0 bis 255 ein. Wählen Sie diese Methode aus, um ein Protokoll anzugeben, das unter „Aus Liste auswählen“ nicht aufgeführt ist.

- **Quell-IP**: Erfordert die Quell-IP-Adresse des Pakets, um die in den entsprechenden Feldern definierte Adresse abzugleichen.
  - **Quell-IP-Adresse**: Geben Sie die IP-Adresse ein, um dieses Kriterium anzuwenden.
  - **Wildcard-Maske**: Geben Sie die Wildcard-Maske der Quell-IP-Adresse ein. Die Wildcard-Maske legt fest, welche Bits verwendet und welche ignoriert werden. Eine Wildcard-Maske von 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Eine Wildcard von 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn „Quell-IP-Adresse“ aktiviert ist.

    Eine Wildcard-Maske ist im Wesentlichen das Gegenteil einer Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Wildcard-Maske von 0.0.0.0. Um die Kriterien mit einem 24-Bit-Subnetz abzugleichen (zum Beispiel 192.168.10.0/24) verwenden Sie eine Wildcard-Maske von 0.0.0.255.

- **Quell-Port**: Umfasst einen Quell-Port in der Abgleichbedingung für die Regel. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Aus Liste auswählen**: Wählen Sie das dem Quellport entsprechende Schlüsselwort aus, das abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Mit Port abgleichen**: 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
  - **Maske**: Geben Sie die Port-Maske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 0 bedeutet, dass der Bit wichtig ist, 1 bedeutet, dass dieser Bit ignoriert werden sollte.

- **Ziel-IP**: Es ist erforderlich, dass die Ziel-IP-Adresse eines Pakets der in den entsprechenden Feldern definierten Adresse entspricht.
  - **Ziel-IP Adresse**: Geben Sie eine IP-Adresse an, um dieses Kriterium anzuwenden.

    Wildcard-Maske: Geben Sie die Wildcard-Maske der Ziel-IP-Adresse ein. Die Wildcard-Maske legt fest, welche Bits verwendet und welche ignoriert werden. Eine Wildcard-Maske von 255.255.255.255 gibt an, dass alle Bits ignoriert werden. Eine Wildcard von 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn „Quell-IP-Adresse“ ausgewählt ist.

    Eine Wildcard-Maske ist im Wesentlichen das Gegenteil einer Subnetzmaske. Verwenden Sie beispielsweise zum Abgleich der Kriterien mit einer einzelnen Host-Adresse eine Wildcard-Maske von 0.0.0.0. Um die Kriterien mit einem 24-Bit-Subnetz abzugleichen (zum Beispiel 192.168.10.0/24) verwenden Sie eine Wildcard-Maske von 0.0.0.255.
- **Ziel-Port**: Wenn diese Option gewählt wird, werden die Abgleichbedingungen für die Regel um eine Ziel-Port-Bedingung erweitert. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Aus Liste auswählen**: Wählen Sie das dem Zielport entsprechende Schlüsselwort aus, das abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Jedes dieser Stichworte steht für die ihm zugeordnete Portnummer.
  - **Mit Port abgleichen**: 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
  - **Maske**: Geben Sie die Port-Maske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 0 bedeutet, dass der Bit wichtig ist, 1 bedeutet, dass dieser Bit ignoriert werden sollte.
- **Servicetyp**: Gleicht die Pakete auf der Grundlage eines speziellen Servicetyps ab.

- **IP DSCP aus Liste auswählen**: Gleicht die Pakete basierend auf deren DSCP-Werten „Assured Forwarding“ (AS), „Class of Service“ (CS) oder „Expedited Forwarding“ (EF) ab.
- **IP-DSCP mit Wert abgleichen**: 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.
- **IP-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.
- **IP-ToS-Bits**: Legt einen Wert fest, um die ToS-Bits im IP-Header eines Pakets als Abgleichkriterium zu benutzen.

  Das IP-ToS-Feld in einem Paket ist definiert als alle acht Bits des Servicetyp-Oktetts im IP-Header. Der Wert der IP-ToS-Bits ist eine zweistellige Hexadezimalzahl zwischen 00 und ff. Die höherwertigen drei Bits stellen den IP-Vorrangwert dar. Die höherwertigen sechs Bits stellen den IP-DSCP-Wert (Differentiated Service Code Point) 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.

  Beim IP-ToS-Maskenwert handelt es sich um eine zweistellige Hexadezimalzahl von 00 bis FF, die eine umgekehrte (d. h. Wildcard-) 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 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Wenn Sie eine ACL löschen möchten, stellen Sie sicher, dass sie in der ACL Name/ACL Typ-Liste ausgewählt ist, wählen Sie „ACL löschen“ und klicken Sie auf „Speichern“.

Konfiguration von IPv6-ACLs

Konfigurieren einer IPv6-ACL

So konfigurieren Sie eine IPv6-ACL:

SCHRITT 1 Wählen Sie **ACL > ACL-Regel**.

SCHRITT 2 Geben Sie im Feld „ACL-Name“ den Namen zur Kennzeichnung der ACL ein.

SCHRITT 3 Wählen Sie IPv6 als ACL-Typ aus der Liste „ACL-Typ“ aus. IPv6-ACLs kontrollieren den Zugriff auf Netzwerkressourcen auf der Grundlage von Layer-3- und Layer-4-Kriterien.

SCHRITT 4 Klicken Sie auf „ACL hinzufügen“.

SCHRITT 5 Konfigurieren Sie im Bereich „ACL-Regelkonfiguration“ die folgenden ACL-Regelparameter:

- **ACL Name/ACL Typ**: Wählen Sie die ACL aus, die mit der neuen Regel konfiguriert werden soll.
- **Regel**: Wählen Sie „Neue Regel“ aus, um eine neue Regel für die ausgewählte ACL zu konfigurieren. Wenn für eine ACL mehrere Regeln existieren, werden die Regeln auf das Paket oder den Frame in der Reihenfolge angewendet, in der Sie diese zur ACL hinzufügen. Als finale Regel existiert eine implizite „Alle Ablehnen“-Regel.
- **Aktion**: Wählen Sie, ob die ACL-Regel eine Aktion zulassen oder ablehnen soll.
- 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.
- **Jedes Paket abgleichen**: Ist diese Funktion aktiviert, gleicht die Regel, die entweder eine Zulassen- oder eine Verweigern-Aktion bezeichnet, den Frame oder das Paket unabhängig vom jeweiligen Inhalt ab. Wenn Sie diese Funktion aktivieren, können Sie keine zusätzlichen Abgleichkriterien konfigurieren. Bei neuen Regeln ist diese Option standardmäßig ausgewählt. Sie müssen die Option deaktivieren, um andere Abgleichfelder zu konfigurieren.
- **Protokoll**: Wählen Sie das Protokoll aus, das per Stichwort oder Protokoll-ID abgeglichen werden soll.

- **Quell-IPv6**– Erfordert die Quell-IPv6-Adresse eines Pakets, um die in den entsprechenden Feldern definierte IPv6-Adresse abzugleichen.
  - **Quell-IPv6-Adresse**: Geben Sie die IPv6-Adresse ein, um dieses Kriterium anzuwenden.
  - **Quell-IPv6-Präfixlänge**: Geben Sie die Präfixlänge der Quell-IPv6-Adresse ein.
- **Quell-Port**: Umfasst einen Quell-Port in der Abgleichbedingung für die Regel. Der Quell-Port wird im Datagramm-Header identifiziert.
  - **Aus Liste auswählen**: Falls ausgewählt, wählen Sie den Portnamen aus der Liste aus.
  - **Mit Port abgleichen**: 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
  - **Maske**: Geben Sie die Port-Maske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 0 bedeutet, dass der Bit wichtig ist, 1 bedeutet, dass dieser Bit ignoriert werden sollte.
- **Ziel-IPv6**: Erfordert die Ziel-IPv6-Adresse eines Pakets, um die in den entsprechenden Feldern definierte IPv6-Adresse abzugleichen.
  - **Ziel-IPv6-Adresse**: Geben Sie eine IPv6-Adresse ein, um dieses Kriterium anzuwenden.
  - **Quell-IPv6-Präfixlänge**: Geben Sie die Präfixlänge der Ziel-IPv6-Adresse ein.
- **Ziel-Port**: Wenn diese Option gewählt wird, werden die Abgleichbedingungen für die Regel um eine Ziel-Port-Bedingung erweitert. Der Ziel-Port wird im Datagramm-Header identifiziert.
  - **Aus Liste auswählen**: Falls ausgewählt, wählen Sie den Portnamen aus der Liste aus.

- **Mit Port abgleichen**: 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

- **Maske**: Geben Sie die Port-Maske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Der Wert muss hexadezimal (0 bis 0xFFFF) angegeben werden. 0 bedeutet, dass der Bit wichtig ist, 1 bedeutet, dass dieser Bit ignoriert werden sollte.

- **IPv6-Flow-Label**– Spezifiziert eine 20-Bit-Nummer, die für ein IPv6-Paket eindeutig ist. Es wird von Endgeräten verwendet, um die QoS-Behandlung in Routern zu kennzeichnen (Bereich 0 bis 1048575).

- **IPv6-DSCP**: Gleicht die Pakete basierend auf ihrem IP-DSCP-Wert ab. Ist diese Funktion ausgewählt, wählen Sie eine dieser Optionen als Abgleichkriterium aus:

  - **Aus Liste auswählen**: Wählen Sie einen dieser Werte aus: DSCP Assured Forwarding (AS), Class of Service (CS) oder Expedited Forwarding (EF).

  - **Mit Wert abgleichen**: Geben Sie einen benutzerdefinierten DSCP-Wert von 0 bis 63 ein.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Wenn Sie eine ACL löschen möchten, stellen Sie sicher, dass sie in der Liste ACL-Name/ACL-Typ- ausgewählt ist, aktivieren Sie „ACL löschen“ und klicken Sie auf „Speichern“.

Konfiguration von MAC-ACLs

Konfigurieren von MAC-ACLs

So konfigurieren Sie eine MAC-ACL:

SCHRITT 1 Wählen Sie **ACL > ACL-Regel**.

SCHRITT 2 Geben Sie im Feld „ACL-Name“ den Namen zur Kennzeichnung der ACL ein.

SCHRITT 3 Wählen Sie MAC als ACL-Typ aus der Liste „ACL-Typ“ aus. MAC-ACLs kontrollieren Zugriff auf der Grundlage von Layer-2-Kriterien.

SCHRITT 4 Klicken Sie auf „ACL hinzufügen“.

SCHRITT 5 Konfigurieren Sie im Bereich „ACL-Regelkonfiguration“ die folgenden ACL-Regelparameter:

- **ACL Name/ACL Typ**: Wählen Sie die ACL aus, die mit der neuen Regel konfiguriert werden soll.
- **Regel**: Wählen Sie „Neue Regel“ aus, um eine neue Regel für die ausgewählte ACL zu konfigurieren. Wenn für eine ACL mehrere Regeln existieren, werden die Regeln auf das Paket oder den Frame in der Reihenfolge angewendet, in der Sie diese zur ACL hinzufügen. Als finale Regel existiert eine implizite „Alle Ablehnen“-Regel.
- **Aktion**: Wählen Sie, ob die ACL-Regel eine Aktion zulassen oder ablehnen soll.
- 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.
- **Jedes Paket abgleichen**: Ist diese Funktion aktiviert, gleicht die Regel, die entweder eine Zulassen- oder eine Verweigern-Aktion bezeichnet, den Frame oder das Paket unabhängig vom jeweiligen Inhalt ab. Wenn Sie diese Funktion aktivieren, können Sie keine zusätzlichen Abgleichkriterien konfigurieren. Bei neuen Regeln ist diese Option standardmäßig ausgewählt. Sie müssen die Option deaktivieren, um andere Abgleichfelder zu konfigurieren.
- **EtherType**: Wählen Sie dies aus, um die Abgleichkriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Sie können entweder ein EtherType-Stichwort auswählen oder einen EtherType-Wert eingeben, um die Abgleichkriterien festzulegen.
  - **Aus Liste auswählen**: Wählen Sie einen dieser Protokolltypen aus: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.

- **Abgleichwert**: Geben Sie einen Protokoll-Identifikator ein, mit dem Pakete abgeglichen werden sollen. Der Wert ist eine vierstellige Hexadezimalzahl im Bereich zwischen 0600 und FFFF.

- **Class of Service**: Geben Sie eine 802.1p-Benutzerpriorität ein, die mit einem Ethernet-Frame verglichen werden soll. Gültig sind Werte im Bereich von 0 bis 7. Dieses Feld befindet sich im ersten bzw. einzigen 802.1Q-VLAN-Tag.
- **Source MAC**: Erfordert die Quell-MAC-Adresse des Pakets, um die in den entsprechenden Feldern definierte Adresse abzugleichen.
  - **MAC-Quelladresse**: Geben Sie die MAC-Quelladresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **Quell-MAC-Maske**: Geben Sie die Quell-MAC-Adresse 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.
- **Ziel-MAC**: Erfordert die Ziel-MAC-Adresse des Pakets, um die in den entsprechenden Feldern definierte Adresse abzugleichen.
  - **Ziel-MAC-Adresse**: Geben Sie die Ziel-MAC-Adresse ein, die mit einem Ethernet-Frame verglichen werden soll.
  - **Ziel-MAC-Maske**: Geben Sie die Ziel-MAC-Adresse ein, um festzulegen, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.
- **VLAN-ID**: 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.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Wenn Sie eine ACL löschen möchten, stellen Sie sicher, dass sie in der Liste ACL-Name/ACL-Typ- ausgewählt ist, aktivieren Sie „ACL löschen“ und klicken Sie auf „Speichern“.

ACL-Zuordnung

Die Seite „ACL-Zuordnung“ stellt die ACL-Liste für die Wireless- und Ethernet-Schnittstellen bereit. Um allgemeine Datenverkehrskategorien zu kontrollieren, wie beispielsweise HTTP-Datenverkehr oder Verkehr aus einem spezifischen Subnetz, können Sie ACLs konfigurieren und sie einer oder mehreren Schnittstellen zuweisen.

Zuordnung einer ACL zu einer Schnittstelle

So ordnen Sie eine ACL einer Schnittstelle zu:

SCHRITT 1 Wählen Sie **ACL > ACL-Zuordnung**.

SCHRITT 2 Klicken Sie im Feld „Schnittstelle“ auf die Funk- oder Ethernet-Schnittstelle, auf der sie die ACL-Parameter konfigurieren möchten.

SCHRITT 3 Konfigurieren Sie diese Parameter für die ausgewählte Schnittstelle:

- **ACL-Typ**: Wählen Sie den ACL-Typ aus, der auf beim WAP-Gerät eingehenden Datenverkehr angewendet wird. Dabei kann es sich um eine dieser Optionen handeln:
  - **IPv4**: Untersucht die IPv4-Pakete, die den ACL-Regeln entsprechen.
  - **IPv6**: Untersucht die IPv6-Pakete, die den ACL-Regeln entsprechen.
  - **MAC**: Untersucht die Layer-2-Frames, die den ACL-Regeln entsprechen.
  - **Keine**: Der Datenverkehr, der beim WAP-Gerät eingeht, wird nicht untersucht.
- **ACL-Name**: Wählen Sie den Name der ACL aus, die auf beim WAP-Gerät eingehenden Datenverkehr angewendet wird.

  Wenn ein Paket oder ein Frame vom WAP-Gerät empfangen wird, werden die ACL-Regeln auf eine Übereinstimmung überprüft. Falls das Paket oder der Frame zugelassen werden, werden sie verarbeitet, andernfalls verworfen.

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

ACL-Status

Auf der Seite „ACL-Status“ werden die Details für verschiedene Arten von ACL-Regeln angezeigt.

Um den ACL-Status anzuzeigen, wählen Sie „ACL > ACL-Status“ aus.

Die folgenden Informationen werden angezeigt:

- **ACL-Name**: Der Name der ACL.
- **Verbundene Schnittstelle**: Die Schnittstelle, der die ACL zugordnet wurde.
- **Regelnummer**: Die Nummer der Regel, die die ACL enthält.
- **Aktion**: Die Aktion, die von der ACL vorgenommen wird.
- **Alle abgleichen**: Zeigt, ob die ACL-Regel allen Paketen entspricht.

Regelfeld: Zeigt die detaillierten Einstellungen für die ACL an. Weitere Informationen finden Sie unter **ACL-Regel**.

Sie können auf **Aktualisieren** klicken, um die Bildschirmanzeige mit den neuesten Daten zu aktualisieren.

10

SNMP

In diesem Abschnitt wird beschrieben, wie Sie das SNMP-Protokoll (Simple Network Management Protocol) konfigurieren, um Konfigurationen vorzunehmen und Statistiken zu sammeln.

Folgende Themen werden behandelt:

- **Allgemein**
- **Ansichten**
- **Gruppen**
- **Benutzer**
- **Ziele**

Allgemein

Auf der Seite „General“ können Sie SNMP aktivieren und grundlegende Protokolleinstellungen konfigurieren.

So konfigurieren Sie allgemeine SNMP-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich **SNMP** > **Allgemein** aus.

SCHRITT 2 Wählen Sie **Aktivieren** für die **SNMP**-Einstellung aus. SNMP ist standardmäßig deaktiviert.

SCHRITT 3 Legen Sie einen **UDP-Port** für SNMP-Datenverkehr fest.

Standardmäßig hört ein SNMP-Agent nur Anfragen von Port 161 mit. Sie können diese Funktion jedoch so konfigurieren, dass der Agent Anfragen an einem anderen Port mithört. Der gültige Bereich reicht von 1025 bis 65535.

SCHRITT 4 Konfigurieren Sie die folgenden SNMPv2-Einstellungen:

- **Schreibgeschützte Community**: Ein schreibgeschützter Community-Name für SNMPv2-Zugriff. Gültig sind Werte mit 1 bis 256 alphanumerischen Zeichen und Sonderzeichen.

  Der Community-Name dient als einfache Authentifizierungsfunktion zum Beschränken der Computer 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**: Ein Lesen/Schreiben-Community-Name, der für Anfragen nach SNMP-Sätze verwendet wird. Der gülitge 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 der folgenden Optionen aus:

  - **Alle**: Die Menge der Stationen, die über SNMP auf das WAP-Gerät zugreifen können, ist nicht eingeschränkt.

  - **Benutzerdefiniert**: Die Menge der zugelassenen SNMP-Anfragen ist auf die festgelegten beschränkt.

- **NMS-IPv4-Adresse/-Name**: Die IPv4-IP-Adresse, der DNS-Hostname, das Subnetz des Netzwerkverwaltungssystems (Network Management System, NMS) oder die Gruppe der Computer, die GET- und SET-Anfragen an die verwalteten Geräte ausführen können.

  Ein DNS-Hostname kann aus mindestens einem Label, das heißt einer Gruppe aus bis zu 63 alphanumerischen Zeichen, bestehen. Wenn ein Hostname mehrere Labels enthält, werden die einzelnen Beschriftungen 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 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 *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.

Mit dem Adressbereich geben Sie das Subnetz des festgelegten NMS an. Nur Computer mit IP-Adressen aus diesem Bereich können GET- und SET-Anfragen für das verwaltete Gerät ausführen. Im oben gezeigten Beispiel können Computer mit den Adressen 192.168.1.1 bis 192.168.1.254 SNMP-Befehle für das Gerät ausführen. (Die durch das Suffix .0 identifizierte Adresse in einem Subnetzbereich ist immer für die Subnetz-Adresse reserviert, und die durch .255 identifizierte Adresse im Bereich ist immer für die Broadcast-Adresse reserviert.)

Ein weiteres Beispiel: Wenn Sie den Bereich „10.10.1.128/25“ eingeben, können Computer mit den IP-Adressen 10.10.1.129 bis 10.10.1.254 SNMP-Anfragen für verwaltete Geräte ausführen. In diesem Beispiel ist 10.10.1.128 die Netzwerkadresse und 10.10.1.255 die Broadcast-Adresse. Insgesamt werden 126 Adressen festgelegt.

- **NMS-IPv6-Adresse/-Name**: Die IPv6-Adresse, der DNS-Hostname oder das Subnetz der Computer, 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.

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

SCHRITT 5 Konfigurieren Sie die folgenden SNMPv2-Trap-Einstellungen:

- **Trap-Community** – Ein globaler Community-String, der mit SNMP-Traps verbunden ist. Vom Gerät gesendete Traps stellen diese Zeichenfolge als Community-Namen bereit. Der gülitge Bereich liegt zwischen 1 und 60 und kann alphanumerische Zeichen sowie Sonderzeichen enthalten.
- **Trap-Ziel-Tabelle**: Eine Liste mit bis zu drei IP-Adressen oder Hostnamen, die SNMP-Traps empfangen sollen. Aktivieren Sie das Kästchen und wählen Sie einen **Host-IP-Adresstyp** (IPv4 oder IPv6), bevor Sie die **Hostname-/IP-Adresse** hinzufügen.

  Ein Beispiel für einen DNS-Hostnamen ist „snmptraps.foo.com“. Da 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-Adresstyp** auswählen.

Beachten Sie außerdem den Hinweis zu Hostnamen im vorherigen Schritt.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Nachdem neue Einstellungen gespeichert wurden, können die zugehörigen Prozesse gestoppt und neu gestartet werden. Tritt dieser Fall ein, verliert das WAP-Gerät möglicherweise die Anbindung. Es wird empfohlen, die Einstellungen des WAP-Geräts dann zu ändern, wenn Ihre Wireless-Clients am wenigsten davon betroffen sind.

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 AP unterstützt maximal 16 Ansichten.

In diesen Hinweisen werden wichtige Richtlinien zur Konfiguration von SNMPv3-Ansichten zusammengefasst. 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.

So können Sie eine SNMP-Ansicht hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich **SNMP** > **Ansichten** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle „SNMPv3-Ansichten“ zu erstellen.

SCHRITT 3 Aktivieren Sie das Kästchen in der neuen Zeile und klicken Sie 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 .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 4 Klicken Sie auf **Speichern**. Die Ansicht wird der Liste „SNMPv3-Ansichten“ hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

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

Gruppen

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

Der AP verfügt standardmäßig über zwei Gruppen:

- **RO**: Eine nur über Lesezugriff verfügende Gruppe mit Authentifizierung und Datenverschlüsselung. Benutzer in dieser Gruppe verwenden einen MD5-Schlüssel bzw. ein MD5-Kennwort für die Authentifizierung und einen DES-Schlüssel bzw. ein DES-Kennwort für die Verschlüsselung. Die MD5- und DES-Schlüssel bzw. -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 einen MD5-Schlüssel bzw. ein MD5-Kennwort für die Authentifizierung und einen DES-Schlüssel bzw. ein DES-Kennwort für die Verschlüsselung. Die MD5- und DES-Schlüssel bzw. -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.

HINWEIS Der AP unterstützt maximal 8 Gruppen.

So können Sie eine SNMP-Gruppe hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich **SNMP** > **Gruppen** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle „SNMPv3-Gruppen“ zu erstellen.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen für die neue Gruppe und klicken Sie auf **Bearbeiten**:

SCHRITT 4 Konfigurieren Sie die Parameter:

- **Gruppenname**: Ein Name zur Identifizierung der Gruppe. Die Standardgruppennamen lauten „RO“ und „RW“.

  Gruppennamen können bis zu 32 alphanumerische Zeichen enthalten.

- **Sicherheitsstufe**: Legt die Sicherheitsstufe für die Gruppe fest. Die folgenden Optionen stehen zur Verfügung:

  - **noAuthentication-noPrivacy**: Keine Authentifizierung und keine Datenverschlüsselung (keine Sicherheit)

- **Authentication-noPrivacy**: Authentifizierung, aber keine Datenverschlüsselung. Benutzer dieser Sicherheitsstufe senden SNMP-Nachrichten mit einem MD5-Schlüssel bzw. -Kennwort für die Authentifizierung, jedoch keinen DES-Schlüssel bzw. kein DES-Kennwort für die Verschlüsselung.
- **Authentication-Privacy**: Authentifizierung und Datenverschlüsselung. Benutzer dieser Sicherheitsstufe senden einen MD5-Schlüssel bzw. ein MD5-Kennwort für die Authentifizierung und einen DES-Schlüssel bzw. ein DES-Kennwort für die Verschlüsselung.

  Für Gruppen, bei denen Authentifizierung und/oder Verschlüsselung erforderlich ist, müssen Sie die MD5- und DES-Schlüssel bzw. -Kennwörter auf der Seite „SNMP Users“ definieren.

- **Schreibansichten**: Der Schreibzugriff der Gruppe auf MIBs. Die folgenden Optionen stehen zur Verfügung:
  - **view-all:**: Die Gruppe kann MIBs erstellen, ändern und löschen.
  - **view-none:**: Die Gruppe kann MIBs nicht erstellen, ändern oder löschen.
- **Leseansichten**: Der Lesezugriff der Gruppe auf MIBs:
  - **view-all:**: Die Gruppe kann alle MIBs anzeigen und lesen.
  - **view-none:**: Die Gruppe kann MIBs nicht anzeigen oder lesen.

SCHRITT 5 Klicken Sie auf **Speichern**. Die Gruppe wird der Liste „SNMPv3-Gruppen“ hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Entfernen einer Gruppe wählen Sie die Gruppe in der Liste aus, und klicken Sie auf **Löschen**.

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 MD5 unterstützt. Für die Verschlüsselung wird nur der Typ DES unterstützt. Es gibt im AP keine SNMPv3-Standardbenutzer. Sie können bis zu acht Benutzer hinzufügen.

So fügen Sie SNMP-Benutzer hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich **SNMP** > **Benutzer** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle „SNMPv3-Benutzer“ zu erstellen.

SCHRITT 3 Aktivieren Sie das Kästchen in der neuen Zeile und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die Parameter:

- **Benutzername** – Ein Name, der den SNMPv3-Benutzer identifiziert. Benutzernamen können bis zu 32 alphanumerische Zeichen enthalten.
- **Gruppe** – Die Gruppe, der der Benutzer zugeordnet ist. Die Standardgruppen lauten RW und RO. Auf der Seite „SNMP Groups“ können Sie zusätzliche Gruppen definieren.
- **Authentifizierungstyp**: Der Typ der Authentifizierung, die für SNMPv3-Anfragen des Benutzers verwendet werden soll. Die folgenden Optionen stehen zur Verfügung:
  - **MD5**: Für SNMP-Anfragen des Benutzers ist MD5-Authentifizierung erforderlich.
  - **Keine** : Für SNMPv3-Anfragen des Benutzers ist keine Authentifizierung erforderlich.
- **Authentifizierungskennwort**: (Wenn Sie den Authentifizierungstyp MD5 angegeben haben): Ein Kennwort, mit dem der SNMP-Agent vom Benutzer gesendete Anfragen authentifizieren kann. Die Passphrase muss zwischen 8 und 32 Zeichen lang sein.

- **Verschlüsselungstyp**: Der Typ des Datenschutzes, der für SNMP-Anfragen des Benutzers verwendet werden soll. Die folgenden Optionen stehen zur Verfügung:
  - **DES**: Für SNMPv3-Anfragen des Benutzers wird DES-Verschlüsselung verwendet.
  - **Keine**: Für SNMPv3-Anfragen des Benutzers ist kein Datenschutz erforderlich.
- **Verschlüsselungskennwort**: (Wenn Sie den Datenschutztyp DES angegeben haben): Ein Kennwort, das zum Verschlüsseln der SNMP-Anfragen verwendet werden soll. Die Passphrase muss zwischen 8 und 32 Zeichen lang sein.

SCHRITT 5 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**.

Ziele

SNMPv3-Ziele senden SNMP-Benachrichtigungen als Inform-Nachrichten an den SNMP-Manager. Für SNMPv3-Ziele werden nur Inform-Nachrichten gesendet, keine Traps. Für die SNMP-Versionen1 und 2 werden Traps gesendet. Jedes Ziel wird durch eine IP-Zieladresse, einen UDP-Port und einen SNMPv3-Benutzernamen definiert.

HINWEIS Bevor Sie SNMPv3-Ziele konfigurieren, müssen Sie die SNMPv3-Benutzerkonfiguration (siehe Seite **Benutzer**) abschließen.

HINWEIS Der AP unterstützt maximal acht Ziele.

So fügen Sie SNMP-Ziele hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich **SNMP** > **Ziel** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. In der Tabelle wird eine neue Zeile erstellt.

SCHRITT 3 Aktivieren Sie das Kästchen in der neuen Zeile und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die Parameter:

- **IP-Adresse**: Geben Sie die IPv4-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 **Benutzer**.

SCHRITT 5 Klicken Sie auf **Speichern**. Der Benutzer wird der Liste „SNMPv3-Ziele“ hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Um ein SNMP-Ziel zu entfernen, wählen Sie den Benutzer in der Liste aus und klicken Sie auf **Löschen**.

11

Captive Portal

In diesem Abschnitt wird die Captive Portal-Funktion (CP) beschrieben, mit der Sie verhindern können, dass WLAN-Clients auf das Netzwerk zugreifen, solange die Überprüfung des Benutzers nicht durchgeführt wurde. Sie können die CP-Überprüfung konfigurieren, um den Zugriff für Gastbenutzer und authentifizierte Benutzer zuzulassen.

Authentifizierte Benutzer müssen anhand einer Datenbank der autorisierten CP-Gruppen oder -Benutzer überprüft werden, bevor der Zugriff gewährt wird. Die Datenbank kann lokal im WAP-Gerät oder auf einem RADIUS-Server gespeichert sein.

Das Captive Portal besteht aus zwei CP-Instanzen. Die einzelnen Instanzen können unabhängig voneinander mit unterschiedlichen Überprüfungsmethoden für die einzelnen VAPs oder SSIDs konfiguriert werden. Die Cisco WAP571/E-Geräte werden gleichzeitig mit einigen für die CP-Authentifizierung konfigurierten VAPs und einigen für normale WLAN-Authentifizierungsverfahren wie beispielsweise WPA oder WPA Enterprise betrieben.

Dieser Abschnitt enthält die folgenden Themen:

- **Globale Konfiguration**
- **Lokale Gruppen/Benutzer**
- **Instanzkonfiguration**
- **Instanzzuordnung**
- **Anpassung des Webportals**
- **Authentifizierte Clients**

Globale Konfiguration

Auf der Seite „Globale CP-Konfiguration“ können Sie den administrativen Status der Captive Portal-Funktion steuern und globale Einstellungen konfigurieren, die sich auf alle im WAP-Gerät konfigurierten CP-Instanzen auswirken.

Konfigurieren der globalen CP-Einstellungen

So konfigurieren Sie globale CP-Einstellungen:

SCHRITT 1 Wählen Sie **Globale >Captive Portal-Konfiguration**.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Captive Portal-Modus**: Aktiviert oder deaktiviert den CP-Betrieb im WAP-Gerät.
- **Authentifizierungstimeout**: Beim Zugriff auf das Netzwerk über ein Portal muss der Client zuerst auf einer Authentifizierungswebseite die Authentifizierungsinformationen eingeben. Dieses Feld gibt an, wie viele Sekunden lang eine Authentifizierungssitzung mit dem zugeordneten WLAN-Client im WAP-Gerät geöffnet bleibt. Wenn der Client nicht innerhalb des zulässigen Timeout-Zeitraums die Anmeldeinformationen zur Authentifizierung eingibt, muss der Client möglicherweise die Authentifizierungswebseite aktualisieren. Der Standardwert für das Authentifizierungs-Timeout beträgt 300 Sekunden. Möglich sind Werte im Bereich von 60 bis 600 Sekunden.
- **Zusätzlicher HTTP-Port**: Für HTTP-Verkehr wird der HTTP-Verwaltungsport verwendet, der standardmäßig auf „80“festgelegt ist. Sie können einen zusätzlichen Port für HTTP-Verkehr konfigurieren. Geben Sie eine Port-Nummer zwischen 1025 und 65535 oder „80“ ein. Der HTTP-Port und der HTTPS-Port können nicht identisch sein.
- **Zusätzlicher HTTP-Port**: Für HTTP-Verkehr über SSL (HTTPS) wird der HTTPS-Verwaltungsport verwendet, der standardmäßig auf „443“ festgelegt ist. Sie können einen zusätzlichen Port für HTTPS-Verkehr konfigurieren. Geben Sie eine Portnummer zwischen 1025 und 65535 oder „443“ ein. Der HTTP-Port und der HTTPS-Port können nicht identisch sein.

SCHRITT 3 Im Bereich „Captive Portal-Konfigurationszähler“ werden schreibgeschützte CP-Informationen angezeigt:

- **Instanzenzähler**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Instanzen. Es können maximal zwei Instanzen konfiguriert sein.
- **Gruppenzähler**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Gruppen. Es können maximal zwei Gruppen konfiguriert sein. Die Gruppe „Standard“ ist standardmäßig vorhanden und kann nicht gelöscht werden.
- **Benutzerzähler**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Benutzer. Es können maximal 128 Benutzer konfiguriert sein.

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

Lokale Gruppen/Benutzer

Verwenden Sie die Seite „Lokale Gruppen/Benutzer“, um lokale Gruppen und Benutzer zu verwalten.

Local Groups

Jeder lokale Benutzer wird einer Benutzergruppe zugewiesen. Jeder Gruppe wird eine CP-Instanz zugewiesen. Die Gruppe erleichtert das Verwalten der Zuordnung von Benutzern zu CP-Instanzen.

Die integrierte Benutzergruppe „Standard“ kann nicht gelöscht werden. Sie können bis zu zwei zusätzliche Benutzergruppen erstellen.

So fügen Sie eine lokale Benutzergruppe hinzu:

SCHRITT 1 Wählen Sie **Captive Portal > Lokale Gruppen/Benutzer** aus.

SCHRITT 2 Konfigurieren Sie im Bereich „Lokale Gruppeneinstellungen“ die folgenden Parameter:

- **Captive Portal-Gruppen**: Wählen Sie „Erstellen“, um eine neue Gruppe zu erstellen.
- **Gruppenname**: Geben Sie einen Namen für die neue Gruppe ein.

SCHRITT 3 Klicken Sie auf **Gruppe hinzufügen**. Die Änderungen werden in der Startkonfiguration gespeichert.

So löschen Sie eine lokale Benutzergruppe:

SCHRITT 1 Wählen Sie **Captive Portal > Lokale Gruppen/Benutzer** aus.

SCHRITT 2 Wählen Sie im Bereich „Lokale Gruppeneinstellungen“ die Gruppe, die Sie löschen möchten.

SCHRITT 3 Aktivieren Sie die Option „Gruppe löschen“.

SCHRITT 4 Klicken Sie auf **Gruppe löschen**. Die Änderungen werden in der Startkonfiguration gespeichert.

Local Users

Sie können eine CP-Instanz so konfigurieren, dass sie Gastbenutzer oder autorisierte Benutzer enthält. Gastbenutzer haben keine zugewiesenen Benutzernamen und Kennwörter.

Autorisierte Benutzer geben einen gültigen Benutzernamen und ein gültiges Kennwort an, das zuerst anhand einer lokalen Datenbank oder eines RADIUS-Servers überprüft werden muss. Autorisierte Benutzer werden in der Regel einer CP-Instanz zugewiesen, die einem anderen VAP zugeordnet ist als die Gastbenutzer.

Auf der Seite „Lokale Benutzer“ können Sie bis zu 128 autorisierte Benutzer in der lokalen Datenbank konfigurieren.

So können Sie einen lokalen Benutzer hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie **Captive Portal** > **Lokale Gruppen/Benutzer** aus.

SCHRITT 2 Konfigurieren Sie im Bereich „Lokale Benutzereinstellungen“ die folgenden Parameter:

- **Captive Portal-Benutzer**: Wählen Sie „Erstellen“, um einen neuen Benutzer zu erstellen.
- **Benutzername**: Geben Sie den Namen des neuen Benutzers ein.

SCHRITT 3 Klicken Sie auf „Benutzer hinzufügen“.

SCHRITT 4 Der Bereich „Lokale Benutzereinstellungen“ wird mit zusätzliche Optionen angezeigt. Konfigurieren Sie die folgenden Parameter:

- **Benutzerkennwort**: Geben Sie das Kennwort ein (8 bis 64 alphanumerische Zeichen und Sonderzeichen). Benutzer müssen das Kennwort eingeben, um sich über das Captive Portal beim Netzwerk anzumelden.
- **Kennwort 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.
- **Löschungstimeout**: Gibt an, wie lange ein Benutzer in der Liste der authentifizierten CP-Clients bleibt, nachdem die Zuordnung zum AP 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 Captive Portal-Instanz konfigurierten Wert, sofern der Benutzerwert nicht auf „0“ festgelegt ist. Wenn der Wert auf „0“ festgelegt ist, wird der für die CP-Instanz konfigurierte Timeout-Wert verwendet.
- **Gruppenname**: Wählen Sie die zugeordnete Benutzergruppe. Jede CP-Instanz ist für die Unterstützung einer bestimmten Benutzergruppe konfiguriert.
- **Maximale Upstream-Bandbreite**: Geben Sie die maximale Upload-Geschwindigkeit in Megabit pro Sekunde ein, mit der ein Client bei Verwendung des Captive Portals Verkehr senden kann. Diese Einstellung begrenzt die Bandbreite, mit der Daten an das Netzwerk gesendet werden. Möglich sind Werte im Bereich von 0 bis 1.300 MBit/s. Die Standardeinstellung ist 0.
- **Maximale Downstream-Bandbreite**: Geben Sie die maximale Download-Geschwindigkeit in Megabit pro Sekunde ein, mit der ein Client bei Verwendung des Captive Portals Verkehr empfangen kann. Diese Einstellung begrenzt die Bandbreite, mit der Daten vom Netzwerk empfangen werden. Möglich sind Werte im Bereich von 0 bis 1.300 MBit/s. Die Standardeinstellung ist 0.

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

So löschen Sie einen lokalen Benutzer:

SCHRITT 1 Wählen Sie **Captive Portal > Lokale Gruppen/Benutzer** aus.

SCHRITT 2 Wählen Sie im Bereich „Lokale Benutzereinstellungen“ den Benutzer aus, den Sie löschen möchten.

SCHRITT 3 Aktivieren Sie die Option „Benutzer löschen“.

SCHRITT 4 Klicken Sie auf **Benutzer löschen**. Die Änderungen werden in der Startkonfiguration gespeichert.

Instanzkonfiguration

Sie können maximal zwei CP-Instanzen erstellen. Jede CP-Instanz stellt einen definierten Satz von Instanzparametern dar. Instanzen können einem oder mehreren VAPs zugeordnet sein. Sie können verschiedene Instanzen konfigurieren, um unterschiedlich auf Benutzer zu reagieren, die auf den zugeordneten VAP zuzugreifen versuchen.

HINWEIS Überprüfen Sie vor dem Erstellen einer Instanz die folgenden Punkte:

- Möchten Sie einen neuen VAP hinzufügen? Wenn ja, rufen Sie die Seite **Netzwerke** auf, um einen VAP hinzuzufügen.

Möchten Sie eine neuen Gruppe oder einen neuen Benutzer hinzufügen? Wenn ja, rufen Sie die Seite **Lokale Gruppen/Benutzer** auf, um einen Benutzer hinzuzufügen.

So erstellen Sie eine CP-Instanz und konfigurieren die Einstellungen:

So erstellen Sie eine CP-Instanz und konfigurieren die Einstellungen:

SCHRITT 1 Wählen Sie **Captive Portal** > **Instanzkonfiguration aus**.

SCHRITT 2 Stellen Sie sicher, dass in der Liste **Captive Portal-Instanzen Erstellen** ausgewählt ist.

SCHRITT 3 Geben Sie im Feld „Instanzname“ den Namen für die CP-Instanz ein (1 bis 32 alphanumerischen Zeichen)

SCHRITT 4 Klicken Sie auf **Speichern**.

SCHRITT 5 Daraufhin wird der Bereich „Captive Portal-Instanzparameter“ mit zusätzlichen Optionen erneut angezeigt. Konfigurieren Sie die folgenden Parameter:

- **Instanz-ID**: Zeigt die Instanz-ID an. Dieses Feld kann nicht konfiguriert werden.
- **Administrativer Modus**: Aktiviert und deaktiviert die CP-Instanz.
- **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.
- **Verifizierung**: Wählen Sie das Authentifizierungsverfahren, das vom CP zum Überprüfen von Clients verwendet wird:
  - **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.
  - **Active Directory-Server**: Das WAP-Gerät führt mittels SSL/TLS über den Befehl `starttls` eine sichere LDAP-Verbindung durch, um die Benutzer mit ihrem sAMAccountName-Attribut in Active Directory zu authentifizieren.
  - **Anmeldedaten von Dritten**: Das WAP-Gerät kann Benutzer anhand von Facebook- oder Google-Konten authentifizieren.
- **Social Login-Methode**: Das WAP-Gerät ist mittels des OAuth-Protokolls in der Lage, Benutzer anhand von Facebook- oder Google-Konten zu authentifizieren.
  - **Facebook**: Aktiviert und deaktiviert den Social Login für die Verwendung des Facebook-Kontos zum Authentifizieren der Clients.
  - **Google**: Aktiviert und deaktiviert den Social Login für die Verwendung des Google-Kontos zum Authentifizieren der Clients.
- **Active Directory Server Host1**: Fügen Sie einen Server hinzu und geben Sie die IP-Adresse des Domänencontrollers ein.
- **Active Directory Server Host2**: Fügen Sie einen Server hinzu und geben Sie die IP-Adresse des Domänencontrollers ein.

- **Active Directory Server Host3**: Fügen Sie einen Server hinzu und geben Sie die IP-Adresse des Domänencontrollers ein.

HINWEIS

- Es können mehrere Server hinzugefügt werden. Der AP führt Tests gegen diese Server in der vorgegebenen Reihenfolge von Host1 bis Host3 durch.

- **Walled Garden-Bereich**: Legen Sie eine Liste von Domänen fest, auf die Benutzer zugreifen können, bevor sie auf die Seite des Webportals gelangen. Die Einträge in dieser Liste müssen durch Kommata voneinander getrennt werden und die Domänen können Platzhalter in Form eines Asterisks (*) beinhalten.

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

- Wenn die Anmeldung mit Facebook oder Google aktiviert ist, wird die Walled Garden-Funktion automatisch aktiviert und fügt die folgenden Domänen zur Liste für die Authentifizierung hinzu. Die Domänenliste kann von Facebook oder Google geändert werden und ist ggf. nicht auf dem aktuellsten Stand. Sie können die Domänen manuell hinzufügen.
  - **Facebook**: *.facebook.com, *.facebook.net, *.fbcdn.net
  - **Google**: *.googleapis.com, apis.google.com, accounts.google.com, *.googleusercontent.com, ssl.gstatic.com, fonts.gstatic.com
  - **Windows 10**: ww.msftconnecttest.com

- **Umleiten**: Sofern aktiviert. Das Captive Portal soll den neu authentifizierten Client an die konfigurierte URL umleiten. Wenn diese Option deaktiviert ist, sehen die Benutzer nach der erfolgreichen Überprüfung die gebietsschemaspezifische Willkommensseite.

- **URL umleiten**: Geben Sie die URL (einschließlich http://) ein, an die der neu authentifizierte Client umgeleitet wird, wenn der URL-Umleitungsmodus aktiviert ist. Möglich sind Werte im Bereich von 0 bis 256 Zeichen.

- **Löschungstimeout**: Geben Sie an, wie lange ein Benutzer in der Liste der authentifizierten CP-Clients bleibt, nachdem die Zuordnung zum AP 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 Minuten“.

Außerdem wird für jeden Benutzer ein Timeout-Wert bei Abwesenheit konfiguriert. Weitere Informationen finden Sie auf der Seite: **Lokale Gruppen/Benutzer**. Der auf der Seite „Local Users“ festgelegte Timeout-Wert bei Abwesenheit hat Vorrang vor dem hier konfigurierten Wert, es sei denn, der Wert ist auf „0“ (Standard) festgelegt. Der Wert „0“ gibt an, dass der Timeout-Wert für die Instanz verwendet werden soll.

- **Sitzungstimeout**: Geben Sie die in Sekunden verbleibende Zeit ein, während der die CP-Sitzung gültig ist. Wenn Null erreicht ist, wird der Client deauthentifiziert. Möglich sind Werte im Bereich von 0 bis 1440 Minuten. Der Standardwert lautet „0“.
- **Maximale Upstream-Bandbreite**: Geben Sie die maximale Upload-Geschwindigkeit in Megabit pro Sekunde ein, mit der ein Client bei Verwendung des Captive Portals Verkehr senden kann. Diese Einstellung begrenzt die Bandbreite, mit der der Client Daten an das Netzwerk senden kann. Möglich sind Werte im Bereich von 0 bis 1.300 MBit/s. Der Standardwert lautet „0“.
- **Maximale Downstream-Bandbreite**: Geben Sie die maximale Download-Geschwindigkeit in Megabit pro Sekunde ein, mit der ein Client bei Verwendung des Captive Portals Verkehr empfangen kann. Diese Einstellung begrenzt die Bandbreite, mit der der Client Daten vom Netzwerk empfangen kann. Möglich sind Werte im Bereich von 0 bis 1.300 MBit/s. Der Standardwert lautet „0“.
- **Benutzergruppenname**: Wenn der Überprüfungsmodus „Local“ oder „RADIUS“ festgelegt ist, wird der CP-Instanz eine vorhandene Benutzergruppe zugewiesen. Alle zu der Gruppe gehörenden Benutzer können über dieses Portal auf das Netzwerk zugreifen.
- **RADIUS-IP-Netzwerk**: Wählen Sie, ob der WAP als RADIUS-Client die konfigurierten IPv4- oder die IPv6-RADIUS-Serveradressen verwendet.
- **Globaler RADIUS**: Wenn für den Überprüfungsmodus RADIUS festgelegt ist, wählen Sie diese Option für die globale Standard-RADIUS-Serverliste zum Authentifizieren von Clients. (Weitere Informationen zum Konfigurieren der globalen RADIUS-Server finden Sie im Abschnitt **RADIUS-Server**.) 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 RADIUS-Benutzerkonten aktivieren, gilt dies für den primären RADIUS-Server, alle Backupserver und global oder lokal konfigurierte Server.

- **Server-IP-Addresse 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** bis **4** oder **Server-IPv6-Adress e2** bis **4**: 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 geheimen Pre-Shared-Key ein, den das WAP-Gerät für die Authentifizierung gegenüber dem 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** bis **Schlüssel 4**: Geben Sie den RADIUS-Schlüssel ein, der den konfigurierten RADIUS-Backup-Servern zugeordnet ist. Der Server an Server-IP-Adresse (IPv6)2 verwendet „Schlüssel 1“, der Server an Server-IP-Adresse (IPv6)3 verwendet „Schlüssel 2“ usw.

- **Anzahl der Gebietsschemas**: Die Anzahl der Gebietsschemas, die der Instanz zugeordnet sind. Auf der Seite „Web Customization“ können Sie bis zu drei verschiedene Gebietsschemas erstellen und diese der CP-Instanz zuweisen.

- **Instanz löschen**: Aktivieren, um die aktuelle Instanz zu löschen.

SCHRITT 6 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

Instanzzuordnung

Nachdem Sie eine Instanz erstellt haben, können Sie diese auf der Seite „Instanzzuordnung“ einem VAP zuordnen. Die Einstellungen für zugeordnete CP-Instanzen gelten für Benutzer, die sich gegenüber dem VAP zu authentifizieren versuchen.

Zuordnen einer Instanz zu einem VAP

So ordnen Sie eine Instanz einem VAP zu:

SCHRITT 1 Wählen Sie **Captive Portal** > **Instanzzuordnung**.

SCHRITT 2 Wählen Sie das Funkmodul aus, das Sie konfigurieren möchten.

SCHRITT 3 Wählen Sie für jeden VAP, dem Sie eine Instanz zuordnen möchten, den Instanznamen aus.

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

Anpassung des Webportals

Nachdem die CP-Instanz einem VAP zugeordnet wurde, müssen Sie ein Gebietsschema (eine Authentifizierungswebseite) erstellen und dieses der CP-Instanz zuordnen. Wenn Benutzer auf einen VAP zugreifen, der einer Captive Portal-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.

Konfigurieren der CP-Authentifizierungsseite

Erstellen und Anpassen einer CP-Authentifizierungsseite

So können Sie eine CP-Authentifizierungsseite erstellen und anpassen:

SCHRITT 1 Wählen Sie **Captive Portal > Anpassung des Webportals**.

SCHRITT 2 **Wählen Sie „Erstellen“** aus der Liste**Gebietsschema für das Captive Portal-Web** aus.

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 Parameter:

- **Gebietsschemaname für das Web**: Geben Sie einen Gebietsschemanamen für das Web ein, der der Seite zugeordnet werden soll. Der Name kann aus 1 bis 32 alphanumerischen Zeichen bestehen.
- **Captive Portal-Instanzen**: Wählen Sie die CP-Instanz aus, der dieses Gebietsschema zugeordnet ist. Sie können einer Instanz mehrere Gebietsschemas zuordnen. Wenn Benutzer auf einen bestimmten VAP zuzugreifen versuchen, der einer CP-Instanz zugeordnet ist, werden die dieser Instanz zugeordneten Gebietsschemas auf der Authentifizierungsseite als Links angezeigt. Die Benutzer können einen Link auswählen, um zum jeweiligen Gebietsschema zu wechseln.

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

SCHRITT 5 Der Bereich „Gebietsschemaparameter für das Captive Portal-Web“ wird erneut mit zusätzlichen Optionen für die Änderung des Gebietsschemas angezeigt. Die Felder „Gebietsschema-ID“ und „Instanzname“ können Sie nicht bearbeiten. Die Felder, die Sie bearbeiten können, sind mit Standardwerten gefüllt.

SCHRITT 6 Konfigurieren Sie die folgenden Parameter:

- **Name des Hintergrundbilds**: Wählen Sie das Bild, das als Seitenhintergrund angezeigt werden soll. Sie können auf **Benutzerdefiniertes Webbild hochladen/löschen** klicken, um Bilder für Captive Portal-Instanzen hochzuladen. Weitere Informationen finden Sie unter **Hochladen und Löschen von Bildern**.
- **Name des Logobilds**: Wählen Sie die Bilddatei, die in der linken oberen Ecke der Seite angezeigt werden soll. Dieses Bild (beispielsweise das Unternehmenslogo) wird zu Brandingzwecken verwendet. Wenn Sie ein benutzerdefiniertes Logobild in das WAP-Gerät hochladen, können Sie das Bild in der Liste auswählen.
- **Vordergrundfarbe**: Geben Sie den HTML-Code für die Vordergrundfarbe im sechsstelligen Hexadezimalformat ein. Möglich sind Werte im Bereich von 1 bis 32 Zeichen. Der Standardwert lautet „#999999“.
- **Hintergrundfarbe**: Geben Sie den HTML-Code für die Hintergrundfarbe im sechsstelligen Hexadezimalformat ein. Möglich sind Werte im Bereich von 1 bis 32 Zeichen. Der Standardwert lautet „#BFBFBF“.

- **Trennzeichen**: Geben Sie den HTML-Code für die Farbe der dicken horizontalen Linie ein, die den Kopfausschnitt der Seite vom Hauptbereich trennt, im sechsstelligen Hexadezimalformat. Möglich sind Werte im Bereich von 1 bis 32 Zeichen. Der Standardwert lautet „#BFBFBF“.
- **Gebietsschemabezeichner**: Geben Sie eine aussagekräftige Beschriftung für das Gebietsschema ein (1 bis 32 Zeichen). Standardmäßig ist das Gebietsschema „Englisch“ festgelegt.
- **Locale**: Geben Sie eine Abkürzung für das Gebietsschema ein (1 bis 32 Zeichen). Der Standardwert lautet „en“.
- **Kontobild**: Wählen Sie die Bilddatei aus, die über dem Anmeldefeld angezeigt werden soll, und eine authentifizierte Anmeldung symbolisiert.
- **Kontobezeichner**: Der Text, mit dem Benutzer angewiesen werden, einen Benutzernamen einzugeben. Möglich sind Werte im Bereich von 1 bis 32 Zeichen.
- **Benutzerbezeichner**: Das Label des Textfelds für den Benutzernamen. Möglich sind Werte im Bereich von 1 bis 32 Zeichen.
- **Kennwortbezeichner**: Das Label des Textfelds für das Benutzerkennwort. Möglich sind Werte im Bereich von 1 bis 64 Zeichen.
- **Schaltflächenbezeichner**: Das Label der Schaltfläche, auf die Benutzer klicken, um den Benutzernamen und das Kennwort zur Authentifizierung zu übermitteln. Möglich sind Werte im Bereich von 2 bis 32 Zeichen. Der Standardwert lautet „Verbinden“.
- **Schriftarten**: Der Name der Schriftart, die für den gesamten Text auf der CP-Seite verwendet werden soll. Sie können mehrere durch Kommas getrennte Schriftartnamen eingeben. Wenn die erste Schriftart auf dem Clientsystem nicht verfügbar ist, wird die nächste Schriftart verwendet usw. Schließen Sie Schriftartnamen, die Leerzeichen enthalten, in Anführungszeichen ein. Möglich sind Werte im Bereich von 1 bis 512 Zeichen. Der Standardwert lautet „MS UI Gothic, Arial, Sans-Serif“.
- **Browsertitel**: Der Text, der in der Titelleiste des Browsers angezeigt werden soll. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet „Captive Portal“.
- **Browserinhalt**: Der Text, der im Seiten-Header rechts neben dem Logo angezeigt wird. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet „Welcome to the Wireless Network“.

- **Inhalt**: Der Anweisungstext, der im Textkörper der Seite unter den Textfeldern für Benutzername und Kennwort angezeigt wird. Möglich sind Werte im Bereich von 1 bis 256 Zeichen. 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. Möglich sind Werte im Bereich von 1 bis 4096 Zeichen. Der Standardwert lautet „Nutzungsrichtlinien akzeptieren“.
- **Akzeptierungsbezeichner**: Der Text, mit dem Benutzer angewiesen werden, durch Aktivieren des Kontrollkästchens zu bestätigen, dass sie die Richtlinien für die Verwendung gelesen haben und akzeptieren. Möglich sind Werte im Bereich von 1 bis 128 Zeichen.
- **Text bei Nicht-Akzeptieren**: Der Text, der in einem Popupfenster angezeigt wird, wenn Benutzer Anmeldeinformationen übermitteln, ohne das Kontrollkästchen „Nutzungsrichtlinie akzeptieren“ zu aktivieren. Möglich sind Werte im Bereich von 1 bis 128 Zeichen.
- **Text während der Authentifizierung**: Der Text, der während der Authentifizierung angezeigt wird. Möglich sind Werte im Bereich von 1 bis 128 Zeichen.
- **Text für fehlgeschlagene Authentifizierung**: Der Text, der angezeigt wird, wenn die Authentifizierung eines Benutzers fehlschlägt. Möglich sind Werte im Bereich von 1 bis 128 Zeichen.
- **Begrüßungstitel**: Der Text, der angezeigt wird, wenn der Client gegenüber dem VAP authentifiziert wurde. Möglich sind Werte im Bereich von 1 bis 128 Zeichen.
- **Begrüßungsinhalt**: Der Text, der angezeigt wird, wenn der Client mit dem Netzwerk verbunden ist. Möglich sind Werte im Bereich von 1 bis 256 Zeichen.
- **Gebietsschema löschen**: Löscht das aktuelle Gebietsschema.

SCHRITT 7 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

SCHRITT 8 Klicken Sie auf **Vorschau**, um die aktualisierte Seite anzuzeigen.

HINWEIS 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.

Hochladen und Löschen von Bildern

Wenn Benutzer den Zugriff auf einen VAP einleiten, der einer Captive Portal-Instanz zugeordnet ist, wird eine Authentifizierungsseite angezeigt. Die Authentifizierungsseite können Sie mit Ihrem eigenen Logo oder anderen Bildern anpassen.

Sie können bis zu 18 Bilder hochladen (dabei wird von sechs Gebietsschemas mit jeweils drei Bildern ausgegangen). Alle Bilder dürfen maximal 5 KB groß sein und müssen im GIF- oder JPG-Format vorliegen.

Die Größe der Bilder wird an die angegebenen Abmessungen angepasst. Die besten Ergebnisse erzielen Sie, wenn die Größenverhältnisse des Logos und der Kontobilder im Wesentlichen den folgenden Angaben für Standardbilder entsprechen:

Bildtyp	Verwendung	Standardbreite x Höhe
Hintergrund	Wird als Seitenhintergrund angezeigt.	10 x 800 Pixel
Logo	Wird links oben auf der Seite angezeigt und enthält Brandinginformationen.	168 x 78 Pixel
Konto	Wird über dem Anmeldefeld angezeigt und symbolisiert eine authentifizierte Anmeldung.	295 x 55 Pixel

Hochladen von binären Grafikdateien in das WAP-Gerät

So laden Sie binäre Grafikdateien in das WAP-Gerät hoch:

SCHRITT 1 Klicken Sie auf der Seite „Anpassung des Webportals“ auf **Benutzerdefiniertes Webbild hochladen/löschen** neben dem Feld **Name des Hintergrundbilds**, **Name des Logobilds** oder **Kontobild**.

Die Seite „Benutzerdefiniertes Webportal-Bild“ wird angezeigt.

SCHRITT 2 Klicken Sie auf „Durchsuchen“, um das Bild zu suchen.

SCHRITT 3 Klicken Sie auf **Hochladen**.

SCHRITT 4 Klicken Sie auf **Zurück**, um zur Seite „Benutzerdefiniertes Webportal-Bild“ zurückzukehren.

SCHRITT 5 Wählen Sie das **Gebietsschema für das Captive Portal-Web**, das Sie konfigurieren möchten.

SCHRITT 6 Wählen Sie für die Felder **Name des Hintergrundbilds**, **Name des Logobilds** oder **Kontobild** das neu hochgeladene Bild aus.

SCHRITT 7 Klicken Sie auf **Speichern**.

SCHRITT 8 Zum Löschen eines Bilds wählen Sie das Bild auf der Seite „Benutzerdefiniertes Webportal-Bild“ in der Liste **Benutzerdefiniertes Webportal-Bild löschen** aus und klicken Sie auf **Löschen**. Die Standardbilder können Sie nicht löschen.

Authentifizierte Clients

Die Seite „Authentifizierte Clients“ bietet zwei Tabellen. Die Tabelle „Authentifizierte Clients“ enthält Informationen zu Clients, die in einer Captive Portal-Instanz authentifiziert wurden. In der Tabelle „Clients mit fehlgeschlagene Authentifizierung“ werden Informationen zu Clients aufgeführt, die erfolglos versucht haben, sich im Captive Portal zu authentifizieren.

Um eine Liste mit authentifizierten Clients anzuzeigen, bei denen die Authentifizierung fehlgeschlagen ist, wählen Sie „Captive Portal“ > „Authentifizierte Clients“. Die folgenden Informationen werden angezeigt:

- **MAC-Adresse**: 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-ID**: Der VAP, dem der Benutzer zugeordnet ist

- **Funk-ID**: Die Funk-ID
- **Captive Portal-ID**: Die ID der Captive Portal-Instanz, der der Benutzer zugeordnet ist
- **Sitzungstimeout**: Die in Sekunden verbleibende Zeit, während der die CP-Sitzung gültig ist. Wenn Null erreicht ist, wird der Client deauthentifiziert.
- **Löschungstimeout**: Die in Sekunden verbleibende Zeit, während der der Clienteintrag gültig ist. Der Timer wird gestartet, wenn die Zuordnung des Clients zum CP aufgehoben wird. Wenn Null erreicht ist, wird der Client deauthentifiziert.
- **Empfangene Pakete**: Die Anzahl der IP-Pakete, die das WAP-Gerät von der Benutzerstation empfangen hat
- **Gesendete Pakete**: Die Anzahl der IP-Pakete, die vom WAP-Gerät an die Benutzerstation gesendet wurden
- **Empfangene Bytes**: Die Anzahl der Bytes, die das WAP-Gerät von der Benutzerstation empfangen hat
- **Gesendete Bytes**: Die Anzahl der Bytes, die vom WAP-Gerät an die Benutzerstation gesendet wurden
- **Fehlerzeit**: Der Zeitpunkt, zu dem der Authentifizierungsfehler aufgetreten ist. Aus dem enthaltenen Zeitstempel geht der Zeitpunkt des Fehlers hervor.

Sie können auf **Aktualisieren** klicken, um die neuesten Daten des WAP-Geräts anzuzeigen.

12

Single Point Setup

This section describes how to configure Single Point Setup over multiple WAP devices.

It includes these topics:

- **Single Point Setup – Übersicht**
- **Access Points**
- **Sitzungen**
- **Kanalverwaltung**
- **Wireless Neighborhood**
- **Cluster-Firmware-Upgrade**

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 WAP571/E-Geräten, jedoch keine anderen Modelle als WAP571/E im selben Cluster.

Single Point Setup ermöglicht die Verwaltung mehrerer Cluster im gleichen Subnetz oder Netzwerk, die jedoch als einzelne unabhängige Entitäten verwaltet werden. In der folgenden Tabelle finden Sie die Single Point Setup-Beschränkungen für WLAN-Dienste.

Gruppentyp/ Clustertyp	WAP-Geräte pro Single Point Setup	Anzahl der aktiven Clients pro Single Point Setup	Maximale Anzahl der Clients (aktiv und im Leerlauf)
WAP571/E	16	960 für das WAP571/E mit zwei Funkmodulen	2048 für das WAP571/E mit zwei Funkmodulen

In einem Cluster können Konfigurationsinformationen wie beispielsweise 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.

Voraussetzungen und Bedingungen für die Erstellung eines Clusters

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

SCHRITT 1 Planen Sie den Single Point Setup-Cluster. Achten Sie darauf, dass die mindestens zwei WAP-Geräte, die Sie in einem Cluster anordnen möchten, miteinander kompatibel sind. Beispielsweise können Cisco WAP571/E-Geräte nur mit anderen Cisco WAP571/E-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. Informationen hierzu finden Sie unter **Access Points**.

SCHRITT 4 Vergewissern Sie sich, dass alle WAP-Geräte auf den gleichen Single Point Setup-Namen verweisen. Informationen hierzu 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 werden ohne Unterbrechung der WLAN-Verbindung weiterhin dem Gerät zugeordnet. Mit anderen Worten: Der Verlust der Verbindung mit dem Cluster hindert dem WAP-Gerät zugeordnete WLAN-Clients nicht zwangsläufig daran, weiterhin auf Netzwerkressourcen zuzugreifen.
- Wenn der Verlust der Verbindung mit dem Cluster auf eine physische oder logische Trennung von der LAN-Infrastruktur zurückzuführen ist, sind abhängig von der Art des Fehlers möglicherweise Netzwerkdienste für die WLAN-Clients betroffen.

In der Tabelle werden die Konfigurationen zusammengefasst, die von allen WAP-Geräten im Cluster gemeinsam genutzt und verbreitet werden.

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

Allgemeine Konfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
Captive Portal	Kennwortkomplexität
Client-QoS	User Accounts
E-Mail-Alarm	QoS
HTTP/HTTP-Service (Ausnahme: Konfiguration mit SSL-Zertifikaten)	Radio Settings einschließlich TSpec Settings (mit Ausnahmen)
Log Settings	Rogue-AP-Erkennung
MAC-Filterung	Planungsmodul
Verwaltungszugangskontrolle	SNMP General und SNMPv3
Netzwerke	WPA-PSK-Komplexität
Zeiteinstellungen	Wireless Multicast Forwarding (WMF)
LED-Anzeige	
LLDP (außer PoE-Prioritätskonfiguration)	
Umbrella	

Funkkonfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden
Mode
Fragmentation Threshold
RTS Threshold
Ratensätze
Primärer Kanal
Schutz
Feste Multicast-Rate
Broadcast or Multicast Rate Limiting
Kanalbandbreite
Kurzes Schutzintervall unterstützt

Funkkonfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden
Channel
Beacon-Intervall
DTIM-Periode
Maximum Stations
Sendeleistung

Andere Konfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden	
Bandbreitenauslastung	Anschlusseinstellungen
Bonjour	VLAN und IPv4
IPv6 Address	WDS-Bridge
IPv6 Tunnel	
Paketerfassung	WorkGroup-Bridge

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 im Navigationsbereich die Option **Single Point Setup > Access Points** aus.

Single Point Setup ist für den AP standardmäßig deaktiviert. Wenn die Option deaktiviert ist, wird die Schaltfläche **Single Point Setup aktivieren** angezeigt. Wenn die Option deaktiviert ist, wird die Schaltfläche **Single Point Setup deaktivieren** angezeigt. Sie können die Optionen für Single Point Setup nur bearbeiten, wenn Single Point Setup deaktiviert ist.

Aus den Symbolen rechts auf der Seite geht hervor, ob Single Point Setup aktiviert ist. Außerdem sehen Sie dort gegebenenfalls die Anzahl der zurzeit zum Cluster gehörenden WAP-Geräte.

SCHRITT 2 Konfigurieren Sie, wenn Single Point Setup deaktiviert ist, die folgenden Informationen für die einzelnen Mitglieder eines Single Point Setup-Clusters.

- **Standort**: Geben Sie eine Beschreibung für den physischen Standort des Access Points ein, beispielsweise „Rezeption“. Das Feld für den Standort ist optional.
- **Clustername**: 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 Cluster-Name muss für jedes im Netzwerk konfigurierte Single Point Setup eindeutig sein. Der Standardwert lautet „ciscosb-cluster“.
- **Clustering-IP-Version**: Geben Sie die IP-Version an, 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 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.

SCHRITT 3 Klicken Sie auf **Single Point Setup aktivieren**.

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

Während der Suche nach anderen Cluster-Mitgliedern geht aus dem Status hervor, dass die Konfiguration angewendet wird. Aktualisieren Sie die Seite, um die neue Konfiguration zu sehen.

Wenn mindestens ein WAP-Gerät bereits mit den gleichen Cluster-Einstellungen konfiguriert ist, tritt das WAP-Gerät dem Cluster bei, und die Informationen zu den einzelnen Mitgliedern werden in einer Tabelle angezeigt.

SCHRITT 4 Wiederholen Sie diese Schritte für weitere WAP-Geräte, die Sie Single Point Setup hinzufügen möchten.

Anzeigen von Single Point Setup-Informationen

Wenn Single Point Setup aktiviert ist, bildet der AP automatisch einen Cluster mit anderen WAP-Geräten mit der gleichen Konfiguration. Auf der Seite „Access Points“ werden die erkannten WAP-Geräte in einer Tabelle aufgeführt. Die folgenden Informationen werden angezeigt:

- **Standort**: Beschreibung des physischen Standorts des Access Points
- **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.
- **IP-Adresse**: Die IP-Adresse für den Access Point

Der Single Point Setup-Status und die Anzahl der WAP-Geräte werden rechts auf der Seite grafisch dargestellt.

Hinzufügen eines Access Points zu einem Single Point Setup

So fügen Sie einen neuen Access Point, der sich zurzeit im eigenständigen Modus befindet, einem Single Point Setup-Cluster hinzu:

SCHRITT 1 Wechseln Sie in dem eigenständigen Access Point zum webbasierten Konfigurationsdienstprogramm.

SCHRITT 2 Wählen Sie im Navigationsbereich die Option **Single Point Setup > Access Points** aus.

SCHRITT 3 Legen Sie **Clustername** auf den gleichen Namen fest, der für die Cluster-Mitglieder konfiguriert ist.

SCHRITT 4 (Optional) Geben Sie in das Feld **Standort** eine Beschreibung für den physischen Standort des Access Points ein, beispielsweise „Rezeption“.

SCHRITT 5 Klicken Sie auf **Single Point Setup aktivieren**.

Der Access Point tritt automatisch dem Single Point Setup bei.

Entfernen eines Access Points aus einem Single Point Setup

So entfernen Sie einen Access Point aus dem Single Point Setup-Cluster:

SCHRITT 1 Klicken Sie in der Tabelle mit den erkannten Geräten auf die IP-Adresse des WAP-Geräts im Cluster, das Sie entfernen möchten.

Das webbasierte Konfigurationsdienstprogramm für das WAP-Gerät wird angezeigt.

SCHRITT 2 Wählen Sie im Navigationsbereich die Option **Single Point Setup > Access Points** aus.

SCHRITT 3 Klicken Sie auf **Single Point Setup deaktivieren**.

Im Statusfeld **Single Point Setup** für den Access Point wird jetzt **Deaktviert**angezeigt.

Navigieren zu Konfigurationsinformationen für ein bestimmtes Gerät

Alle WAP-Geräte in einem Single Point Setup-Cluster weisen die gleiche Konfiguration auf (wenn die konfigurierbaren Elemente verbreitet werden können). Es spielt keine Rolle, mit welchem WAP-Gerät Sie zu Verwaltungszwecken eine Verbindung herstellen – Konfigurationsänderungen an jedem WAP-Gerät im Cluster werden an die anderen Mitglieder verbreitet.

Es kann jedoch Situationen geben, in denen Sie Informationen zu einem bestimmten WAP-Gerät anzeigen oder verwalten möchten. Sie möchten beispielsweise Statusinformationen wie Clientzuordnungen oder Ereignisse für einen Access Point überprüfen. In diesem Fall können Sie in der Tabelle auf der Seite „Access Points“ auf die IP-Adresse klicken, um das webbasierte Konfigurationsdienstprogramm für den jeweiligen Access Point anzuzeigen.

Navigieren zu einem Gerät anhand der IP-Adresse in einer URL

Sie können auch eine Verbindung mit dem webbasierten Konfigurationsdienstprogramm eines bestimmten WAP-Geräts herstellen, indem Sie die IP-Adresse des jeweiligen Access Points als URL im folgenden Format direkt in die Adressleiste des Webbrowsers eingeben:

http://IP-Adresse des Access Points (bei Verwendung von HTTP)

https://IP-Adresse des Access Points (bei Verwendung von HTTPS)

Sitzungen

Auf der Seite „Sessions“ werden Informationen zu WLAN-Clients angezeigt, die den WAP-Geräten im Single Point Setup-Cluster zugeordnet sind. Zu den einzelnen WLAN-Clients werden die jeweilige MAC-Adresse und Gerätestandort, an dem das Gerät zurzeit verbunden ist, angegeben.

HINWEIS Auf der Seite „Sitzungen“ werden maximal 20 Clients pro Funkmodul der WAP-Geräte im Cluster angezeigt. Zum Anzeigen aller einem bestimmten WAP-Gerät zugeordneten WLAN-Clients zeigen Sie die Seite „Status“ > „Associated Clients“ direkt auf dem jeweiligen Gerät an.

Zum Anzeigen einer bestimmten Statistik für eine WLAN-Clientsitzung wählen Sie in der Liste „Anzeigen“ ein Element aus, und klicken Sie auf **Los**. Sie können Informationen zur Leerlaufzeit, zur Datenrate und zur Signalstärke anzeigen.

Bei einer Sitzung handelt es sich in diesem Kontext um den Zeitraum, in dem ein Benutzer eines Client-Geräts (Station) mit einer eindeutigen MAC-Adresse eine Verbindung mit dem WLAN aufrechterhält. Die Sitzung beginnt mit der Anmeldung des WLAN-Clients beim Netzwerk und endet, wenn der WLAN-Client bewusst abgemeldet wird oder die Verbindung aus einem anderen Grund abbricht.

HINWEIS Eine Sitzung ist nicht das Gleiche wie eine Zuordnung, die eine Verbindung eines WLAN-Clients mit einem bestimmten Access Point beschreibt. Eine WLAN-Clientzuordnung kann im Lauf einer Sitzung von einem Access Point im Cluster zu einem anderen Access Point im Cluster verlagert werden.

Zum Anzeigen der dem Cluster zugeordneten Sitzungen wählen Sie **Single Point Setup > Sitzungen**.

Die folgenden Daten werden für jede WLAN-Clientsitzung mit Single Point Setup angezeigt.

- **AP-Standort**: Der Standort des Access Points.

  Der Standort wird von dem Standort abgeleitet, den Sie auf der Seite „Administration“ > „System Settings“ angegeben haben.

- **Benutzer-MAC**: Die MAC-Adresse des WLAN-Clients.

  Eine MAC-Adresse ist eine Hardwareadresse, mit der jeder Knoten eines Netzwerks eindeutig identifiziert wird.

- **Leerlauf**: Gibt an, wie lange dieser WLAN-Client inaktiv war.

  Ein WLAN-Client gilt als inaktiv, wenn er keine Daten empfängt oder sendet.

- **Rate**: Die ausgehandelte Datenrate. Die tatsächlichen Übertragungsraten können je nach Aufwand unterschiedlich sein.

  Die Datenübertragungsrate wird in Megabit pro Sekunde (MBit/s) gemessen. Der Wert sollte im Bereich des angekündigten Ratensatzes für den vom Access Point verwendeten Modus liegen. Beispiel: 6 bis 54 MBit/s für 802.11a.

  Die gemeldete Rate entspricht der Geschwindigkeit des letzten Pakets, das vom Access Point an den Client übertragen wurde. Dieser Wert kann innerhalb des angezeigten Ratensatzes auf Basis der Signalqualität zwischen AP und Client und der Geschwindigkeit, mit der Broadcast- oder Multicast-Frames gesendet werden, variieren. Wenn der Access Point mit Standardraten einen Broadcast-Frame an eine WLAN-Station sendet, wird das Feld 1 Mbit/s für 2,4-Ghz- und 6 Mbit/s für 5-Ghz-Funkmodule berichten. Clients, die inaktiv sind, übertragen mit hoher Wahrscheinlichkeit die niedrigen Standardraten.

- **Signal**: Die Stärke des Funkfrequenzsignals (Radio Frequency, RF), das der WLAN-Client vom Access Point empfängt. Der Messwert wird als RSSI (Received Signal Strength Indication) bezeichnet und liegt zwischen 0 und 100.

- **Gesamt empfangen**: Die Gesamtanzahl der Pakete, die der WLAN-Client während der aktuellen Sitzung empfangen hat

- **Gesamt gesendet**: Die Gesamtanzahl der Pakete, die während dieser Sitzung an den WLAN-Client gesendet wurden

- **Fehlerrate**: Der Prozentanteil der Zeit-Frames, die bei der Übertragung über diesen Access Point gelöscht wurden

---

Zum Sortieren der Informationen in den Tabellen nach einem bestimmten Indikator klicken Sie auf die Spaltenüberschrift, nach der Sie sortieren möchten. Wenn Sie beispielsweise die Tabellenzeilen nach der Signalstärke sortieren möchten, klicken Sie auf die Spaltenüberschrift „Signal“.

Kanalverwaltung

Auf der Seite „Channel Management“ werden die aktuellen und geplanten Kanalzuweisungen für WAP-Geräte in einem Single Point Setup-Cluster angezeigt.

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

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

Der Kanal-Manager (das heißt das Gerät, das dem Cluster die Konfiguration bereitgestellt hat) ordnet in einem angegebenen Intervall alle WAP-Geräte im Cluster anderen Kanälen zu und misst die Interferenzstufen der Cluster-Mitglieder. Wenn erhebliche Kanalinterferenzen erkannt werden, weist der Kanal-Manager automatisch anhand eines Effizienzalgorithmus (oder eines automatisierten Kanalplans) einige oder alle Geräte neuen Kanälen zu. Wenn der Kanal-Manager eine Änderung für notwendig hält, werden die Informationen für die Neuzuweisung an alle Mitglieder des Clusters gesendet. Außerdem wird eine Syslog-Nachricht generiert, aus der das sendende Gerät sowie die neuen und die alten Kanalzuweisungen hervorgehen.

Konfigurieren und Anzeigen von Kanalzuweisungen für Single Point Setup-Mitglieder

So können Sie die Kanalzuweisungen für die Single Point Setup-Mitglieder konfigurieren und anzeigen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Single Point Setup** > **Kanalverwaltung** aus.

Auf der Seite „Kanalverwaltung“ können Sie die Kanalzuweisungen für alle WAP-Geräte im Cluster anzeigen und die automatische Kanalverwaltung beenden oder starten. Außerdem können Sie mit den erweiterten Einstellungen die Reduzierung von Störspannungen ändern, die Neuzuweisungen von Kanälen auslösen, den Zeitplan für automatische Updates ändern und die Gruppe der für Zuweisungen verwendeten Kanäle neu konfigurieren.

SCHRITT 2 Zum Starten der automatischen Kanalzuweisung klicken Sie auf **Start**.

Die Kanalverwaltung setzt das standardmäßige Cluster-Verhalten außer Kraft, bei dem die Funkkanäle aller WAP-Geräte, die Mitglieder des Clusters sind, synchronisiert werden. Wenn die Kanalverwaltung aktiviert ist, wird der Funkkanal nicht im Cluster mit anderen Geräten synchronisiert.

Wenn die automatische Kanalzuweisung aktiviert ist, ordnet der Kanal-Manager in regelmäßigen Abständen die von WAP-Geräten in einem Single Point Setup-Cluster verwendeten Funkkanäle zu und weist gegebenenfalls Kanäle neu zu, um Interferenzen mit anderen Cluster-Mitgliedern oder Geräten außerhalb des Clusters zu reduzieren. Die Kanalrichtlinie für das Funkmodul wird automatisch auf den statischen Modus festgelegt, und die Option **Auto** ist für das Feld **Kanal** auf der Seite „Wireless > Funkmodul“ nicht verfügbar.

Informationen zu den aktuellen und vorgeschlagenen Kanalzuweisungen finden Sie unter „Anzeigen von Kanalzuweisungen und Festlegen von Sperren“.

SCHRITT 3 Zum Beenden der automatischen Kanalzuweisung klicken Sie auf **Anhalten**.

Es werden keine Kanalverwendungszuordnungen oder Kanalneuzuweisungen vorgenommen. Nur manuelle Aktualisierungen wirken sich auf die Kanalzuweisung aus.

Anzeigen von Kanalzuweisungen und Festlegen von Sperren

Wenn die Kanalverwaltung aktiviert ist, werden auf der Seite die Tabellen „Aktuelle Kanalzuordnung“ und „Vorgeschlagene Kanalzuordnung“ angezeigt.

Aktuelle Kanalzuordnung – Tabelle

Die Tabelle „Aktuelle Kanalzuordnung“ 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.

- **Standort**: Der physische Standort des Geräts
- **IP-Adresse**: Die IP-Adresse für den Access Point
- **Wireless-Funkmodul**: Die MAC-Adresse des Funkmoduls
- **Band**: Das Band, über das der Access Point sendet
- **Kanal**: Der Funkkanal, über den dieser Access Point zurzeit sendet
- **Gesperrt**: Zwingt den Access Point, den aktuellen Kanal beizubehalten.
- **Status**: Zeigt den Status des WLAN-Funkmoduls im 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).

Wenn automatisierte Kanalverwaltungspläne für einen Access Point ausgewählt sind, werden die WAP-Geräte nicht im Rahmen der Optimierungsstrategie 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.

Vorgeschlagene Kanalzuordnung – Tabelle

Die Tabelle „Vorgeschlagene Kanalzuordnung“ enthält 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 anderen Kanälen als den bisher verwendeten zugewiesen werden.

Für jedes WAP-Gerät im Single Point Setup werden in der Tabelle „Vorgeschlagene Kanalzuordnung“ wie in der Tabelle „Aktuelle Kanalzuordnung“ Standort, IP-Adresse und WLAN-Funkmodul angezeigt. Außerdem wird der vorgeschlagene Kanal angezeigt, das heißt der Funkkanal, dem dieses WAP-Gerät bei der Anwendung des Kanalplans zugewiesen würde.

Konfigurieren der erweiterten Einstellungen

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

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

Sie können die erweiterten Einstellungen ändern, um Folgendes zu konfigurieren:

- **Kanäle ändern, wenn die Interferenz reduziert wurde um mindestens**: Der Prozentanteil der Interferenzreduzierung, der mindestens erreicht werden muss, damit ein vorgeschlagener Plan angewendet wird. Der Standardwert lautet „75 Prozent“. Mit dem Dropdownmenü können Sie Prozentsätze zwischen 5 und 75 Prozent auswählen. 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.

- **Prüfen, ob es einen bessere Kanäle gibt, alle**: Der Zeitplan für automatisierte Updates. Sie können zwischen Intervallen im Bereich von 30 Minuten bis sechs Monaten wählen.

  Standardmäßig ist eine Stunde festgelegt, das heißt, die Kanalverwendung wird stündlich neu bewertet, und der sich ergebende Kanalplan wird angewendet.

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

Wireless Neighborhood

Auf der Seite „WLANS in der Nähe“ werden bis zu 20 Geräte pro Funkmodul innerhalb der Reichweite der einzelnen WLAN-Funkmodule im Cluster angezeigt. (Wenn beispielsweise ein WAP-Gerät über zwei WLAN-Funkmodule verfügt, werden im Cluster 40 Geräte angezeigt.) Auf der Seite „Wireless Neighborhood“ wird außerdem zwischen Cluster-Mitgliedern und Nichtmitgliedern unterschieden.

Die Ansicht „Wireless Neighborhood“ bietet Ihnen folgende Möglichkeiten:

- Erkennen und Suchen unerwarteter Geräte (oder von Rogue-Geräten) in einer WLAN-Domäne, damit Sie Maßnahmen ergreifen können, um die damit verbundenen Risiken zu begrenzen.
- Überprüfen der Erwartungen hinsichtlich der Abdeckung. Indem Sie ermitteln, welche WAP-Geräte mit welcher Signalstärke von anderen Geräten aus sichtbar sind, können Sie überprüfen, ob die Bereitstellung den Planungszielen entspricht.
- Suchen nach Fehlern. Unerwartete Änderungen des Abdeckungsmusters sind in der farblich codierten Tabelle auf einen Blick erkennbar.

Zum Anzeigen von benachbarten Geräte wählen Sie **Single Point Setup** > **Wireless Neighborhood**. Zum Anzeigen aller erkannten Geräte in einem bestimmten Single Point Setup navigieren Sie zur Weboberfläche eines Mitglieds, und wählen Sie im Navigationsbereich die Option **Wireless** > **Rogue-AP-Erkennung**.

Für jeden benachbarten Access Point werden die folgenden Informationen angezeigt:

- **Benachbarte APs anzeigen**: Wählen Sie eines der folgenden Optionsfelder aus, um die Ansicht zu ändern:
  - **Im Cluster**: Nur benachbarte WAP-Geräte, die Mitglieder des Clusters sind
  - **Nicht im Cluster**: Nur benachbarte WAP-Geräte, die nicht Mitglieder des Clusters sind
  - **Beide**: Zeigt alle benachbarten WAP-Geräte an (Cluster-Mitglieder und Nichtmitglieder).

HINWEIS Bei einem erkannten AP, der auch Cluster-Mitglied ist, werden mit „Im Cluster“ nur die SSIDs des Standard-VAPs (VAP0) angezeigt. Für Nichtstandard-VAPs im AP wird „Nicht im Cluster“ angezeigt.

- **Cluster**: Die Liste oben in der Tabelle enthält die IP-Adressen aller im Cluster gruppierten WAP-Geräte. (Diese Liste ist mit der Liste der Mitglieder auf der Seite **Single Point Setup** > **Access Points** identisch).

  Wenn im Cluster nur ein WAP-Gerät vorhanden ist, wird nur eine einzige IP-Adressen-Spalte angezeigt. Daran erkennen Sie, dass das WAP-Gerät mit sich selbst gruppiert ist.

  Sie können auf eine IP-Adresse klicken, um weitere Details zu einem bestimmten WAP-Gerät anzuzeigen.

- **Nachbarn**: Benachbarte Geräte mindestens eines der Geräte im Cluster werden in der linken Spalte nach der SSID (Netzwerkname) aufgeführt.

Ein als Nachbar erkanntes Gerät kann auch selbst Cluster-Mitglied sein. Nachbarn, die auch Cluster-Mitglieder sind, werden immer oben in der Liste mit einem dicken Balken darüber und mit einer Angabe des Standorts angezeigt.

Die farbigen Balken rechts neben den einzelnen WAP-Geräten in der Liste „Neighbors“ geben die Signalstärke für die einzelnen benachbarten WAP-Geräte an, die von dem Cluster-Mitglied mit der über der jeweiligen Spalte genannten IP-Adresse erkannt wird. Wenn Sie den Mauszeiger über die Balken bewegen, wird eine Zahl angezeigt, die die Stärke in Dezibel (dB) angibt.

Anzeigen von Details für ein Single Point Setup-Mitglied

Zum Anzeigen von Details zu einem Cluster-Mitglied klicken Sie oben auf der Seite auf die IP-Adresse eines Mitglieds.

In der Liste „Nachbarn“ werden die folgenden Details für das Gerät angezeigt.

- **SSID**: Die SSID (Netzwerkadresse) für den benachbarten Access Point
- **MAC-Adress**: Die MAC-Adresse des benachbarten Access Points
- **Kanal**: Der Kanal, über den der Access Point zurzeit sendet
- **Rate**: Die Rate (in Megabit pro Sekunde), mit der dieser Access Point zurzeit sendet. Bei der aktuellen Rate handelt es sich immer um eine der unter „Supported Rates“ angezeigten Raten.
- **Signal**: Die in Dezibel (dB) gemessene Stärke des erkannten Funksignals des Access Points
- **Beacon-Intervall**: Das vom Access Point verwendete Beacon-Intervall
- **Beacon-Alter**: Datum und Uhrzeit des letzten von diesem Access Point empfangenen Beacons

Cluster-Firmware-Upgrade

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.

Auswählen von Cluster-Mitglied für Upgrade

So wählen Sie ein Cluster-Mitglied für ein Upgrade aus

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Single Point Setup > Cluster Firmware Upgrade**.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen neben dem AP, der aktualisiert werden soll.

SCHRITT 3 Klicken Sie auf **Speichern**.

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

Klicken Sie auf **Aktualisieren**.

Aktualisieren der Firmware eines Cluster-Mitglieds mittels TFTP

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

SCHRITT 1 Wählen Sie **TFTP als Transfermethode**.

SCHRITT 2 Geben Sie in das Feld **Quelldateiname** einen Namen (1 bis 128 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** und klicken Sie auf **Upgrade starten**.

Durchführen eines Upgrade über HTTP

So führen Sie das Upgrade über HTTP durch:

SCHRITT 1 Wählen **HTTP als Transfermethode**.

SCHRITT 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.

SCHRITT 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**.

13

Umbrella

In diesem Kapitel wird die Konfiguration der Umbrella-Funktion auf den WAP-Geräten beschrieben.

Das Kapitel enthält die folgenden Themen:

- **Cisco Umbrella – Übersich**
- **Konfigurieren von Umbrella**

Cisco Umbrella – Übersich

Cisco Umbrella ist ein in der Cloud bereitgestellter Netzwerksicherheitsdienst, der Einblicke liefert, um Geräte in Echtzeit vor Malware und Sicherheitsverletzungen zu schützen. Der Dienst nutzt sich weiterentwickelnde Big-Data- und Data-Mining-Methoden für die proaktive Vorhersage von Angriffen und für die kategoriebasierte Filterung.

Cisco Umbrella-Server lösen die DNS-Anfrage auf und setzen vorkonfigurierte Sicherheitsfilterregeln identitätsbasiert durch, um die Domäne entweder als schädlich (auf dem Client wird eine blockierte Seite ausgegeben) oder als sicher (auf dem Client wird eine aufgelöste IP-Adresse ausgegeben) zu kennzeichnen.

Konfigurieren von Umbrella

Gehen Sie wie folgt vor, um Umbrella zu konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich **Umbrella** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Aktivieren**: Aktiviert oder deaktiviert die Umbrella-Funktion auf dem WAP-Gerät.

- **API Key**: Rufen Sie den API Key von Ihrem Umbrella-Dashboard ab: **Admin** -> **API Keys**.
- **API-Key-Geheimnis**: Das API-Key-Geheimnis wird nur einmal bei der Erstellung des API Key im Umbrella-Dashboard angezeigt.

HINWEIS

- Bei Änderungen des API Key, des API-Key-Geheimnisses und des Geräte-Tags wird eine erneute Registrierung für die Erstellung eines Netzwerkgeräts ausgelöst.
- **Geräte-Tag (optional)**: Ein Text-Tag, das das Gerät oder einen bestimmten, dem Gerät zugeordneten Ursprung beschreibt. Vergewissern Sie sich, dass das Tag für Ihre Organisation eindeutig ist.
- **Zu umgehende lokale Domänen (optional)**: Der AP leitet die DNS-Anfrage weiter, wenn sie in der Liste enthalten ist. Die Einträge in dieser Liste müssen durch Kommata voneinander getrennt werden und die Domänen können Platzhalter in Form eines Asterisks (*) beinhalten. Beispiel: *.cisco.com.*.
- **DNSCrypt**: Legt fest, ob die DNSCrypt-Funktion aktiv ist
- .**Registrierungsstatus**: Der Registrierungsstatus wird angezeigt: Mögliche Status sind **Erfolgreich**, **Registrierung läuft** oder **Fehlgeschlagen.**

A

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 **Status und Statistiken > Protokoll** klicken.

Tabelle mit Ursachencodes für Deauthentifizierungen

In der folgenden Tabelle werden die Ursachencodes für Deauthentifizierungen beschrieben.

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.
6	Es wurde ein Klasse-2-Frame von einer nicht authentifizierten STA empfangen.

Ursachencode	Bedeutung
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	Die Zuordnung wurde aufgrund der BSS-Übergangsverwaltung aufgehoben.
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

B

Weitere Informationen

Cisco bietet eine breite Palette von Ressourcen an, die Ihnen und Ihren Kunden helfen, den WAP571/E optimal zu nutzen.

Support	
Cisco Support Community	www.cisco.com/go/smallbizsupport
Telefonischer Kundensupport des Support Center (SBSC)	www.cisco.com/go/sbsc
Business-Support und -Ressourcen	www.cisco.com/go/smallbizhelp
Supportinformationen	www.cisco.com/go/sbs www.cisco.com/go/software (Registrierung/Anmeldung erforderlich).
Cisco Firmware-Downloads	www.cisco.com/go/smallbizfirmware Wählen Sie einen Link aus, um Firmware für Cisco Produkte herunterzuladen. Es ist keine Anmeldung erforderlich. Downloads von Software und Firmware für alle anderen Cisco Small Business-Produkte stehen im Download-Bereich von Cisco.com unter www.cisco.com/go/software zur Verfügung (Registrierung/Anmeldung erforderlich).
Cisco Open Source-Anfragen	www.cisco.com/go/smallbiz_opensource_request

Cisco Partner Central (Partner-Anmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Produktdokumentation	
Cisco WAP571/E – Wireless-AC/N Premium Dual Radio Access Point mit PoE – Kurzanleitung und Administratorhandbuch	http://www.cisco.com/go/500_wap_resources