ADMINISTRATOR-HANDBUCH

Cisco Small Business

Wireless-N-Access Point WAP551 mit PoE

und

Wireless-N-Access Point WAP561 mit PoE und Bandauswahl

Inhalt

1

Erste Schritte

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

- **Starten des webbasierten Konfigurationsdienstprogramms**
- **Verwenden des Einrichtungsassistenten für Access Points**
- **Erste Schritte**
- **Fensternavigation**

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 das WAP-Gerät 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 **Extras > Internetoptionen** und dann die Registerkarte **Sicherheit** aus. Wählen Sie **Lokales Intranet** und dann **Sites** aus. Wählen Sie **Erweitert** und dann **Hinzufügen** aus. Fügen Sie die Intranetadresse für das WAP-Gerät (**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 das WAP-Gerät zuzugreifen.

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

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

Verwenden des Einrichtungsassistenten für Access Points

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

HINWEIS Wenn Sie auf **Abbrechen** klicken, um den Assistenten zu umgehen, wird die Seite **Change Password** 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 **Configure Device - IP Address** wird angezeigt.

SCHRITT 2 Klicken Sie auf **Dynamic IP Address (DHCP)**, wenn das WAP-Gerät eine IP-Adresse von einem DHCP-Server beziehen soll. Wählen Sie alternativ **Static IP Address** aus, um die IP-Adresse manuell zu konfigurieren. Eine Beschreibung dieser Felder finden Sie unter **VLAN and IPv4 Address Settings**.

SCHRITT 3 Klicken Sie auf **Weiter**. Das Fenster **Single Point Setup - Set a Cluster** wird angezeigt. Eine Beschreibung von Single Point Setup finden Sie unter **Single Point Setup**.

SCHRITT 4 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 **Join an Existing Cluster** klicken und in **Existing Cluster Name** den Namen des vorhandenen Clusters eingeben.

Wenn das Gerät zurzeit nicht Bestandteil eines Single Point Setups sein soll, klicken Sie auf **Do not Enable Single Point Setup**.

(Optional) Sie können in das Feld **AP Location** Text eingeben, aus dem der physische Standort des WAP-Geräts hervorgeht.

SCHRITT 5 Klicken Sie auf **Weiter**. Das Fenster **Configure Device - Set System Date and Time** wird angezeigt.

SCHRITT 6 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 **Time Settings**.

SCHRITT 7 Klicken Sie auf **Weiter**. Das Fenster **Enable Security - Set Password** wird angezeigt.

SCHRITT 8 Geben Sie in **New Password** ein neues Kennwort ein, und geben Sie das Kennwort in das Textfeld **Confirm Password** erneut ein. Weitere Informationen zu Kennwörtern finden Sie unter **User Accounts**.

> **HINWEIS** Sie können das Kontrollkästchen **Password Complexity** deaktivieren, wenn Sie die Regeln für die Kennwortsicherheit deaktivieren möchten. Es wird jedoch dringend empfohlen, die Regeln für die Kennwortsicherheit aktiviert zu lassen.

SCHRITT 9 Klicken Sie auf **Weiter**. Das Fenster **Enable Security - Name Your Wireless Network** wird für die Schnittstelle **Radio 1** angezeigt.

> **HINWEIS** In diesem Fenster und den beiden nächsten Fenstern (**Wireless Security** und **VLAN ID**) konfigurieren Sie diese Einstellungen zuerst für die Schnittstelle **Radio 1**. Bei WAP561-Geräten werden die Fenster dann erneut angezeigt, damit Sie die Einstellungen für **Radio 2** konfigurieren können.

SCHRITT 10 Geben Sie in **Network Name** einen Netzwerknamen ein. Dieser Name dient als SSID für das Standard-WLAN.

SCHRITT 11 Klicken Sie auf **Weiter**. Das Fenster **Enable Security - Secure Your Wireless Network** wird angezeigt.

SCHRITT 12 Wählen Sie einen Sicherheitsverschlüsselungstyp aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter **Systemsicherheit**.

SCHRITT 13 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster **Enable Security- Assign the VLAN ID For Your Wireless Network** an.

SCHRITT 14 Geben Sie eine VLAN-ID für im WLAN empfangenen Verkehr ein.

Es wird vorgeschlagen, für WLAN-Verkehr eine andere VLAN-ID als den Standardwert (**1**) zuzuweisen. Dadurch soll dieser Verkehr vom Verwaltungsverkehr in VLAN 1 getrennt werden.

SCHRITT 15 Klicken Sie auf **Weiter**.

SCHRITT 16 Für das WAP561-Gerät werden die Seiten **Network Name**, **Wireless Security** und **VLAN ID** angezeigt, auf denen Sie **Radio 2** konfigurieren können. Wenn Sie **Radio 2** konfiguriert haben, klicken Sie auf **Weiter**.

Für das WAP321-Gerät zeigt der Assistent das Fenster **Enable Captive Portal - Create Your Guest Network** an.

SCHRITT 17 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 25** fort.

Wenn Sie auf **Ja** klicken, zeigt der Assistent das Fenster **Enable Captive Portal - Name Your Guest Network** an.

SCHRITT 18 Geben Sie in **Guest Network Name** einen Gastnetzwerknamen für **Radio 1** an. Wählen Sie für das WAP561-Gerät aus, ob das Gastnetzwerk **Radio 1** oder **Radio 2** verwendet.

SCHRITT 19 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster **Enable Captive Portal - Secure Your Guest Network** an.

SCHRITT 20 Wählen Sie einen Sicherheitsverschlüsselungstyp für das Gastnetzwerk aus, und geben Sie einen Sicherheitsschlüssel ein. Eine Beschreibung dieser Optionen finden Sie unter **Systemsicherheit**.

SCHRITT 21 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster **Enable Captive Portal - Assign the VLAN ID** an.

SCHRITT 22 Geben Sie eine VLAN-ID für das Gastnetzwerk an. Die VLAN-ID des Gastnetzwerks sollte nicht mit der Verwaltungs-VLAN-ID identisch sein.

SCHRITT 23 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster **Enable Captive Portal - Enable Redirect URL** an.

SCHRITT 24 Wählen Sie die Option **Enable Redirect URL** aus, und geben Sie in das Feld **Redirect 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 25 Klicken Sie auf **Weiter**. Der Assistent zeigt das Fenster **Summary - Confirm Your Settings** an.

SCHRITT 26 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 27 Wenn die Einstellungen richtig sind, klicken Sie auf **Submit**. Die WAP-Setup-Einstellungen werden gespeichert, und es wird ein Bestätigungsfenster angezeigt.

SCHRITT 28 Klicken Sie auf **Fertigstellen**. Das Fenster **Getting Started** wird angezeigt.

Erste Schritte

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

Links auf der Seite **Getting Started**

Kategorie	Linkname (auf der Seite)	Verlinkte Seite
Ersteinrichtung	Run Setup Wizard	Verwenden des Einrichtungsassistenten für Access Points
	Configure Radio Settings	Funk
	Configure Wireless Network Settings	Netzwerke
	Configure LAN Settings	LAN
	Run WPS	WPS-Einrichtung
	Configure Single Point Setup	Single Point Setup
Gerätestatus	System Summary	System Summary
	Wireless Status	Network Interfaces
Schnellzugriff	Change Account Password	User Accounts
	Upgrade Device Firmware	Manage Firmware
	Backup/Restore Configuration	Download/Backup Configuration File

Fensternavigation

In diesem Abschnitt werden die Funktionen des webbasierten AP-Konfigurationsdienstprogramms beschrieben.

Der Header des Konfigurationsdienstprogramms enthält Standardinformationen und wird oben auf jeder Seite angezeigt. Dort befinden sich die folgenden Schaltflächen:

Schaltflächen

Schaltflächenname	Beschreibung
(Benutzer)	Der Kontoname (**Administrator** oder **Gast**) des beim WAP-Gerät angemeldeten Benutzers. Der werksseitige Standardbenutzername lautet **cisco**.
Log Out	Klicken Sie auf diese Schaltfläche, um sich vom webbasierten AP-Konfigurationsdienstprogramm abzumelden.
About	Klicken Sie auf diese Schaltfläche, um Typ und Versionsnummern für das WAP-Gerät 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.

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

Verwaltungsschaltflächen

Schaltflächenname	Beschreibung
Hinzufügen	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.
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.
Neu anzeigen	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 Kapitel wird beschrieben, wie Sie Status und Statistiken anzeigen. Das Kapitel enthält die folgenden Themen:

- System Summary
- Network Interfaces
- Traffic Statistics
- WorkGroup Bridge Transmit/Receive
- Associated Clients
- TSPEC Client Associations
- TSPEC Status and Statistics
- TSPEC AP Statistics
- Radio Statistics
- Email Alert Status
- Log

System Summary

Auf der Seite **System Summary** werden grundlegende Informationen angezeigt, beispielsweise die Beschreibung des Hardwaremodells, die Softwareversion und die seit dem letzten Neustart verstrichene Zeit.

Zum Anzeigen von Systeminformationen wählen Sie im Navigationsbereich die Option **Status and Statistics** > **System Summary** aus. Alternativ können Sie auf der Seite **Getting Started** unter **Device Status** die Option **System Summary** auswählen.

Auf der Seite **System Summary** werden die folgenden Informationen angezeigt:

- **PID VID**: Hardwaremodell und -version des WAP-Geräts
- **Serial Number**: Die Seriennummer des Cisco WAP-Geräts
- **Base MAC Address**: Die MAC-Adresse des WAP-Geräts
- **Firmware Version (Active Image)**: Die Firmwareversion des aktiven Images
- **Firmware MD5 Checksum (Active Image)**: Die Prüfsumme des aktiven Images
- **Firmware Version (Non-active)**: Die Firmwareversionsnummer des Backup-Images
- **Firmware MD5 Checksum (Non-active)**: Die Prüfsumme des Backup-Images
- **Host Name**: Ein dem Gerät zugewiesener Name
- **System Uptime**: Die seit dem letzten Neustart verstrichene Zeit
- **System Time**: Die aktuelle Systemzeit

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

- **Service**: Der Name des Diensts, falls verfügbar
- **Protocol**: Das vom Dienst verwendete zugrunde liegende Transportprotokoll (TCP oder UDP)
- **Local IP Address**: Gegebenenfalls die IP-Adresse eines Remotegeräts, das mit diesem Service im WAP-Gerät verbunden ist. **All** bedeutet, dass jede IP-Adresse im Gerät diesen Dienst verwenden kann.
- **Local Port**: Die Portnummer für den Dienst
- **Remote IP Address**: Gegebenenfalls die IP-Adresse eines Remotehosts, der diesen Dienst verwendet. **All** 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

- **Connection State**: Der Status des Diensts. Für UDP werden in der Tabelle nur Verbindungen mit dem Status **Active** oder **Established** angezeigt. Die TCP-Status lauten:
  - **Listening**: Der Dienst hört Verbindungsanfragen mit.
  - **Active**: Eine Verbindungssitzung ist hergestellt, und es werden Pakete gesendet und empfangen.
  - **Established**: 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.
  - **Time Wait**: Die Schlusssequenz wurde initiiert, und der WAP wartet vor dem Schließen der Verbindung während eines vom System definierten Timeout-Zeitraums (in der Regel 60 Sekunden).

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

Network Interfaces

Auf der Seite **Network Interfaces** können Sie Konfigurations- und Statusinformationen zu den drahtgebundenen Schnittstellen und WLAN-Schnittstellen anzeigen. Zum Anzeigen der Seite **Network Interfaces** wählen Sie im Navigationsbereich die Option **Status and Statistics** > **Network Interface** aus.

Auf der Seite **Network Interfaces** werden die folgenden Informationen angezeigt:

- **LAN Status**: Diese Einstellungen gelten für die interne Schnittstelle.

  Zum Ändern dieser Einstellungen klicken Sie auf den Link **Bearbeiten**. Nach dem Klicken auf **Edit** werden Sie zur Seite **VLAN and IPv4 Address Settings** umgeleitet. Beschreibungen dieser Felder finden Sie unter **VLAN and IPv4 Address Settings**.

- **Radio Status**: Zu diesen Einstellungen gehören der Modus von **Wireless Radio** (**Enabled** oder **Disabled**), die der Funkschnittstelle zugeordnete MAC-Adresse (oder bei WAP561-Geräten beide Funkschnittstellen), der 802.11-Modus (a/b/g/n) und der von der Schnittstelle verwendete Kanal.

  Zum Ändern der WLAN-Einstellungen klicken Sie auf den Link **Bearbeiten**. Nach dem Klicken auf **Bearbeiten** werden Sie zur Seite **Radio** umgeleitet. Beschreibungen dieser Felder finden Sie unter **Funk**.

- **Interface Status**: In dieser Tabelle werden Statusinformationen für die einzelnen VAPs (Virtual Access Points) und WDS-Schnittstellen (Wireless Distribution System) aufgeführt. Bei WAP561-Geräten ist der Schnittstellen-ID die Zeichenfolge **WLAN0** oder **WLAN1** vorangestellt, die auf die zugeordnete Funkschnittstelle hinweist. **WLAN0** steht für **Radio 1** und **WLAN1** für **Radio 2**.

  Wenn der VAP konfiguriert ist, werden in der Tabelle die SSID, der administrative Status (aktiv oder nicht aktiv), die MAC-Adresse der Funkschnittstelle, die VLAN-ID, der Name eines zugeordneten Scheduler-Profils und der aktuelle Status (aktiv oder nicht aktiv) aufgeführt. 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.

Traffic Statistics

Auf der Seite **Traffic Statistics** 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 **Traffic Statistics** wählen Sie im Navigationsbereich die Option **Status and Statistics** > **Traffic Statistics** aus.

Auf der Seite **Traffic Statistics** werden zusammengefasste Daten und Statistiken für den Verkehr in beiden Richtungen angezeigt.

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

  Bei WAP561-Geräten sind dem Namen der VAP-Schnittstelle die Zeichenfolgen **WLAN0** und **WLAN1** vorangestellt, die auf die Funkschnittstelle hinweisen. (**WLAN0** steht für **Radio 1** und **WLAN1** für **Radio 2**.)

- **Total Packets**: Die Gesamtanzahl der von diesem WAP-Gerät gesendeten (in der Tabelle **Transmit**) oder empfangenen Pakete (in der Tabelle **Received**)

- **Total Bytes**: Die Gesamtanzahl der von diesem WAP-Gerät gesendeten (in der Tabelle **Transmit**) oder empfangenen Bytes (in der Tabelle **Received**)
- **Total Dropped Packets**: Die Gesamtanzahl der von diesem WAP-Gerät gelöschten gesendeten (in der Tabelle **Transmit**) oder empfangenen Pakete (in der Tabelle **Received**)
- **Total Dropped Bytes**: Die Gesamtanzahl der von diesem WAP-Gerät gelöschten gesendeten (in der Tabelle **Transmit**) oder empfangenen Bytes (in der Tabelle **Received**)
- **Errors**: Die Gesamtanzahl der Fehler beim Senden und Empfangen von Daten über dieses WAP-Gerät

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

WorkGroup Bridge Transmit/Receive

Auf der Seite **WorkGroup Bridge Transmit/Receive** 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 Transmit/Receive** wählen Sie im Navigationsbereich die Option **Status and Statistics** > **WorkGroup Bridge** aus.

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

- **Network Interface**: Der Name der Ethernet- oder VAP-Schnittstelle. Bei WAP561-Geräten steht **WLAN0** für **Radio 1** und **WLAN1** für **Radio 2**.
- **Status and Statistics**: 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:

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

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

Associated Clients

Auf der Seite **Associated Clients** können Sie die Clientstationen anzeigen, die einem bestimmten Access Point zugeordnet sind.

Zum Anzeigen der Seite **Associated Clients** wählen Sie im Navigationsbereich die Option **Status and Statistics** > **Associated Clients** aus.

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

- **Total Number of Associated Clients**: Die Gesamtanzahl der Clients, die zurzeit dem WAP-Gerät zugeordnet sind
- **Network Interface**: Der VAP, dem der Client zugeordnet ist. Bei WAP561-Geräten sind dem Namen der VAP-Schnittstelle die Zeichenfolgen **WLAN0** und **WLAN1** vorangestellt, die auf die Funkschnittstelle hinweisen. (**WLAN0** steht für **Radio 1** und **WLAN1** für **Radio 2**.)
- **Station**: Die MAC-Adresse des zugeordneten WLAN-Clients
- **Status**: Der Status **Authenticated and Associated** 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 **None** 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.

- **From Station/To Station**: Die Zähler für **From Station** geben die vom WLAN-Client empfangenen 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.
  - **Packets**: Die Anzahl der vom WLAN-Client empfangenen (gesendeten) Pakete
  - **Bytes**: Die Anzahl der vom WLAN-Client empfangenen (gesendeten) Bytes
  - **Drop Packets**: Die Anzahl der nach dem Empfang (nach dem Senden) gelöschten Pakete
  - **Drop Bytes**: Die Anzahl der nach dem Empfang (nach dem Senden) gelöschten Bytes
  - **TS Violate Packets (From 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 Violate Packets (To 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
- **Up Time**: 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 Client Associations

Auf der Seite **TSPEC Client Associations** werden Echtzeitinformationen zu den von diesem Access Point gesendeten und empfangenen TSPEC-Clientdaten angezeigt. In den Tabellen auf der Seite **TSPEC Client Associations** 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 die Option **Status and Statistics** > **TSPEC Client Associations** aus.

Auf der Seite **TSPEC Client Associations** werden die folgenden Informationen angezeigt:

Status und Statistik:

- **Network Interface**: Die vom Client verwendete Funkschnittstelle. Bei WAP561-Geräten steht **WLAN0** 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 Identifier**: Die ID der TSPEC-Verkehrssitzung (Bereich: 0 bis 7)
- **Access Category**: Die TS-Zugriffskategorie (Sprache oder Video)
- **Direction**: Die Verkehrsrichtung für diesen TS. Für **Direction** ist eine der folgenden Optionen möglich:
  - **uplink**: Vom Client zum Gerät
  - **downlink**: Vom Gerät zum Client
  - **bidirectional**

- **User Priority**: 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.
- **Medium Time**: Gibt an, wie lange der TS-Verkehr das Übertragungsmedium belegt.
- **Excess Usage Events**: Gibt an, wie oft der Client die für TSPEC festgelegte mittlere Zeit überschritten hat. Geringfügige seltene Verstöße werden ignoriert.
- **VAP MAC Address**: MAC-Adresse des virtuellen Access Points

Statistiken:

- **Network Interface**: Die vom Client verwendete Funkschnittstelle
- **Station**: Die MAC-Adresse der Clientstation
- **TS Identifier**: Die ID der TSPEC-Verkehrssitzung (Bereich: 0 bis 7)
- **Access Category**: Die TS-Zugriffskategorie (Sprache oder Video)
- **Direction**: Die Verkehrsrichtung für diesen TS. Für **Direction** ist eine der folgenden Optionen möglich:
  - **uplink**: Vom Client zum Gerät
  - **downlink**: Vom Gerät zum Client
  - **bidirectional**
- **From Station**: Zeigt die Anzahl der Pakete und Bytes an, die vom WLAN-Client empfangen wurden, sowie die Anzahl der Pakete und Bytes, die nach dem Empfang gelöscht wurden.
  - **Packets**: 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

- **To Station**: Die Anzahl der Pakete und Bytes, die vom WAP-Gerät an den WLAN-Client gesendet wurden, und die Anzahl der Pakete und Bytes die beim Senden gelöscht wurden
  - **Packets**: 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 den Bildschirm zu aktualisieren und die aktuellen Informationen anzuzeigen.

TSPEC Status and Statistics

Auf der Seite **TSPEC Status and Statistics** 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 die Option **Status and Statistics > TSPEC Status and Statistics** aus.

Auf der Seite **TSPEC Status and Statistics** werden die folgenden Statusinformationen für die WLAN-Schnittstellen (Funk) und VAP-Schnittstellen angezeigt:

- **Network Interface**: Der Name der Funkschnittstelle oder VAP-Schnittstelle. Bei WAP561-Geräten steht **WLAN0** für **Radio 1** und **WLAN1** für **Radio 2**.
- **Access Category**: 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.

- **Active Traffic Stream**: Die Anzahl der zurzeit aktiven TSPEC-Verkehrsströme für dieses Funkmodul und diese Zugriffskategorie
- **Traffic Stream Clients**: Die Anzahl der TS-Clients, die diesem Funkmodul und dieser Zugriffskategorie zugeordnet sind
- **Medium Time Admitted**: 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.
- **Medium Time Unallocated**: Die Zeit für die nicht verwendete Bandbreite für diese Zugriffskategorie

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

- **Access Category**: Die Zugriffskategorie, die diesem Verkehrsstrom zugeordnet ist (Sprache oder Video)
- **Total Packets**: Die Gesamtanzahl der von diesem Funkmodul gesendeten (in der Tabelle **Transmit**) oder empfangenen (in der Tabelle **Received**) TS-Pakete für die angegebene Zugriffskategorie
- **Total Bytes**: Die Gesamtanzahl der in der angegebenen Zugriffskategorie empfangenen Bytes

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

- **Total Voice Packets**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle **Transmit**) oder empfangenen (in der Tabelle **Received**) TS-Sprachpakete
- **Total Voice Bytes**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle **Transmit**) oder empfangenen (in der Tabelle **Received**) TS-Sprachbytes
- **Total Video Packets**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle **Transmit**) oder empfangenen (in der Tabelle **Received**) TS-Videopakete
- **Total Video Bytes**: Die Gesamtanzahl der von diesem WAP-Gerät für diesen VAP gesendeten (in der Tabelle **Transmit**) oder empfangenen (in der Tabelle **Received**) TS-Videobytes

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

TSPEC AP Statistics

Auf der Seite **TSPEC AP Statistics** werden Informationen zu den vom WAP-Gerät akzeptierten und abgelehnten Sprach- und Videoverkehrsströmen angezeigt. Zum Anzeigen der Seite **TSPEC AP Statistics** wählen Sie im Navigationsbereich die Option **Status and Statistics > TSPEC AP Statistics** aus.

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

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

Radio Statistics

Auf der Seite **Radio Statistics** können Sie Statistiken auf Paketebene und auf Byte-Ebene für einzelnen Funkschnittstellen anzeigen. Zum Anzeigen der Seite **Radio Statistics** wählen Sie im Navigationsbereich die Option **Status and Statistics > Radio Statistics** aus.

Beim WAP561-Gerät wählen Sie das Funkmodul aus, für das Sie Statistiken anzeigen möchten.

- **Packets Received**: Die Gesamtanzahl der vom WAP-Gerät empfangenen Pakete
- **Packets Transmitted**: Die Gesamtanzahl der vom WAP-Gerät gesendeten Pakete
- **Bytes Received**: Die Gesamtanzahl der vom WAP-Gerät empfangenen Bytes
- **Bytes Transmitted**: Die Gesamtanzahl der vom WAP-Gerät gesendeten Bytes

- **Packets Receive Dropped**: Die Anzahl der vom WAP-Gerät empfangenen Pakete, die gelöscht wurden
- **Packets Transmit Dropped**: Die Anzahl der vom WAP-Gerät gesendeten Pakete, die gelöscht wurden
- **Bytes Receive Dropped**: Die Anzahl der vom WAP-Gerät empfangenen Bytes, die gelöscht wurden
- **Bytes Transmit Dropped**: Die Anzahl der vom WAP-Gerät gesendeten Bytes, die gelöscht wurden
- **Fragments Received**: Die Anzahl der vom WAP-Gerät empfangenen fragmentierten Frames
- **Fragments Transmitted**: Die Anzahl der vom WAP-Gerät gesendeten fragmentierten Frames
- **Multicast Frames Received**: Die Anzahl der empfangenen MSDU-Frames, bei denen das Multicast-Bit in der MAC-Zieladresse festgelegt war
- **Multicast Frames Transmitted**: Die Anzahl der erfolgreich gesendeten MSDU-Frames, bei denen das Multicast-Bit in der MAC-Zieladresse festgelegt war
- **Duplicate Frame Count**: Gibt an, wie oft ein Frame empfangen wurde, bei dem aus dem Feld **Sequence Control** hervorging, dass es sich um ein Duplikat handelte.
- **Failed Transmit Count**: Gibt an, wie oft ein MSDU nicht erfolgreich gesendet wurde, da bei den Sendeversuchen der kurze oder lange Wiederholungsgrenzwert überschritten wurde.
- **FCS Error Count**: Die Anzahl der in einem empfangenen MPDU-Frame erkannten Fehler
- **Transmit Retry Count**: Gibt an, wie oft ein MSDU nach mindestens einer Wiederholung erfolgreich gesendet wurde.
- **ACK Failure Count**: Die Anzahl der ACK-Frames, die nicht wie erwartet empfangen wurden
- **RTS Failure Count**: Die Anzahl der CTS-Frames, die nicht als Antwort auf einen RTS-Frame empfangen wurden
- **WEP Undecryptable Count**: 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.

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

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

Email Alert Status

Auf der Seite **Email Alert Status** werden Informationen zu den E-Mail-Alarmen angezeigt, die basierend auf den im WAP-Gerät generierten Syslog-Nachrichten gesendet wurden. Zum Anzeigen der Seite **Email Alert Status** wählen Sie im Navigationsbereich die Option **Status and Statistics > Email Alert Status** aus.

- **Email Alert Status**: Der konfigurierte Status für E-Mail-Alarme. Als Status ist **Enabled** oder **Disabled** möglich. Standardmäßig ist **Disabled** festgelegt.
- **Number of Emails Sent**: Die Gesamtanzahl der gesendeten E-Mails. Möglich ist eine vorzeichenlose 32-Bit-Ganzzahl. Der Standardwert lautet **0**.
- **Number of Emails Failed**: Die Gesamtanzahl der E-Mail-Fehler. Möglich ist eine nicht signierte Ganzzahl mit 32 Bits. Der Standardwert lautet **0**.
- **Time Last Email Sent**: Tag, Datum und Uhrzeit der letzten gesendeten E-Mail

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

Log

Auf der Seite **Log** 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 **Log** wählen Sie im Navigationsbereich die Option **Status and Statistics > Log** aus.

- **Time Stamp**: Der Zeitpunkt, zu dem das Ereignis aufgetreten ist
- **Severity**: 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
- **Description**: Eine Beschreibung des Ereignisses

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

Sie können auf **Alle löschen** klicken, um alle Einträge aus dem Protokollieren zu löschen.

3

Verwaltung

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

Das Kapitel umfasst die folgenden Themen:

- **System Settings**
- **User Accounts**
- **Time Settings**
- **Log Settings**
- **E-Mail-Alarm**
- **HTTP/HTTPS Service**
- **Management Access Control**
- **Manage Firmware**
- **Download/Backup Configuration File**
- **Configuration Files Properties**
- **Copy/Save Configuration**
- **Reboot**
- **Discovery - Bonjour**
- **Paketerfassung**
- **Support Information**

System Settings

Auf der Seite **System Settings** können Sie Informationen konfigurieren, die das WAP-Gerät im Netzwerk identifizieren.

So konfigurieren Sie die Systemeinstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **System Settings** aus.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

- **Host Name**: 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 **switch** 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.
- **System Contact**: Eine Kontaktperson für das WAP-Gerät. Der Systemkontakt kann aus 0 bis 255 Zeichen bestehen und Leerzeichen und Sonderzeichen enthalten.
- **System Location**: 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.

User Accounts

Im WAP-Gerät ist standardmäßig ein Verwaltungsbenutzer konfiguriert.

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

Auf der Seite **User Accounts** können Sie bis zu vier zusätzliche Benutzer konfigurieren und Benutzerkennwörter ändern.

So fügen Sie einen neuen Benutzer hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **User Accounts** 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 **User Name** 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 **New Password** ein neues Kennwort mit 1 bis 64 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld **Confirm New Password** 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: Das 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.

So ändern Sie ein Benutzerkennwort:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **User Accounts** 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 **New Password** ein neues Kennwort mit 1 bis 64 Zeichen ein. Geben Sie dann das gleiche Kennwort in das Textfeld **Confirm New Password** 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: Das 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.

Time Settings

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. Das WAP-Gerät ist standardmäßig so konfiguriert, dass die Uhrzeit von NTP-Servern aus einer vordefinierten Liste bezogen wird.

Die aktuelle Systemzeit wird oben auf der Seite zusammen mit der Option **System Clock Source** angezeigt.

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

SCHRITT 1 Wählen Sie für das Feld **System Clock Source** die Option **Network Time Protocol (NTP)** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **NTP Server/IPv4/IPv6 Address Name**: 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.

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

SCHRITT 3 Wählen Sie **Adjust Time for Daylight Savings** aus, wenn die Sommerzeit für die Zeitzone gilt. Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die folgenden Felder:

- **Daylight Savings Start**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
- **Daylight Savings End**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitendes aus.
- **Daylight Savings Offset**: 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.

So konfigurieren Sie die Zeiteinstellungen manuell:

SCHRITT 1 Wählen Sie für das Feld **System Clock Source** die Option **Manually** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **System Date**: Wählen Sie in den Dropdownlisten das aktuelle Datum (Monat, Tag und Jahr) aus.
- **System Time**: Wählen Sie die aktuelle Uhrzeit (Stunden und Minuten) im 24-Stunden-Format aus, beispielsweise 22:00:00 Uhr.
- **Time Zone**: Wählen Sie die Zeitzone für den Standort aus.

SCHRITT 3 Wählen Sie **Adjust Time for Daylight Savings** aus, wenn die Sommerzeit für die Zeitzone gilt. Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die folgenden Felder:

- **Daylight Savings Start**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitbeginns aus.
- **Daylight Savings End**: Wählen Sie Woche, Tag, Monat und Uhrzeit des Sommerzeitendes aus.
- **Daylight Savings Offset**: 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.

Log Settings

Auf der Seite **Log Settings** können Sie das Speichern von Protokollnachrichten im permanenten Speicher aktivieren. Sie können Protokolle auch an einen Remotehost senden.

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

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

So konfigurieren Sie die dauerhafte Protokollierung:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Log Settings** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Persistence**: Klicken Sie auf **Enable**, 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.
- **Severity**: 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.
- **Depth**: 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.

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.

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

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Log Settings** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Remote Log**: Aktiviert das Senden von Protokollnachrichten vom WAP-Gerät an einen Remotehost. Wenn diese Option deaktiviert ist, bleiben alle Protokollnachrichten auf dem lokalen System.
- **Server IPv4/IPv6 Address/Name**: Die IPv4- bzw. IPv6-Adresse oder der Hostname des Remoteprotokollservers.

  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.
- **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 aktiviert 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 Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

E-Mail-Alarm

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.

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Email Alert** aus.

SCHRITT 2 Konfigurieren Sie im Bereich **Global Configuration** die folgenden Parameter:

- **Administrative Mode**: Wählen Sie diese Option aus, um die Funktion für E-Mail-Alarme global zu aktivieren.

- **From Email Address**: 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.
- **Log Duration**: 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.
- **Scheduled Message Severity**: 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: **None**, **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info** und **Debug**. Wenn Sie **None** festlegen, werden keine geplanten Schweregradnachrichten gesendet. Der Standardschweregrad lautet **Warning**.
- **Urgent Message Severity**: Protokollnachrichten mit diesem oder einem höheren Schweregrad werden sofort an die konfigurierte E-Mail-Adresse gesendet. Wählen Sie einen dieser Werte aus: **None**, **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info** und **Debug**. Wenn Sie **None** festlegen, werden keine dringenden Schweregradnachrichten gesendet. Der Standardwert lautet **Alert**.

SCHRITT 3 Konfigurieren Sie im Bereich **Mail Server Configuration** die folgenden Parameter:

- **Server IPv4 Address/Name**: 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.
- **Data Encryption**: 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.
- **Username**: 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.
- **Password**: Geben Sie das Kennwort für das E-Mail-Konto ein, das zum Senden dieser E-Mails verwendet werden soll. Das Kennwort kann 1 bis 64 Zeichen umfassen.

SCHRITT 4 Konfigurieren Sie die E-Mail-Adressen und die Betreffzeile.

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

Im folgenden Beispiel wird gezeigt, wie Sie die Parameter für **Mail Server Configuration** 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
```

```
Username: Ihre vollständige E-Mail-Adresse, beispielsweise
meinName@hotmail.com oder meinName@meineDomäne.com
Password: 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
Username: Ihre E-Mail-Adresse ohne den Domänennamen, beispielsweise meinName
(ohne @yahoo.com)
Password: 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
An: administrator@mailserver.com
Betreff: 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
```

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.

So konfigurieren Sie HTTP- und HTTP-Dienste:

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

SCHRITT 2 Konfigurieren Sie die folgenden globalen Einstellungen:

- **Maximum Sessions**: 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.

- **Session Timeout**: 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.
- **Redirect HTTP to HTTPS**: 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.

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 **Generate SSL Certificate**. Dies sollte geschehen, nachdem das WAP-Gerät eine IP-Adresse bezogen hat. Dadurch wird sichergestellt, dass der allgemeine Name für das Zertifikat der IP-Adresse für das WAP-Gerät 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:

- **Certificate File Present**
- **Certificate Expiration Date**
- **Certificate Issuer Common Name**

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 **Download SSL Certificate (From Device to PC)** die Option **HTTP** oder **TFTP** für **Download Method** aus, und klicken Sie auf **Download**.

- 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 **Upload SSL Certificate (From PC to Device)** die Option **HTTP** oder **TFTP** für **Upload Method** aus.

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

Nach dem erfolgreichen Upload wird eine Bestätigung angezeigt.

Management Access Control

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.

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.

Manage Firmware

Das WAP-Gerät enthält zwei Firmwareimages. 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 primäre Image und das sekundäre Image tauschen.

Wenn neue Versionen der Firmware für das WAP-Gerät zur Verfügung stehen, können Sie die Firmware der Geräte aktualisieren, um von neuen Funktionen und Verbesserungen zu profitieren. Das WAP-Gerät 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.

Austauschen des Firmware-Images

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.

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 für **Transfer Method** die Option **TFTP** aus.

SCHRITT 3 Geben Sie in das Feld **Source File Name** einen Namen (1 bis 256 Zeichen) für die Image-Datei ein. Der Name muss den Pfad des Verzeichnisses enthalten, in dem sich das hochzuladende Image befindet.

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

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

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * und zwei oder mehr aufeinander folgende 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.

So führen Sie das Upgrade über HTTP durch:

SCHRITT 1 Wählen Sie für **Transfer Method** die Option **HTTP** aus.

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.

Download/Backup Configuration File

Die Konfigurationsdateien für das WAP-Gerät liegen im XML-Format vor und enthalten alle Informationen zu den Einstellungen des WAP-Geräts. Sie können die Konfigurationsdateien auf einem Netzwerk-Host oder einem TFTP-Server sichern (hochladen), um den Inhalt manuell zu bearbeiten oder Sicherungen zu erstellen. 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 WAP-Gerät gespeichert:

- **Startkonfiguration**: Die im Flash-Speicher abgelegte Konfigurationsdatei.
- **Backupkonfiguration**: 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 Sie können die Dateien auch in andere Dateitypen im WAP-Gerät kopieren. Weitere Informationen hierzu finden Sie unter **Copy/Save Configuration**.

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Download/ Backup Configuration File** aus.

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

SCHRITT 3 Wählen Sie für **Save Action** die Option **Backup (AP to PC)** aus.

SCHRITT 4 Bei einer reinen TFTP-Sicherung geben Sie in **Destination File Name** 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 in **TFTP Server IPv4 Address** die IPv4-Adresse des TFTP-Servers ein.

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * und zwei oder mehr aufeinander folgende Punkte.

SCHRITT 5 Bei einer reinen TFTP-Sicherung geben Sie in **TFTP Server IPv4 Address** 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 das WAP-Gerät herunterladen, um die Konfiguration zu aktualisieren oder eine zuvor gesicherte Konfiguration im WAP-Gerät wiederherzustellen.

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Download/ Backup Configuration File** aus.

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

SCHRITT 3 Wählen Sie für **Save Action** die Option **Download (PC to AP)** aus.

SCHRITT 4 Bei einem reinen TFTP-Download geben Sie in **Source File Name** den Quelldateinamen mit der Erweiterung **.xml** ein. Geben Sie dabei auch den Pfad der Datei auf dem Server an. Geben Sie dann in **TFTP Server IPv4 Address** die IPv4-Adresse des TFTP-Servers ein.

Die folgenden Zeichen dürfen nicht im Dateinamen enthalten sein: Leerzeichen, <, >, |, \, : , (,), &, ; , #, ? , * und zwei oder mehr aufeinander folgende Punkte.

SCHRITT 5 Wählen Sie die Konfigurationsdatei im WAP-Gerät 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 WAP-Geräts 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 das WAP-Gerät 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.

Configuration Files Properties

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 WAP-Geräts aktiv.

So löschen Sie die Startkonfigurationsdatei oder die Backup-Konfigurationsdatei:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Configuration Files Properties** aus.

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

SCHRITT 3 Klicken Sie auf **Clear Files**.

Copy/Save Configuration

Auf der Seite **Copy/Save Configuration** können Sie Dateien innerhalb des Dateisystems im WAP-Gerät kopieren. Sie können beispielsweise die Backup-Konfigurationsdatei in die Startkonfigurationsdatei kopieren, damit sie beim nächsten Start des WAP-Geräts verwendet wird.

So kopieren Sie eine Datei in einen anderen Dateityp:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Copy/Save Configuration** 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 **Destination File Name** 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.

Reboot

Über die Seite **Reboot** können Sie das WAP-Gerät neu starten.

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

SCHRITT 2 Wählen Sie eine der folgenden Optionen aus:

- **Reboot**: Das WAP-Gerät wird mit der Startkonfiguration neu gestartet.
- **Reboot to Factory Default**: 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 WAP-Geräts 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.

Das WAP-Gerät 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 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. So ändern Sie den administrativen Status:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Administration** > **Discovery - Bonjour** aus.

SCHRITT 2 Klicken Sie auf **Enable**, um Bonjour zu aktivieren, oder heben Sie die Auswahl von **Enable** auf, 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. Die Datei kann vom WAP-Gerät an einen TFTP-Server übertragen werden. 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.

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.

Klicken Sie auf **Administration > Packet Capture**, um die Seite **Packet Capture** 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 **Packet Capture Configuration** können Sie Parameter konfigurieren und eine Paketerfassung initiieren.

So konfigurieren Sie die Paketerfassungseinstellungen:

SCHRITT 1 Konfigurieren Sie die folgenden Parameter:

- **Capture Beacons**: Aktiviert oder deaktiviert die Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder gesendet wurden.

- **Promiscuous Capture**: 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.

- **Radio Client Filter**: 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.

- **Client Filter MAC Address**: 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.

- **Packet Capture Method**: Wählen Sie eine der folgenden Optionen aus:

  - **Local File**: 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.

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.

So initiieren Sie eine lokale Paketerfassung:

SCHRITT 1 Stellen Sie sicher, dass für **Packet Capture Method** die Option **Local File** ausgewählt ist.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Capture Interface**: Geben Sie einen Erfassungsschnittstellentyp für die Paketerfassung ein:
  - **radio1**: 802.11-Verkehr an der Funkschnittstelle Radio 1
  - **radio2**: 802.11-Verkehr an **Radio 2** (nur WAP561)
  - **eth0**: 802.3-Verkehr am Ethernet-Anschluss
  - **VAP0** oder **WLAN0:VAP0**: VAP0-Verkehr. Beim WAP561 wird **WLAN0:VAP0** angezeigt. Dabei steht **WLAN0** für **Radio 1**.
  - **WLAN1:VAP0**: VAP0-Verkehr an **Radio 2** (nur für WAP561-Geräte)
  - **VAP1** bis **VAP15**, falls konfiguriert: Verkehr am angegebenen VAP. Beim WAP561 wird den Schnittstellennamen die Zeichenfolge **WLAN0:** oder **WLAN1:** vorangestellt. Dabei steht **WLAN0** für **Radio 1** und **WLAN1** für **Radio 2**.
  - **brtrunk**: Linux-Bridge-Schnittstelle im WAP-Gerät
- **Capture Duration**: Geben Sie die Dauer der Erfassung in Sekunden ein. Möglich sind Werte im Bereich von 10 bis 3600. Der Standardwert lautet **60**.
- **Max Capture File Size**: Geben Sie die maximal zulässige Größe für die Erfassungsdatei in KB ein. Möglich sind Werte im Bereich von 64 bis 4096. Der Standardwert lautet **1024**.

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

SCHRITT 4 Klicken Sie auf **Start Capture**.

Im Modus **Packet File Capture** 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.

- **Current Capture Status**: Gibt an, ob die Paketerfassung ausgeführt wird oder beendet wurde.
- **Packet Capture Time**: Die verstrichene Dauer der Erfassung
- **Packet Capture File Size**: Die aktuelle Größe der Erfassungsdatei

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

HINWEIS Zum Beenden einer Paketdateierfassung klicken Sie auf **Stop Capture**.

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.

So initiieren Sie eine Remoteerfassung in einem WAP-Gerät:

SCHRITT 1 Klicken Sie auf **Administration** > **Packet Capture**.

SCHRITT 2 Aktivieren Sie die Option **Promiscuous Capture**.

SCHRITT 3 Wählen Sie für **Packet Capture Method** die Option **Remote** aus.

SCHRITT 4 Verwenden Sie für **Remote Capture Port** 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 **Start Capture**.

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 **Capture** > **Options** aus. Daraufhin wird ein Popup-Fenster angezeigt.

SCHRITT 3 Wählen Sie für **Interface** die Option **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 auf Funk 1
`-- rpcap://[192.168.1.220]:2002/wlan0`
802.11-Verkehr
`-- rpcap://[192.168.1.220]:2002/Funk1`
Bei WAP561, VAP1 ~ VAP7-Verkehr
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
Bei WAP561, VAP1 ~ VAP3-Verkehr
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3`

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. Beim Auslösen des Befehls zum Herunterladen einer Paketerfassungsdatei wird die Erfassung automatisch beendet.

Da sich die Erfassungsdatei im RAM-Dateisystem befindet, wird sie beim Zurücksetzen des WAP-Geräts gelöscht.

So laden Sie eine Paketerfassungsdatei über TFTP herunter:

SCHRITT 1 Wählen Sie **Use TFTP** zum Herunterladen der Erfassungsdatei.

SCHRITT 2 Geben Sie in **TFTP Server Filename** den Dateinamen auf dem TFTP-Server ein, 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 **TFTP Server IPv4 Address** eine IPv4-Adresse eines TFTP-Servers ein.

SCHRITT 4 Klicken Sie auf **Download**.

So laden Sie eine Paketerfassungsdatei über HTTP herunter:

SCHRITT 1 Heben Sie die Auswahl von **Use TFTP** zum Herunterladen der Erfassungsdatei auf.

SCHRITT 2 Klicken Sie auf **Download**. 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.

Support Information

Auf der Seite **Support Information** 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 **Administration > Support Information** aus, um die Seite **Support Information** 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.

4

LAN

In diesem Kapitel wird beschrieben, wie Sie die Anschluss-, Netzwerk- und Uhrzeiteinstellungen der WAP-Geräte konfigurieren.

Das Kapitel enthält die folgenden Themen:

- **Port Settings**
- **VLAN and IPv4 Address Settings**
- **IPv6 Addresses**
- **IPv6-Tunnel**

Port Settings

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

So können Sie LAN-Einstellungen anzeigen und konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **LAN** > **Port Settings** aus.

Im Bereich **Operational Status** werden der Typ und die Verbindungsmerkmale des LAN-Anschlusses gemäß der Konfiguration im Bereich **Administrative Settings** angezeigt. Wenn die Einstellungen durch Konfiguration oder automatische Aushandlung geändert werden, können Sie auf **Aktualisieren** klicken, um die neuesten Einstellungen anzuzeigen.

SCHRITT 2 Aktivieren oder deaktivieren Sie die Option **Auto Negotiation**.

- 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 Anschlussgeschwindigkeit und den Duplexmodus manuell konfigurieren.

SCHRITT 3 Wenn die automatische Aushandlung deaktiviert ist, wählen Sie in **Port Speed** eine Anschlussgeschwindigkeit (10/100/1000 MB/s) und den Duplexmodus (Halb- oder Vollduplex) aus.

SCHRITT 4 Aktivieren oder deaktivieren Sie die Option **Green Ethernet Mode**. Wenn diese Option aktiviert ist, wechselt das WAP-Gerät automatisch in einen Energiesparmodus, wenn in der Leitung keine Energie vorhanden ist, und nimmt den Normalbetrieb wieder auf, wenn Energie erkannt wird.

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

VLAN and IPv4 Address Settings

Auf der Seite **VLAN and IPv4 Address Settings** können Sie Einstellungen für die LAN-Schnittstelle konfigurieren, einschließlich der Zuweisung statischer oder dynamischer IPv4-Adressen.

So konfigurieren Sie LAN-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **LAN** > **VLAN and IPv4 Address** aus.

Auf der Seite werden die Optionen **Global Settings** und **IPv4 Settings** angezeigt. Im Bereich **Global Settings** wird die MAC-Adresse des Anschlusses der LAN-Schnittstelle angezeigt. Dieses Feld ist schreibgeschützt.

SCHRITT 2 Konfigurieren Sie die folgenden globalen Einstellungen:

- **Untagged VLAN**: Aktiviert oder deaktiviert VLAN-Tagging. Wenn die Option aktiviert ist (Standardeinstellung), wird der gesamte Verkehr mit einer VLAN-ID versehen.

  Standardmäßig wird für den gesamten Verkehr des Access Points VLAN 1, das Standard-VLAN ohne Tag, verwendet. Dies bedeutet, dass der gesamte Verkehr erst mit einem Tag versehen wird, wenn Sie das VLAN ohne Tag deaktivieren, die VLAN-ID für Verkehr ohne Tag ändern oder die VLAN-ID für einen VAP oder Client, der RADIUS verwendet, ändern.

- **Untagged VLAN ID**: Gibt eine Zahl zwischen 1 und 4094 für die VLAN-ID ohne Tag an. Der Standardwert lautet **1**. Der Verkehr in dem in diesem Feld angegebenen VLAN wird bei der Weiterleitung an das Netzwerk nicht mit einer VLAN-ID versehen.

  VLAN 1 ist das Standard-VLAN ohne Tag und das Standardverwaltungs-VLAN. Wenn Sie den Verwaltungsverkehr vom VLAN-Verkehr ohne Tag trennen möchten, konfigurieren Sie die neue VLAN-ID im Router, und verwenden Sie dann diese neue VLAN-ID im WAP-Gerät.

- **Management VLAN ID**: Das VLAN, das der für den Zugriff auf das WAP-Gerät verwendeten IP-Adresse zugeordnet ist. Geben Sie als Verwaltungs-VLAN-ID eine Zahl zwischen 1 und 4094 an. Der Standardwert lautet **1**.

  Dieses VLAN ist außerdem das Standard-VLAN ohne Tag. Wenn im Netzwerk bereits ein Verwaltungs-VLAN mit einer anderen VLAN-ID konfiguriert ist, müssen Sie die VLAN-ID des Verwaltungs-VLANs im WAP-Gerät ändern.

SCHRITT 3 Konfigurieren Sie die folgenden IPv4-Einstellungen:

- **Connection Type**: Standardmäßig sendet der DHCP-Client im Cisco Access Point WAP551 und WAP561 automatisch Anfragen für 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 in der Liste einen der folgenden Werte aus:

  - **DHCP**: Das WAP-Gerät bezieht seine IP-Adresse von einem DHCP-Server im LAN.
  - **Static IP**: Sie konfigurieren die IPv4-Adresse manuell. Geben Sie die IPv4-Adresse im Format xxx.xxx.xxx.xxx (192.0.2.10) ein.

- **Static IP Address, Subnet Mask, and Default Gateway**: Wenn Sie die Zuweisung einer statischen IP-Adresse ausgewählt haben, geben Sie die IP-Informationen ein.

- **Domain Name Servers**: Wählen Sie in der Liste eine Option aus:

  - **Dynamic**: Das WAP-Gerät bezieht DNS-Serveradressen von einem DHCP-Server im LAN.
  - **Manual**: Sie konfigurieren manuell eine oder mehrere DNS-Serveradressen. Geben Sie bis zu zwei IP-Adressen in die Textfelder ein.

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

HINWEIS Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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 Addresses

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

So konfigurieren Sie IPv6-Adresseinstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **LAN** > **IPv6 Addresses** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

- **IPv6 Connection Type**: Wählen Sie aus, auf welche Weise das WAP-Gerät eine IPv6-Adresse bezieht:
  - **DHCPv6**: Die IPv6-Adresse wird von einem DHCPv6-Server zugewiesen.
  - **Static IPv6**: Sie konfigurieren die IPv6-Adresse manuell. Geben Sie die IPv6-Adresse im Format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91) ein.
- **IPv6 Administration Mode**: Aktiviert den IPv6-Verwaltungszugriff.
- **IPv6 Auto Configuration Administration Mode**: 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.
- **Static IPv6 Address**: 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**.
- **Static IPv6 Address Status**: Einer der folgenden Werte wird angezeigt:
  - **Operational**: Die Eindeutigkeit der IP-Adresse im LAN wurde überprüft. Die IP-Adresse kann an der Schnittstelle verwendet werden.
  - **Tentative**: Das WAP-Gerät initiiert den Erkennungsprozess für automatische 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.
- **IPv6 Autoconfigured Global Addresses**: Wenn dem WAP-Gerät automatisch eine oder mehrere IPv6-Adressen zugewiesen wurde, werden die Adressen aufgeführt.
- **IPv6 Link Local Address**: 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.
- **Default IPv6 Gateway**: Das statisch konfigurierte Standard-IPv6-Gateway
- **IPv6 DNS Nameservers**: Wählen Sie einen der folgenden Werte aus:
  - **Dynamic**: Die DNS-Nameserver werden dynamisch über DHCPv6 vermittelt.
  - **Manual**: Sie geben bis zu zwei IPv6-DNS-Nameserver in die entsprechenden Felder ein.

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

HINWEIS Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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 WAP551- und WAP561-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 die Option **LAN** > **IPv6 Tunnel** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **ISATAP Status**: Aktiviert oder deaktiviert den administrativen ISATAP-Modus im WAP-Gerät.
- **ISATAP Capable Host**: Die IP-Adresse oder der DNS-Name des ISATAP-Routers. Der Standardwert lautet **isatap**.
- **ISATAP Query Interval**: Gibt an, wie oft das WAP-Gerät 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.

- **ISATAP Solicitation Interval**: Gibt an, wie oft das WAP-Gerät Routeranfragenachrichten an die ISATAP-Router senden soll, von denen es durch die DNS-Abfragenachrichten erfährt. Das WAP-Gerät sendet nur dann Routeranfragenachrichten, wenn kein aktiver ISATAP-Router vorhanden ist. Gültig sind Werte im Bereich von 120 bis 3600 Sekunden.

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

Wenn der Tunnel aufgebaut ist, werden auf der Seite die Optionen **ISATAP IPv6 Link Local Address** und **ISATAP IPv6 Global Address** angezeigt. Dabei handelt es sich um die virtuellen IPv6-Schnittstellenadressen für das IPv4-Netzwerk.

5

WLAN

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

Das Kapitel enthält die folgenden Themen:

- **Funk**
- **Rogue-AP-Erkennung**
- **Netzwerke**
- **Planungsmodul**
- **Planungsverweis**
- **Bandwidth Utilization**
- **MAC-Filterung**
- **WDS-Bridge**
- **WorkGroup Bridge**
- **Quality of Service**
- **WPS-Einrichtung**
- **WPS Process**

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.

So konfigurieren Sie die Funkeinstellungen:

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

SCHRITT 2 Konfigurieren Sie im Bereich **Global Settings** den Wert für **TSPEC Violation Interval**. Dabei handelt es sich um das Zeitintervall in Sekunden, in dem das WAP-Gerät zugeordnete Clients meldet, die die obligatorischen Verfahren für die Zugangskontrolle nicht einhalten. Die Berichterstattung erfolgt über das Systemprotokoll und über SNMP-Traps. Geben Sie einen Zeitraum zwischen 0 und 900 Sekunden ein. Der Standardwert beträgt 300 Sekunden.

SCHRITT 3 Bei WAP561-Geräten wählen Sie in **Radio** die zu konfigurierende Funkschnittstelle aus (**Radio 1** oder **Radio 2**).

SCHRITT 4 Konfigurieren Sie im Bereich **Basic Settings** die folgenden Einstellungen:

HINWEIS Bestimmte Funkmodi dürfen möglicherweise aufgrund lokaler Bestimmungen nicht verwendet werden. Nicht alle Modi sind in allen Ländern verfügbar. Außerdem unterstützt **Radio 1** beim WAP561 mit zwei Funkmodulen das 2,4-GHz-Band (Standardauswahl) oder das 5-GHz-Band, während **Radio 2** nur das 5-GHz-Band unterstützt. Das Einzelfunkfeld des WAP551-Geräts unterstützt beide Bänder.

- **Radio**: Aktiviert oder deaktiviert die Funkschnittstelle. Das Funkmodul ist standardmäßig deaktiviert.
- **MAC Address**: Die MAC-Adresse (Hardwareadresse) der Schnittstelle. Die MAC-Adresse wird vom Hersteller zugewiesen und kann nicht geändert werden.
- **Mode**: Der vom Funkmodul verwendete IEEE 802.11-Standard und die verwendete Frequenz. Für jedes Funkmodul wählen Sie einen der verfügbaren Modi aus:
  - 802.11a: Nur 802.11a-Clients können eine Verbindung mit dem WAP-Gerät herstellen.
  - 802.11b/g-802.11b- und 802.11g-Clients können eine Verbindung mit dem WAP-Gerät herstellen.
  - 802.11a/n-802.11a- und 802.11n-Clients mit 5-GHz-Frequenz können eine Verbindung mit dem WAP-Gerät herstellen.
  - 802.11b/g/n (default)-802.11b-, 802.11g- und 802.11n-Clients mit 2,4-GHz-Frequenz können eine Verbindung mit dem WAP-Gerät herstellen.
  - 5 GHz 802.11n: Nur 802.11n-Clients mit 5-GHz-Frequenz können eine Verbindung mit dem WAP-Gerät herstellen.

- 2.4 GHz 802.11n: Nur 802.11n-Clients mit 2,4-GHz-Frequenz können eine Verbindung mit dem WAP-Gerät herstellen.

- **Channel Bandwidth**: Die 802.11n-Spezifikation lässt einen gleichzeitig vorhandenen 20/40-MHz-Kanal zusätzlich zu dem in anderen Modi verfügbaren älteren 20-MHz-Kanal zu. Der 20/40-MHz-Kanal ermöglicht höhere Datenraten, jedoch bleiben weniger Kanäle zur Verwendung durch andere 2,4-GHz- und 5-GHz-Geräte übrig.

  Wenn der Funkmodus 802.11n einschließt, wird die Kanalbandbreite standardmäßig auf 20/40 MHz festgelegt, um beide Kanalbreiten zu aktivieren. Legen Sie das Feld auf 20 MHz fest, um die Verwendung der Kanalbandbreite auf einen 20-MHz-Kanal zu beschränken.

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

  Wählen Sie eine der folgenden Optionen aus:

  - **Upper**: Legt den primären Kanal als oberen 20-MHz-Kanal im 40-MHz-Band fest.

  - **Lower**: Legt den primären Kanal als unteren 20-MHz-Kanal im 40-MHz-Band fest. Die Standardauswahl lautet **Lower**.

- **Channel**: Der Teil des Funkspektrums, den das Funkmodul zum Senden und Empfangen verwendet

  Der Bereich der verfügbaren Kanäle hängt vom Modus der Funkschnittstelle und von der Einstellung für den Ländercode ab. Wenn Sie die Kanaleinstellung **Auto** auswählen, sucht das WAP-Gerät nach verfügbaren Kanälen und wählt den Kanal aus, in dem die niedrigste Verkehrsmenge 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.

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

- **Short Guard Interval Supported**: Dieses Feld ist nur verfügbar, wenn der ausgewählte Funkmodus 802.11n einschließt.

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 Guard Interval von den für a und g definierten 800 Nanosekunden auf 400 Nanosekunden reduziert werden. Durch die Reduzierung des Guard Intervals 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:

- **Yes**: Das WAP-Gerät sendet Daten bei der Kommunikation mit Clients, die das kurze Guard Interval ebenfalls unterstützen, mit einem Guard Interval von 400 Nanosekunden. Die Standardauswahl lautet **Yes**.
- **No**: Das WAP-Gerät sendet Daten mit einem Guard Interval von 800 Nanosekunden.

- **Protection**: Die Schutzfunktion enthält Regeln, die garantieren sollen, 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 Interval**: 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 zwischen 20 und 2000 Millisekunden ein. Das Standardintervall beträgt 100 Millisekunden.

- **DTIM Period**: Der Zeitraum für DTIM-Nachrichten (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.

- **Fragmentation Threshold**: Die Schwelle für die Frame-Größe in Bytes. 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.

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 Threshold**: Der Wert für den RTS-Schwellenwert (Request to Send). Gültig ist eine Ganzzahl im Bereich von 0 bis 2347. Der Standardwert lautet **2347 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.

- **Maximum Associated Clients**: Die maximale Anzahl der Stationen, die gleichzeitig auf die einzelnen Funkmodule dieses WAP-Geräts zugreifen können. Sie können eine Ganzzahl zwischen 0 und 200 eingeben. Der Standardwert lautet **200 Stationen**. Daher kann das WAP551-Gerät mit einem einzigen Funkmodul bis zu 200 Clients unterstützen, während das WAP561-Gerät mit Doppelfunkfeld ingesamt bis zu 400 Clients unterstützen kann.

- **Transmit Power**: Ein Prozentwert für die Sendeleistung dieses WAP-Geräts.

  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 Sendeleistung auf die niedrigeren Bereiche (beispielsweise 25 % oder 12 %) festzulegen, geht die Sendeleistung möglicherweise nicht wie erwartet zurück, da für bestimmte Verstärker eine Mindestsendeleistung erforderlich ist.

- **Fixed 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.

  Wenn **Auto** ausgewählt ist, wählt das WAP-Gerät die beste Rate für die zugeordneten Clients aus. Der Bereich der gültigen Werte hängt vom konfigurierten Funkmodus ab.

- **Legacy Rate Sets**: Raten werden in Megabit pro Sekunde 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.

- **MCS (Data Rate) Settings**: Die vom WAP-Gerät angekündigten MCS-Indexwerte (Modulation and Coding Scheme). Mit MCS können Sie den Durchsatz für 802.11n-WLAN-Clients verbessern.

  Aktivieren Sie das Kontrollkästchen unter der MCS-Indexnummer, um den Index zu aktivieren. Sie können nicht alle Indizes gleichzeitig deaktivieren.

  Das WAP-Gerät unterstützt die MCS-Indizes 0 bis 23. Der MSC-Index 23 ermöglicht eine maximale Übertragungsrate von 450 MBit/s. Wenn kein MCS-Index ausgewählt ist, wird das Funkmodul mit MCS-Index 0 betrieben, der eine maximale Übertragungsrate von 15 MBit/s ermöglicht.

  Die MCS-Einstellungen können Sie nur konfigurieren, wenn der Funkmodus Unterstützung für 802.11n umfasst.

- **Broadcast/Multicast Rate Limiting**: 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:

  - **Rate Limit**: Die Ratenbegrenzung für Multicast- und Broadcast-Verkehr. Die Begrenzung sollte größer als 1, jedoch kleiner als 50 Pakete pro Sekunde sein. Verkehr unterhalb dieser Ratenbegrenzung ist immer konform und wird an das entsprechende Ziel gesendet. Die Einstellung für die Standardratenbegrenzung und die maximale Ratenbegrenzung entspricht 50 Paketen pro Sekunde.

  - **Rate Limit 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 Mode**: Regelt den allgemeinen TSPEC-Modus für das WAP-Gerät. Standardmäßig ist der TSPEC-Modus deaktiviert. Folgende Optionen sind möglich:

  - **On**: Das WAP-Gerät behandelt TSPEC-Anfragen gemäß den TSPEC-Einstellungen, die Sie auf der Seite **Radio** konfigurieren. Verwenden Sie diese Einstellung, wenn das WAP-Gerät Verkehr von QoS-fähigen Geräten wie beispielsweise Wi-Fi-zertifizierten Telefonen verarbeitet.

  - **Off**: 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 Voice ACM Mode**: Regelt die obligatorische Zugangskontrolle (ACM) für die Zugriffskategorie **Sprachdaten**. Standardmäßig ist der TSPEC Voice ACM-Modus deaktiviert. Folgende Optionen sind möglich:

  - **On**: 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.

  - **Off**: 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 Voice ACM Limit**: 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 Video ACM Mode**: Regelt die obligatorische Zugangskontrolle für die Zugriffskategorie **Video**. Standardmäßig ist der TSPEC Video ACM-Modus deaktiviert. Folgende Optionen sind möglich:
  - **On**: 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.
  - **Off**: 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 Video ACM Limit**: 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 AP Inactivity Timeout**: 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 Station Inactivity Timeout**: 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 Legacy WMM Queue Map Mode**: Aktiviert oder deaktiviert die Mischung von älterem Verkehr in Warteschlangen im ACM-Betrieb. Standardmäßig ist dieser Modus deaktiviert.

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

VORSICHT Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

Rogue-AP-Erkennung

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

Das WAP-Gerät 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.

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

Sie können die Rogue-AP-Erkennung aktivieren und deaktivieren. Zum Aktivieren der Sammlung von Informationen zu Rogue-APs durch das Funkmodul klicken Sie auf **Enable** neben **AP Detection** für **Radio 1** (oder **Radio 2** bei WAP561-Geräten) und dann auf **Speichern**.

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.

- **Action**: Wenn der AP in **Detected Rogue AP List** enthalten ist, können Sie auf **Trust** klicken, um den AP in **Trusted AP List** zu verschieben.

Wenn der AP in **Trusted AP List** enthalten ist, können Sie auf **Untrust** klicken, um den AP in **Detected AP List** zu verschieben.

HINWEIS **Detected Rogue AP List** und **Trusted AP List** enthalten Informationen. Das WAP-Gerät hat keine Kontrolle über APs in der Liste und kann auf die beim RF-Scan erkannten APs keine Sicherheitsrichtlinien anwenden.

- **MAC Address**: Die MAC-Adresse des Rogue-APs
- **Beacon Interval**: Das vom Rogue-AP verwendete Beacon-Intervall

  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.
- **Type**: 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.
- **Privacy**: 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 802.11a oder 802.11n (oder beide Modi).
- **Channel**: 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.
- **Rate**: Die Rate (in Megabit pro Sekunde), mit der der Rogue-AP zurzeit sendet

  Bei der aktuellen Rate handelt es sich immer eine der unter **Supported Rates** angezeigten Raten.
- **Signal**: Die Stärke des von dem Rogue-AP ausgehenden Funksignals. Wenn Sie den Mauszeiger über die Balken bewegen, wird eine Zahl angezeigt, die die Stärke in Dezibel (dB) angibt.
- **Beacons**: Die Gesamtanzahl der Beacons, die seit der Erkennung des Rogue-APs von diesem empfangen wurden
- **Last Beacon**: Datum und Uhrzeit des Zeitpunkts, zu dem der letzte Beacon vom Rogue-AP empfangen wurde
- **Rates**: 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**.

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

SCHRITT 1 Klicken Sie in **Detected Rogue AP List** neben den Ihnen bekannten APs auf **Trust**. Die vertrauenswürdigen APs werden in **Trusted AP List** verschoben.

SCHRITT 2 Wählen Sie im Bereich **Download/Backup Trusted AP List** die Option **Backup (AP to 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.

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 **Download/Backup Trusted AP List** die Option **Download (PC to AP)** aus.

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 **Replace** aus, um die Liste zu importieren und den Inhalt von **Known AP List** zu ersetzen.

b. Wählen Sie **Merge** aus, um die Liste zu importieren und die APs in der importierten Datei den zurzeit in **Known AP List** 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. Das WAP-Gerät 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.

Die Standard-SSID für VAP0 lautet **ciscosb**. Jeder zusätzlich erstellte VAP hat einen leeren SSID-Namen. Sie können die SSIDs aller VAPs mit anderen Werten konfigurieren.

Die SSID kann ein beliebiger alphanumerischer Wert aus 2 bis 32 Zeichen sein, bei dem zwischen Groß- und Kleinschreibung unterschieden wird. Zulässig sind druckbare Zeichen sowie Leerzeichen (ASCII 0x20). Die folgenden sechs Zeichen sind jedoch nicht zulässig:

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

Die folgenden Zeichen sind zulässig:

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

Außerdem können Sie die folgenden drei Zeichen nicht als erstes Zeichen verwenden:

!, # und ; (ASCII 0x21, 0x23 bzw. 0x3B).

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.

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. Die Geräte WAP551 und WAP561 unterstützen 17 aktive VLANs (16 für WLAN plus ein Verwaltungs-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.

So konfigurieren Sie VAPs:

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

SCHRITT 2 Bei WAP561-Geräten wählen Sie unter **Radio** die Funkschnittstelle aus, für die Sie VAPs konfigurieren möchten (**Radio 1** oder **Radio 2**).

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **Enabled** 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 folgenden 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 einem 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 and IPv4 Address Settings**.

- **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.

- **Broadcast SSID**: 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.

- **Security**: Der Typ der für den Zugriff auf den VAP erforderlichen Authentifizierung:
  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal

- WPA Enterprise

Wenn Sie einen anderen Sicherheitsmodus als **None** auswählen, werden zusätzliche Felder angezeigt.

HINWEIS 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 Filtering**: Gibt an, ob die Stationen, die auf diesen VAP zugreifen können, auf eine konfigurierte globale Liste von MAC-Adressen beschränkt sind. Sie können für die MAC-Filterung die folgenden Typen auswählen:
  - **Disabled**: Die MAC-Filterung wird nicht verwendet.
  - **Local**: Die auf der Seite **MAC-Filterung** konfigurierte MAC-Authentifizierungsliste wird verwendet.
  - **RADIUS**: Die MAC-Authentifizierungsliste auf einem externen RADIUS-Server wird verwendet.
- **Channel Isolation**: 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.

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

VORSICHT Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

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.

In diesen Abschnitten werden die Sicherheitseinstellungen beschrieben, die Sie abhängig von der Auswahl in der Liste **Security** auf der Seite **Networks** konfigurieren.

Wenn Sie den Sicherheitsmodus **None** auswählen, können Sie keine zusätzlichen Sicherheitseinstellungen für das WAP-Gerät konfigurieren. In diesem Modus werden die zum und vom WAP-Gerät übertragenen Daten nicht verschlüsselt. Dieser Sicherheitsmodus kann bei der anfänglichen Netzwerkkonfiguration oder bei der Problembehandlung hilfreich sein. Für die reguläre Verwendung im internen Netzwerk wird der Modus jedoch nicht empfohlen, da er nicht sicher ist.

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 128-Bit-Pre-Shared-Key (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:

- **Transfer Key Index**: Eine Liste der Schlüsselindizes. Zur Verfügung stehen die Schlüsselindizes 1 bis 4. Der Standardwert lautet **1**.

  Aus dem **Transfer Key Index** geht hervor, welchen WEP-Schlüssel das WAP-Gerät zum Verschlüsseln der übertragenen Daten verwendet.

- **Key Length**: Die Länge des Schlüssels. Wählen Sie eine Option aus:
  - 64 Bit
  - 128 Bit
- **Key Type**: Der Schlüsseltyp. Wählen Sie eine Option aus:
  - ASCII
  - Hex
- **WEP Keys**: 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.
- **Characters Required**: 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 Authentication**: 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:
  - **Open 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.

- **Shared Key**: Bei dieser Authentifizierung benötigt die Clientstation den richtigen WEP-Schlüssel, damit sie dem WAP-Gerät zugeordnet werden kann. Wenn der Authentifizierungsalgorithmus **Shared Key** festgelegt ist, kann eine Station mit einem falschen WEP-Schlüssel nicht mit dem WAP-Gerät verbunden werden.
- **Open System** und **Shared Key**: 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.

Wenn Sie **Static WEP** verwenden, gelten die folgenden Regeln:

- Die WLAN-Sicherheit aller Clientstationen muss auf WEP festgelegt sein, und alle Clients benötigen zum Decodieren der Übertragungen vom AP zur Station einen der im WAP angegebenen WEP-Schlüssel.
- Das WAP-Gerät benötigt zum Dekodieren der Übertragungen von Stationen alle Schlüssel, die von Clients für Übertragungen von der Station zum AP verwendet werden.
- Der gleiche Schlüssel muss sich in allen Knoten (AP und Clients) an der gleichen Position befinden. Wenn beispielsweise für das WAP-Gerät der Schlüssel **abc123** als WEP-Schlüssel 3 definiert ist, muss die gleiche Zeichenfolge für die Clientstationen als WEP-Schlüssel 3 definiert sein.
- 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 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:

- **Use Global RADIUS Server Settings**: 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 Address Type**: Die vom RADIUS-Server verwendete IP-Version.

  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 Address 1** oder **Server IPv6 Address 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 Address 2** bis **4** oder **Server IPv6 Address 2** bis **4**: Bis zu drei IPv4- oder IPv6-Adressen für RADIUS-Backup-Server.

  Wenn die Authentifizierung beim primären Server fehlschlägt, wird der Vorgang nacheinander mit den konfigurierten Backup-Servern wiederholt.

- **Key**: Der hinterlegte 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 mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Der eingegebene Text wird in Form von Sternchen angezeigt.

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

- **Enable RADIUS Accounting**: Ermöglicht das Verfolgen und Messen der von einem bestimmten Benutzer verwendeten Ressourcen, beispielsweise Systemzeit, Menge der gesendeten und empfangenen Daten usw.

  Wenn Sie RADIUS Accounting aktivieren, gilt dies für den primären RADIUS-Server und alle Backup-Server.

- **Active 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.
- **Broadcast Key Refresh Rate**: 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.
- **Session Key Refresh Rate**: Das Intervall, in dem das WAP-Gerät Sitzungsschüssel (Unicast) für die einzelnen dem VAP zugeordneten Clients aktualisiert

  Gültig sind Werte im Bereich von 0 bis 86400 Sekunden. Der Wert **0** bedeutet, dass der Broadcast-Schlüssel nicht aktualisiert wird.

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 Versions**: Die Typen der zu unterstützenden Clientstationen:
  - **WPA**: Im Netzwerk befinden sich Clientstationen mit Unterstützung für den ursprünglichen WPA-Modus und keine Clientstationen mit Unterstützung für den neueren WPA2-Modus.
  - **WPA2**: Alle Clientstationen im Netzwerk unterstützen WPA2. Diese Protokollversion bietet die höchste Sicherheit gemäß dem IEEE 802.11i-Standard.

  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.

- **Cipher Suites**: Die zu verwendende Verschlüsselungssuite:
  - TKIP
  - CCMP (AES)

  Sie können eine oder beide Optionen auswählen. Dem WAP-Gerät können sowohl TKIP- als auch AES-Clients zugeordnet werden. Für die Zuordnung zum WAP-Gerät benötigen WPA-Clients einen der folgenden Schlüssel:
  - Einen gültigen TKIP-Schlüssel
  - Einen gültigen AES-CCMP-Schlüssel

  Clients, die nicht für die Verwendung von WPA Personal konfiguriert sind, können dem WAP-Gerät nicht zugeordnet werden.
- **Key**: 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 #.
- **Key Strength Meter**: 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 Complexity**.
- **Broadcast Key Refresh Rate**: Das Intervall, in dem der Broadcast-Schlüssel (Gruppenschlüssel) für diesem VAP zugeordnete Clients aktualisiert wird. Der Standardwert lautet **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 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 Versions**: Die Typen der zu unterstützenden Clientstationen:
  - **WPA**: Wenn alle Clientstationen im Netzwerk den ursprünglichen WPA-Modus unterstützen, während keine Clientstation den neueren WPA2-Modus unterstützt, wählen Sie **WPA** aus.
  - **WPA2**: Wenn alle Clientstationen im Netzwerk WPA2 unterstützen, sollten Sie WPA2 verwenden, da dieser Modus die höchste Sicherheit gemäß dem IEEE 802.11i-Standard bietet.
  - **WPA and WPA2**: Wenn 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 WPA und WPA2. Mit dieser Einstellung 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 zugunsten besserer Operativität aufgegeben.
- **Enable pre-authentication**: 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.
- **Cipher Suites**: Die zu verwendende Verschlüsselungssuite:
  - TKIP
  - CCMP (AES)
  - TKIP und CCMP (AES)

  Standardmäßig sind TKIP und CCMP ausgewählt. Wenn TKIP und CCMP ausgewählt sind, müssen Clientstationen, die für die Verwendung von WPA mit RADIUS konfiguriert sind, über eine der folgenden Kombinationen aus Schlüssel und Adresse verfügen:

- Eine gültige TKIP-RADIUS-IP-Adresse und einen RADIUS-Schlüssel
- Eine gültige CCMP (AES)-RADIUS-IP-Adresse und einen RADIUS-Schlüssel

- **Use Global RADIUS Server Settings**: 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 Address Type**: Die vom RADIUS-Server verwendete IP-Version.

  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 Address 1** oder **Server IPv6 Address 1**: Die Adresse des primären RADIUS-Servers für diesen VAP.

  Wenn **IPv4** als Option für **Server IP Address Type** 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 Address 2** bis **4** oder **Server IPv6 Address 2** bis **4**: Bis zu drei IPv4- und/oder IPv6-Adressen, die als RADIUS-Backupserver für diesen VAP verwendet werden sollen.

  Wenn die Authentifizierung beim primären Server fehlschlägt, wird der Vorgang nacheinander mit den konfigurierten Backup-Servern wiederholt.

- **Key 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.

- **Key 2** bis **Key 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 IP (IPv6) Address 3** verwendet **Key 3** usw.
- **Enable RADIUS Accounting**: Verfolgt und misst die von einem bestimmten Benutzer verwendeten Ressourcen, beispielsweise Systemzeit, Menge der gesendeten und empfangenen Daten usw.

  Wenn Sie RADIUS Accounting aktivieren, gilt dies für den primären RADIUS-Server und alle Backup-Server.
- **Active 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.

  Broadcast Key Refresh Rate: 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.
- **Session Key Refresh Rate**: Das Intervall, in dem das WAP-Gerät Sitzungsschüssel (Unicast) für die einzelnen dem VAP zugeordneten Clients aktualisiert

  Gültig sind Werte im Bereich von 0 bis 86400 Sekunden. Der Wert **0** bedeutet, dass der Sitzungsschlüssel nicht aktualisiert wird.

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.

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

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

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

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

SCHRITT 2 Vergewissern Sie sich, dass die Option **Administrative Mode** aktiviert ist. Standardmäßig ist die Option deaktiviert.

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

- **Status**: Der Betriebsstatus des Planungsmoduls. Möglich sind die Werte **Up** oder **Down**. Der Standardwert lautet **Down**.
- **Reason**: Der Grund für den Betriebsstatus des Planungsmoduls. Folgende Werte sind möglich:
  - **IsActive**: Das Planungsmodul ist administrativ aktiviert.
  - **Administrative Mode is disabled**: Der Betriebsstatus entspricht **Down**, da die globale Konfiguration deaktiviert ist.

SCHRITT 3 Zum Hinzufügen eines Profils geben Sie in das Textfeld **Scheduler Profile Configuration** einen Profilnamen ein, und klicken Sie auf **Hinzufügen**. Der Profilname kann aus bis zu 32 alphanumerischen Zeichen bestehen.

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.

So konfigurieren Sie eine Regel für ein Profil:

SCHRITT 1 Wählen Sie in der Liste **Select a Profile Name** das Profil aus.

SCHRITT 2 Klicken Sie auf **Add Rule**.

Die neue Regel wird in der Regeltabelle angezeigt.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen neben **Profile Name**, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Wählen Sie im Menü **Day of the Week** 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:

- **Start Time**: 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>. Der Standardwert lautet **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>. Der Standardwert lautet **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. Informationen hierzu finden Sie auf der Seite **Planungsverweis**.

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

Planungsverweis

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.

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless** > **Scheduler Association** aus. Bei WAP561-Geräten wählen Sie unter **Radio** die Funkschnittstelle aus, der Sie ein Planungsmodulprofil zuordnen möchten (**Radio 1** oder **Radio 2**).

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

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

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

Bandwidth Utilization

Auf der Seite **Bandwidth Utilization** können Sie konfigurieren, welcher Anteil der Funkbandbreite verwendet werden kann, bis das WAP-Gerät keine neuen Clientzuordnungen mehr zulässt. Diese Funktion ist standardmäßig aktiviert.

So ändern Sie die Einstellungen für die Bandbreitennutzung:

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

SCHRITT 2 Klicken Sie auf **Enable**, um die Option **Bandwidth Utilization** zu aktivieren, oder deaktivieren Sie **Enable**, um die Bandbreitennutzung zu deaktivieren.

SCHRITT 3 Wenn die Bandbreitennutzung aktiviert ist, geben Sie in das Feld **Maximum Utilization Threshold** den Prozentanteil der Nutzung der Netzwerkbandbreite für das Funkmodul ein, die zulässig ist, bis das WAP-Gerät keine neuen Clientzuordnungen mehr zulässt.

Gültig sind Ganzzahlen von 0 bis 100 Prozent. Der Standardwert lautet **70 Prozent**. Wenn der Wert auf **0** festgelegt ist, sind unabhängig von der Nutzungsrate alle neuen Zuordnungen zulässig.

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

HINWEIS Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

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.

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.

So konfigurieren Sie die MAC-Filterung:

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

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

- **Allow only stations in the list**: Allen nicht in der Stationsliste enthaltenen Stationen wird der Zugriff auf das Netzwerk über das WAP-Gerät verweigert.
- **Block all stations in list**: 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 Address** die zuzulassende oder zu blockierende MAC-Adresse ein, und klicken Sie auf **Hinzufügen**.

Die MAC-Adresse wird in der **Stations List** 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 Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

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

WDS-Bridge

Mithilfe von WDS (Wireless Distribution System) können Sie mehrere WAP551- und WAP561-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.

Das WAP-Gerät kann auch als Repeater fungieren. In diesem Modus dient das WAP-Gerät als Verbindung zwischen zwei WAP-Geräten, die möglicherweise zu weit voneinander entfernt sind, um das Funksignal zu empfangen. Wenn das WAP-Gerät als Repeater fungiert, ist keine Kabelverbindung mit dem LAN erforderlich, und die Signale werden über die WLAN-Verbindung weitergesendet. Sie müssen

keine besonderen Einstellungen konfigurieren, um das WAP-Gerät als Repeater zu verwenden, und es gibt keine Einstellungen für den Repeater-Modus. 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:

- WDS kann nur für Cisco WAP551- und Cisco WAP561-Geräte verwendet werden.
- Alle an einer WDS-Verbindung beteiligten WAP-Geräte von Cisco müssen über die folgenden identischen Einstellungen verfügen:
  - **Radio**
  - **IEEE 802.11 Mode**
  - **Channel Bandwidth**
  - **Channel** (**Auto** wird nicht empfohlen.)

  HINWEIS Wenn Sie Bridging im 802.11n-2,4-GHz-Band verwenden, legen Sie **Channel Bandwidth** 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 die Option **Wireless** > **WDS Bridge** aus.

SCHRITT 2 Wählen Sie für **Spanning Tree Mode** die Option **Enable** aus. Wenn STP aktiviert ist, können Switching-Loops vermieden werden. STP wird empfohlen, wenn Sie WDS-Verbindungen konfigurieren. Bei WAP561-Geräten wählen Sie für jede zu konfigurierende WDS-Verbindung die Option **Radio 1** oder **Radio 2** aus.

SCHRITT 3 Wählen Sie für **WDS Interface** die Option **Enable** aus.

SCHRITT 4 Konfigurieren Sie die übrigen Parameter:

- **Remote MAC Address**: 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**.

- **Encryption**: 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**.

  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**.

SCHRITT 5 Wiederholen Sie diese Schritte für bis zu drei weitere WDS-Schnittstellen.

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

SCHRITT 7 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.

VORSICHT Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

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

- **Key Length**: Wenn WEP aktiviert ist, geben Sie **64 Bit** oder **128 Bit** für die Länge des WEP-Schlüssels an.
- **Key Type**: Wenn WEP aktiviert ist, geben Sie den Typ des WEP-Schlüssels an: **ASCII** oder **Hex**.
- **WEP Key**: 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 **Key Type** und **Key Length** ändert.

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.

- **Key**: 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 das WAP-Gerät im WLAN als WLAN-Station (STA). Es kann Verkehr zwischen einem drahtgebundenen Remotenetzwerk oder zugeordneten WLAN-Clients und dem im WorkGroup Bridge-Modus verbundenen WLAN überbrücken.

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

Es wird empfohlen, den WorkGroup-Bridge-Modus nur zu verwenden, wenn die WDS-Bridge-Funktion nicht mit einem Peer-WAP-Gerät verwendet werden kann. WDS ist als bessere Lösung der WorkGroup-Bridge-Lösung vorzuziehen. Verwenden Sie WDS, wenn Sie Cisco WAP121-, WAP321-, WAP551- und WAP561-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 das WAP-Gerät aktiviert ist.

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

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

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

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

- Alle an der WorkGroup-Bridge beteiligten WAP-Geräte müssen über die folgenden identischen Einstellungen verfügen:
  - **Radio**
  - **IEEE 802.11 Mode**
  - **Channel Bandwidth**
  - **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.
- Es wird nicht empfohlen, einen anderen AP der Downstream-Schnittstelle des im WorkGroup-Bridge-Modus betriebenen WAP-Geräts zuzuordnen; das heißt, das Verketten oder Kaskadieren von APs wird nicht unterstützt.

So konfigurieren Sie den WorkGroup-Bridge-Modus:

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

SCHRITT 2 Wählen Sie für **WorkGroup Bridge Mode** die Option **Enable** aus.

SCHRITT 3 Bei WAP561-Geräten wählen Sie die Funkschnittstelle aus, für die Sie den WorkGroup-Bridge-Modus konfigurieren möchten (**Radio 1** oder **Radio 2**).

SCHRITT 4 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 Detection** die (ebenfalls standardmäßig deaktivierte) Option **AP Detection** aktiviert ist.

- **Security**: Der Typ der Sicherheit, die für die Authentifizierung als Clientstation für das Upstream-WAP-Gerät verwendet werden soll. Zur Auswahl stehen die folgenden Optionen:
  - **None**
  - **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 oben auf der Seite auf die Schaltfläche **Aktualisieren** klicken, um den aktuellen Verbindungsstatus anzuzeigen.

SCHRITT 5 Konfigurieren Sie die folgenden Felder für die Access Point-Schnittstelle:

- **Status**: Wählen Sie für die Access Point-Schnittstelle die Option **Enable** aus.
- **SSID**: Die SSID für die Access Point-Schnittstelle muss nicht mit der für den Infrastrukturclient übereinstimmen. Wenn Sie jedoch ein Roaming-Szenario unterstützen möchten, müssen die SSID und die Sicherheit übereinstimmen.

- **SSID Broadcast**: Wählen Sie aus, ob die Downstream-SSID übertragen werden soll. Standardmäßig sind SSID-Broadcasts aktiviert.
- **Security**: Der Typ der für die Authentifizierung zu verwendenden Sicherheit. Zur Auswahl stehen die folgenden Optionen:
  - **None**
  - **Static WEP**
  - **WPA Personal**
- **MAC Filtering**: Wählen Sie eine der folgenden Optionen aus:
  - **Disabled**: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist nicht auf die in einer MAC-Adressenliste angegebenen Clients beschränkt.
  - **Local**: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist auf die in einer lokal definierten MAC-Adressenliste angegebenen Clients beschränkt.
  - **RADIUS**: Die Gruppe der Clients im BSS des APs, die auf das Upstream-Netzwerk zugreifen können, ist auf die in einer MAC-Adressenliste auf einem RADIUS-Server angegebenen Clients beschränkt.

  Wenn Sie **Local** oder **RADIUS** auswählen, finden Sie unter **MAC-Filterung** Anweisungen zum Erstellen der MAC-Filterliste.
- **VLAN ID**: Konfigurieren Sie die Access Point-Schnittstelle mit der gleichen VLAN-ID, die an der Infrastrukturclient-Schnittstelle angekündigt wird.

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

Die zugeordneten Downstream-Clients verfügen jetzt über Konnektivität mit dem Upstream-Netzwerk.

Quality of Service

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 das WAP-Gerät 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.

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

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Wireless** > **QoS** aus. Bei WAP561-Geräten wählen Sie die Funkschnittstelle aus, für die Sie QoS-Einstellungen konfigurieren möchten (**Radio 1** oder **Radio 2**).

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

- **WFA Defaults**: 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.
- **Optimized for Voice**: Füllt die EDCA-Parameter für das WAP-Gerät und die Stationen mit für Sprachverkehr am besten geeigneten Werten.
- **Custom**: 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:

- **Data 0 (Voice)**: Warteschlange mit hoher Priorität und minimaler Verzögerung. Zeitkritische Daten wie beispielsweise VoIP und Streaming-Medien werden automatisch an diese Warteschlange gesendet.
- **Data 1 (Video)**: Warteschlange mit hoher Priorität und minimaler Verzögerung. Zeitkritische Videodaten werden automatisch an diese Warteschlange gesendet.
- **Data 2 (Best Effort)**: Warteschlange mit mittlerer Priorität, mittlerem Durchsatz und mittlerer Verzögerung. Die meisten herkömmlichen IP-Daten werden an diese Warteschlange gesendet.
- **Data 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.
- **Minimum Contention Window**: 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**.

- **Maximum Contention Window**: 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**.

- **Maximum Burst** (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 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 **Enable** 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 das WAP-Gerät den Downstream-Verkehrsfluss vom WAP-Gerät zur Clientstation (AP-EDCA-Parameter) und den Upstream-Verkehrsfluss von der Station zum AP (EDCA-Stationsparameter).

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

- **TXOP Limit** (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:

- **No Acknowledgement**: Wählen Sie **Enable** aus, um anzugeben, dass das WAP-Gerät Frames mit dem Dienstklassenwert **QosNoAck** nicht bestätigen soll.
- **Unscheduled Automatic Power Save Delivery**: Wählen Sie **Enable** 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 Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

WPS-Einrichtung

In diesem Abschnitt wird das WPS-Protokoll (Wi-Fi Protected Setup) und dessen Konfiguration für das WAP-Gerät beschrieben.

WPS ist ein Standard, der das einfache Einrichten von WLANs ohne Beeinträchtigung der Netzwerksicherheit ermöglicht. Dabei müssen weder die Benutzer von WLAN-Clients noch der Administrator des WAP-Geräts Netzwerknamen, Schlüssel und verschiedene andere kryptographische Konfigurationsoptionen kennen.

WPS erleichtert die Netzwerkeinrichtung, da der Administrator durch Drücken einer Taste oder Eingeben einer PIN ein WLAN einrichten kann. Dabei entfällt das manuelle Eingeben von Netzwerknamen (SSIDs) und WLAN-Sicherheitsparametern:

- **Taste**: Die WPS-Taste befindet sich am Produkt. Alternativ kann es sich um eine Schaltfläche zum Klicken auf der Benutzeroberfläche handeln.
- **PIN (Personal Identification Number)**: Sie können die PIN auf der Benutzeroberfläche des Produkts anzeigen.

WPS gewährleistet die Netzwerksicherheit, da sowohl die Benutzer neuer Clientgeräte als auch WLAN-Administratoren entweder über physischen Zugriff oder sicheren Remotezugriff auf die jeweiligen Geräte verfügen müssen.

Typische Szenarien für die Verwendung von WPS:

- Ein Benutzer möchte eine Clientstation in einem WPS-fähigen WLAN registrieren. (Möglicherweise erkennt das zu registrierende Clientgerät das Netzwerk und fordert den Benutzer zur Registrierung auf. Dies ist jedoch nicht notwendig.) Der Benutzer löst die Registrierung aus, indem er eine Taste am Clientgerät drückt. Anschließend drückt der Administrator des WAP-Geräts eine Taste am WAP-Gerät. In einem kurzen Austausch von WPS-Protokollnachrichten stellt das WAP-Gerät dem neuen Client über das EAP-Protokoll (Extensible Authentication Protocol) eine neue Sicherheitskonfiguration bereit. Die Zuordnung der beiden Geräte wird aufgehoben und anschließend erneut hergestellt. Dabei werden die Geräte mit den neuen Einstellungen authentifiziert.
- Ein Benutzer möchte eine Clientstation in einem WPS-fähigen WLAN registrieren, indem er dem Administrator des WAP-Geräts die PIN des Client-Geräts nennt. Der Administrator gibt die PIN in das Konfigurationsdienstprogramm des WAP-Geräts ein und löst die Geräteregistrierung aus. Das neu registrierte Gerät und das WAP-Gerät tauschen WPS-Nachrichten aus, die eine neue Sicherheitskonfiguration enthalten, heben ihre Zuordnung auf, stellen die Zuordnung erneut her und authentifizieren sich.
- Der Administrator eines WAP-Geräts kauft ein neues WAP-Gerät, das von der WiFi Alliance als mit WPS Version 2.0 kompatibel zertifiziert wurde, und möchte das WAP-Gerät einem vorhandenen drahtgebundenen Netzwerk oder WLAN hinzufügen. Der Administrator schaltet das WAP-Gerät ein und greift auf einen Netzwerk-Host zu, der das WPS-Registrierungsprotokoll unterstützt. Der Administrator gibt die PIN des WAP-Geräts in das Konfigurationsdienstprogramm des externen Registrars ein und löst den WPS-Registrierungsprozess aus. (In einem drahtgebundenen LAN werden

die WPS-Protokollnachrichten über das UPnP-Protokoll übertragen.) Der Host registriert den WAP als neues Netzwerkgerät und konfiguriert den WAP mit neuen Sicherheitseinstellungen.

- Der Administrator eines WAP-Geräts hat gerade über WPS ein neues WAP-Gerät einem vorhandenen WLAN oder drahtgebundenen Netzwerk hinzugefügt und möchte einem neuen Clientgerät Netzwerkzugriff gewähren. Das Gerät wird mit den oben beschriebenen Methoden (PIN oder Tastensteuerung (Push-Button Control, PBC)) registriert. Diesmal wird das Gerät jedoch beim externen Registrar registriert, und das WAP-Gerät fungiert nur als Proxy.
- Ein WLAN-Gerät ohne WPS-Unterstützung muss dem WPS-fähigen WLAN beitreten. Der Administrator, der WPS in diesem Fall nicht verwenden kann, konfiguriert stattdessen das Gerät manuell mit der SSID, dem öffentlichen gemeinsamen Schlüssel und den Kryptographiemodi des WPS-fähigen WAP-Geräts. Das Gerät tritt dem Netzwerk bei.

Bei der PIN handelt es sich um eine achtstellige Zahl, deren letzte Ziffer als Prüfsummenwert dient, oder um eine vierstellige Zahl ohne Prüfsumme. Beide Zahlen können führende Nullen enthalten.

Der WPS-Standard weist den verschiedenen Komponenten seiner Architektur spezifische Rollen zu:

- **Zu registrierendes Gerät**: Ein Gerät, das dem WLAN beitreten kann
- **AP**: Ein Gerät, das WLAN-Zugriff auf das Netzwerk bereitstellt
- **Registrar**: Eine Entität, die zu registrierenden Geräten zu Sicherheitszwecken erforderliche Anmeldeinformationen bereitstellt und APs konfiguriert

Die WAP-Geräte fungieren als AP-Geräte und unterstützen einen integrierten Registrar. Sie fungieren nicht als zu registrierende Geräte.

Der Administrator kann WPS nur für einen VAP aktivieren oder deaktivieren. WPS kann nur verwendet werden, wenn der jeweilige VAP diese Bedingungen erfüllt:

- Das WAP-Gerät ist so konfiguriert, dass die VAP-SSID übertragen wird.
- MAC-Adressfilterung ist für den VAP deaktiviert.
- WEP-Verschlüsselung ist für den VAP deaktiviert.
- Der VAP ist für die Verwendung von WPA Personal-Sicherheit oder ohne Sicherheit konfiguriert. Wenn der WPA2-PSK-Verschlüsselungsmodus aktiviert ist, muss ein gültiger vorher vereinbarter Schlüssel (Pre-Shared

Key, PSK) konfiguriert sein und Verschlüsselung mit CCMP (AES) muss aktiviert sein.

- Der Betrieb des VAPs ist aktiviert.

Der Betrieb von WPS ist für den VAP deaktiviert, wenn eine dieser Bedingungen nicht erfüllt ist.

HINWEIS Durch das Deaktivieren von WPS für einen VAP wird die Zuordnung von zuvor für den jeweiligen VAP über WPS authentifizierten Clients nicht aufgehoben.

Die Registrierung der Clients im Netzwerk muss nicht von den WAP-Geräten selbst vorgenommen werden. Das WAP-Gerät kann den integrierten Registrar verwenden oder als Proxy für einen externen Registrar fungieren. Der Zugriff auf den externen Registrar kann über das drahtgebundene LAN oder das WLAN erfolgen. Ein externer Registrar kann auch die SSID, den Verschlüsselungsmodus und den öffentlichen gemeinsamen Schlüssel eines WPS-fähigen BSS konfigurieren. Diese Funktion ist sehr hilfreich bei Bereitstellungen im Auslieferungszustand, das heißt Bereitstellungen, bei denen ein Administrator ein neues WAP-Gerät einfach erstmals mit einem LAN verbindet.

Wenn das WAP-Gerät einen integrierten Registrar verwendet, werden neue Clients mit der Konfiguration des dem WPS-Dienst zugeordneten VAPs registriert. Dabei spielt es keine Rolle, ob diese Konfiguration direkt im WAP-Gerät vorgenommen wurde oder über WPS von einem externen Registrar abgerufen wurde.

Tastensteuerung

Das WAP-Gerät registriert 802.11-Clients mit einer der folgenden zwei Methoden über WPS: PBC-Methode (Push-Button Control, Tastensteuerung) oder PIN-Methode (Personal Identification Number).

Bei der PBC-Methode drückt der Benutzer eines potenziellen Clients eine Taste am zu registrierenden Gerät, und der Administrator des WAP-Geräts mit integriertem Registrar drückt eine ähnliche Hardwaretaste oder klickt auf eine entsprechende Schaltfläche in der Software. Mit dieser Sequenz beginnt der Registrierungsprozess, und das Clientgerät tritt dem Netzwerk bei. Obwohl die WAP-Geräte von Cisco keine tatsächliche Hardwaretaste unterstützen, kann der Administrator die Registrierung für einen bestimmten VAP über eine Softwareschaltfläche im webbasierten Konfigurationsdienstprogramm initiieren.

HINWEIS Die Tasten am Clientgerät und am WAP-Gerät müssen nicht in einer bestimmten Reihenfolge gedrückt werden. Die Registrierung kann von beiden Geräten initiiert werden. Wenn Sie jedoch in der Software auf die Schaltfläche für das WAP-Gerät klicken und nach 120 Sekunden kein Client sich zu registrieren versucht hat, beendet das WAP-Gerät die ausstehende WPS-Registrierungstransaktion.

PIN-Steuerung

Ein Client kann auch mithilfe einer PIN bei einem Registrar registriert werden. Beispielsweise kann der Administrator des WAP-Geräts eine Registrierungstransaktion für einen bestimmten VAP starten, indem er die PIN eines Clients eingibt. Wenn der Client das WPS-fähige Gerät erkennt, kann der Benutzer dem WAP-Gerät die PIN bereitstellen, um den Registrierungsprozess fortzusetzen. Nach Abschluss des WPS-Protokolls tritt der Client sicher dem Netzwerk bei. Der Client kann diesen Prozess ebenfalls initiieren.

Wie bei der PBC-Methode beendet das WAP-Gerät die ausstehende Transaktion, wenn die Registrierungstransaktion vom WAP-Gerät begonnen wurde und nach 120 Sekunden kein Client sich zu registrieren versucht hat.

Das WAP-Gerät unterstützt zwar einen integrierten Registrar für WPS, die Verwendung ist jedoch optional. Wenn ein externer Registrar das WAP-Gerät konfiguriert hat, fungiert das WAP-Gerät als Proxy für diesen externen Registrar. Dabei spielt es keine Rolle, ob der integrierte Registrar des WAP-Geräts aktiviert ist (Standardeinstellung).

Jedes WAP-Gerät speichert im nichtflüchtigen RAM eine WPS-kompatible Geräte-PIN. Diese PIN ist für WPS erforderlich, wenn ein Administrator das Beitreten eines nicht konfigurierten WAP-Geräts (das heißt eines WAP-Geräts, das nur über Werkseinstellungen verfügt, einschließlich der Aktivierung von WPS für einen VAP) zum Netzwerk zulassen möchte. In diesem Szenario bezieht der Administrator den PIN-Wert vom Konfigurationsdienstprogramm für das WAP-Gerät.

Wenn die Integrität des Netzwerks beeinträchtigt wurde, sollte der Administrator die PIN ändern. Das WAP-Gerät stellt eine Methode zum Generieren einer neuen PIN und zum Speichern dieses Werts im NVRAM bereit. Wenn der Wert im NVRAM beschädigt ist, gelöscht wurde oder fehlt, generiert das WAP-Gerät eine neue PIN und speichert diese im NVRAM.

Die Registrierungsmethode mit PIN ist potenziell für Brute-Force-Angriffe anfällig. Ein Eindringling im Netzwerk könnte versuchen, sich im WLAN als externer Registrar auszugeben und den PIN-Wert des WAP-Geräts durch fortgesetztes Anwenden WPS-kompatibler PINs abzuleiten. Diese Schwachstelle wird auf folgende Weise behoben: Wenn ein Registrar bei drei Versuchen innerhalb von 60 Sekunden nicht die richtige PIN bereitstellt, verhindert das WAP-Gerät 60 Sekunden lang weitere Registrierungsversuche eines externen Registrars beim WAP-Gerät im WPS-fähigen VAP. Die Sperrdauer verlängert sich bei weiteren Fehlern auf maximal 64 Minuten. Nach dem zehnten fehlgeschlagenen Versuch in Folge wird die Registrierungsfunktionalität des WAP-Geräts dauerhaft gesperrt. Setzen Sie das Gerät zurück, um die Registrierungsfunktionalität neu zu starten.

WLAN-Clientstationen können sich jedoch während dieses Sperrzeitraums beim integrierten Registrar des WAP-Geräts registrieren, wenn dieser aktiviert ist. Außerdem stellt das WAP-Gerät weiterhin Proxy-Dienste für Registrierungsanfragen an externe Registrare bereit.

Das WAP-Gerät verfügt über eine zusätzliche Sicherheitsfunktion für den Schutz der Geräte-PIN. Wenn das WAP-Gerät bei einem externen Registrar registriert und die sich ergebende WPS-Transaktion abgeschlossen ist, wird die Geräte-PIN automatisch neu generiert.

Durch das WPS-Protokoll können für einen WPS-fähigen VAP in einem WAP-Gerät die folgenden Parameter konfiguriert werden:

- Netzwerk-SSID
- Schlüsselverwaltungsoptionen (WPA-PSK oder WPA-PSK und WPA2-PSK)
- Kryptographieoptionen (CCMP/AES oder TKIP und CCMP/AES)
- (Öffentlicher gemeinsamer) Netzwerkschlüssel

Wenn WPS für einen VAP aktiviert ist, können diese Konfigurationsparameter geändert werden. Beim Neustart des WAP-Geräts bleiben sie erhalten.

Das WAP-Gerät unterstützt die Registrierung bei externen WPS-Registraren (External Registrars, ERs) im drahtgebundenen LAN und im WLAN. Im WLAN kündigen externe Registrare ihre Funktionen in WPS-spezifischen Informationselementen (IEs) der Beacon-Frames an. Im drahtgebundenen LAN kündigen externe Registrare ihre Funktionen über UPnP an.

WPS Version 2.0 erfordert keine Registrierung bei einem ER über die Benutzeroberfläche. Der Administrator kann das WAP-Gerät mit den folgenden Schritten bei einem ER registrieren:

SCHRITT 1 Eingeben der PIN für den externen Registrar im WAP-Gerät

SCHRITT 2 Eingeben der PIN des WAP-Geräts auf der Benutzeroberfläche des externen Registrars

HINWEIS Beim Registrierungsprozess kann das WAP-Gerät außerdem gemäß den Angaben im Abschnitt **VAP Configuration Changes** konfiguriert werden, wenn das WAP-Gerät in den WPS-spezifischen IEs der Beacon-Frames oder in UPnP-Nachrichten angegeben hat, dass diese Konfiguration erforderlich ist.

Das WAP-Gerät kann als Proxy für bis zu drei externe Registrare gleichzeitig dienen.

WPS kann für jeden VAP im WAP-Gerät aktiviert sein. Es kann jeweils höchstens eine WPS-Transaktion (beispielsweise Registrierung und Zuordnung eines 802.11-Clients) im WAP-Gerät durchgeführt werden. Der Administrator des WAP-Geräts kann die ausgeführte Transaktion über das webbasierte AP-Konfigurationsdienstprogramm beenden. Die Konfiguration des VAPs sollte jedoch während der Transaktion nicht geändert werden. Außerdem sollten während des Authentifizierungsprozesses keine Änderungen am VAP vorgenommen werden. Diese Einschränkung wird empfohlen, jedoch für das WAP-Gerät nicht erzwungen.

Obwohl WAP-Geräte WPS Version 2.0 unterstützen, interagiert das WAP-Gerät mit zu registrierenden Geräten und Registraren, deren Konformität mit Version 1.0 des WPS-Protokolls durch die WiFi Alliance zertifiziert wurde.

Auf der Seite **WPS Setup** können Sie das WAP-Gerät als WPS-fähiges Gerät aktivieren und grundlegende Einstellungen konfigurieren. Wenn Sie bereit sind, die Funktion zum Registrieren eines neuen Geräts oder zum Hinzufügen des WAP-Geräts zu einem WPS-fähigen Netzwerk zu verwenden, ist dies auf der Seite **WPS Process** möglich.

VORSICHT Aus Sicherheitsgründen wird empfohlen, beim Konfigurieren von WPS eine HTTPS-Verbindung mit dem webbasierten AP-Konfigurationsdienstprogramm zu verwenden. Dies ist jedoch nicht erforderlich.

So konfigurieren Sie das WAP-Gerät als WPS-fähiges Gerät:

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

Auf der Seite **WPS Setup** werden globale Parameter und der Status sowie die Parameter und der Status der WPS-Instanz angezeigt. Bei einer Instanz handelt es sich um eine WPS-Implementierung, die einem VAP im Netzwerk zugeordnet ist. Das WAP-Gerät unterstützt nur eine Instanz.

SCHRITT 2 Konfigurieren Sie die globalen Parameter:

- **Supported WPS Version**: Die vom WAP-Gerät unterstützte Version des WPS-Protokolls
- **WPS Device Name**: Stellt einen Standardgerätenamen bereit. Sie können einen anderen Namen zuweisen, der aus 1 bis 32 Zeichen besteht und Leerzeichen und Sonderzeichen enthält.
- **WPS Global Operational Status**: Gibt an, ob der WPS-Betriebsstatus des WAP-Geräts **Up** oder **Down** entspricht.

- **WPS Device PIN**: Eine vom System generierte achtstellige WPS-PIN für das WAP-Gerät. Der Administrator kann diese generierte PIN verwenden, um das WAP-Gerät bei einem externen Registrar zu registrieren.

  Sie können auf **Generate** klicken, um eine neue PIN zu generieren. Wenn die Integrität des Netzwerks beeinträchtigt wurde, sollten Sie eine neue PIN generieren.

SCHRITT 3 Konfigurieren Sie die Parameter für die WPS-Instanz:

- **WPS Instance ID**: Eine ID für die Instanz. Da nur eine Instanz vorhanden ist, lautet die einzige Option **wps1**.
- **WPS Mode**: Aktiviert oder deaktiviert die Instanz.
- **WPS Radio**: Das Funkmodul, für das diese WPS-Instanz gilt (nur bei WAP561-Geräten).
- **WPS VAP**: Der dieser WPS-Instanz zugeordnete VAP
- **WPS Built-in Registrar**: Aktiviert die integrierte Registrar-Funktion. Wenn die Funktion aktiviert ist, können sich zu registrierende Geräte (in der Regel WLAN-Clients) beim WAP-Gerät registrieren. Wenn die Funktion deaktiviert ist, ist die Registrar-Funktionalität im WAP-Gerät deaktiviert, und das zu registrierende Gerät muss sich bei einem anderen Registrar im Netzwerk registrieren. In diesem Fall fungiert ein anderes Gerät im Netzwerk als Registrar, und das WAP-Gerät dient als Proxy für die Weiterleitung von Clientregistrierungsanfragen und für die Antworten des Registrars.
- **WPS Configuration State**: Gibt an, ob der VAP im Rahmen des WPS-Prozesses vom externen Registrar konfiguriert wird. Sie können einen der folgenden Werte festlegen:
  - **Unconfigured**: Die VAP-Einstellungen werden mit WPS konfiguriert. Anschließend wird der Status in **Configured** geändert.
  - **Configured**: Die VAP-Einstellungen werden nicht vom externen Registrar konfiguriert, und die vorhandene Konfiguration wird beibehalten.

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

Der Betriebsstatus der Instanz und der Grund für den Status werden angezeigt. Weitere Informationen zu Bedingungen, die zur Deaktivierung der Instanz führen können, finden Sie unter "Aktivieren oder Deaktivieren von WPS für einen VAP".

Im Bereich **Instance Status** werden die folgenden Informationen zur ausgewählten WPS-Instanz angezeigt:

- **WPS Operational Status**: Gibt an, ob die WPS-Instanz betriebsbereit ist.
- **AP Lockdown Status**: Gibt an, ob sich der AP im Sperrmodus befindet, in dem die Registrierung externer Registrare beim AP gesperrt ist. Im Sperrstatus wird in diesem Feld die Startzeit der Sperrung angegeben, ob es sich um eine temporäre oder dauerhafte Sperrung handelt, und bei einer temporären Sperrung die Dauer des Sperrzeitraums. Wenn der Sperrmodus nicht aktiv ist, wird der Status **Disabled** angezeigt.
- **Failed Attempts with Invalid PIN**: Gibt an, wie oft der Registrierungsversuch eines externen Registrars beim WAP-Gerät fehlgeschlagen ist.

Im Sperrstatus werden die folgenden Felder angezeigt:

- **AP Lockdown Duration**: Die Dauer der Sperrung des WAPs in Minuten. Wenn der WAP dauerhaft gesperrt ist, ist dieser Wert auf **-1** festgelegt.
- **AP Lockdown Timestamp**: Der Zeitpunkt der Sperrung des WAP-Geräts

Sie können auf **Aktualisieren** klicken, um die Seite mit den neuesten Statusinformationen zu aktualisieren.

WPS Process

Auf der Seite **WPS Process** können Sie eine Clientstation mithilfe von WPA im Netzwerk registrieren. Sie können einen Client mit einer PIN oder mit der Tastenmethode registrieren, wenn die Clientstation dies unterstützt.

So registrieren Sie eine Clientstation mit der PIN-Methode:

SCHRITT 1 Bringen Sie die PIN des Clientgeräts in Erfahrung. Die PIN kann auf die Hardware selbst gedruckt sein. Möglicherweise finden Sie die PIN auch auf der Benutzeroberfläche der Software des Geräts.

SCHRITT 2 Wählen Sie im Navigationsbereich die Option **Wireless** > **WPS Process** aus.

SCHRITT 3 Geben Sie in das Textfeld **PIN Enrollment** die PIN des Clients ein, und klicken Sie auf **Start**.

HINWEIS Neben der WPS-kompatiblen achtstelligen Geräte-PIN (die führende Nullen enthalten kann) können Sie in das Feld **PIN Enrollment** auch die Zeichenfolge **stop** eingeben, um die Registrierung zu beenden.

SCHRITT 4 Geben Sie innerhalb von zwei Minuten die WAP-PIN auf der Benutzeroberfläche der Software des Clientgeräts ein. Die WAP-PIN konfigurieren Sie auf der Seite **WPS-Einrichtung**.

Wenn Sie die PIN am Clientgerät eingeben, ändert sich der Betriebsstatus unter **WPS Operational Status** in **Adding Enrollee**. Nach Abschluss des Registrierungsprozesses ändert sich **WPS Operational Status** in **Ready** und **Transaction Status** in **Success**.

Wenn der Client registriert ist, konfiguriert der integrierte Registrar des WAP-Geräts oder der externe Registrar im Netzwerk den Client mit der SSID, dem Verschlüsselungsmodus und dem öffentlichen gemeinsamen Schlüssel eines WPS-fähigen BSS.

VORSICHT Diese Registrierungssequenz kann auch in umgekehrter Reihenfolge ablaufen, das heißt, Sie können den Prozess in der Clientstation initiieren, indem Sie die PIN des WAP-Geräts eingeben. Diese Methode wird jedoch aus Sicherheitsgründen **nicht empfohlen**, da die SSID und die Sicherheitseinstellungen für den AP vom Client konfiguriert werden können. Der Administrator sollte die PIN nur für vertrauenswürdige Geräte verwenden.

So registrieren Sie eine Clientstation mit der Tastenmethode:

SCHRITT 1 Klicken Sie neben **PBC Enrollment** auf **Start**.

SCHRITT 2 Drücken Sie die Hardwaretaste an der Clientstation.

HINWEIS Alternativ können Sie diesen Prozess an der Clientstation initiieren und dann für das WAP-Gerät auf die Schaltfläche **PBC Enrollment Start** klicken.

Wenn Sie die Taste an der Clientstation drücken, ändert sich der Betriebsstatus unter **WPS Operational Status** in **Adding Enrollee**. Nach Abschluss des Registrierungsprozesses ändert sich **WPS Operational Status** in **Ready** und **Transaction Status** in **Success**.

Wenn der Client registriert ist, konfiguriert der integrierte Registrar des WAP-Geräts oder der externe Registrar im Netzwerk den Client mit der SSID, dem Verschlüsselungsmodus und dem öffentlichen gemeinsamen Schlüssel eines WPS-fähigen BSS.

Im Abschnitt **Instance Status** werden die folgenden Informationen zu der in der Liste **WPS Instance ID** ausgewählten WPS-Instanz angezeigt:

- **WPS Status**: Gibt an, ob die ausgewählte WPS-Instanz aktiviert oder deaktiviert ist.
- **WPS Configuration State**: Gibt an, ob der VAP im Rahmen des WPS-Prozesses vom externen Registrar konfiguriert wird.
- **Transaction Status**: Der Status der letzten WPS-Transaktion. Folgende Werte sind möglich: **None**, **Success**, **WPS Message Error** und **Timed Out**.
- **WPS Operational Status**: Der Status der aktuellen oder letzten WPS-Transaktion. Folgende Werte sind möglich: **Disabled**, **Ready**, **Configuring**, **Proxying** und **Adding Enrollee**. Wenn seit der Aktivierung von WPS keine WPS-Transaktion ausgeführt wurde, wird der Status **Ready** angezeigt.
- **AP Lockdown Status**: Gibt an, ob die Instanz zurzeit gesperrt ist.
- **Failed Attempts with Invalid PIN**: Gibt an, wie oft der Authentifizierungsversuch eines externen Registrars aufgrund eines ungültigen Kennworts fehlgeschlagen ist.

Die folgenden Informationen werden für die WPS-Instanz angezeigt:

- **WPS Radio** (nur WAP561)
- **WPS VAP**
- **SSID**
- **Security**
- **Shared Key**

Wenn das Feld **WPS Configuration State** auf der Seite **WPS Setup** auf **Unconfigured** festgelegt ist, werden die Werte für **SSID** und **Security** vom externen Registrar konfiguriert. Wenn das Feld auf **Configured** festgelegt ist, werden diese Werte vom Administrator konfiguriert.

HINWEIS Sie können auf **Aktualisieren** klicken, um die Seite mit den neuesten Statusinformationen zu aktualisieren.

6

Systemsicherheit

In diesem Kapitel wird beschrieben, wie Sie die Sicherheitseinstellungen für das WAP-Gerät konfigurieren.

Das Kapitel umfasst die folgenden Themen:

- **RADIUS-Server**
- **802.1X Supplicant**
- **Password Complexity**
- **WPA-PSK Complexity**

RADIUS-Server

Verschiedene Funktionen erfordern Kommunikation mit einem RADIUS-Authentifizierungsserver. Wenn Sie beispielsweise im WAP-Gerät virtuelle Access Points (VAPs) konfigurieren, können Sie Sicherheitsmethoden zum Steuern des Zugriffs durch WLAN-Clients konfigurieren (siehe Seite **Funk**). Bei den Sicherheitsmethoden **Dynamic WEP** und **WPA Enterprise** erfolgt die Authentifizierung von Clients über einen externen RADIUS-Server. Sie können auch die Funktion für die MAC-Adressfilterung, bei der der Clientzugriff auf eine Liste beschränkt ist, für die Steuerung des Zugriffs mithilfe eines RADIUS-Servers konfigurieren. Die Captive Portal-Funktion verwendet ebenfalls RADIUS für die Authentifizierung von Clients.

Auf der Seite **Radius Server** können Sie die von diesen Funktionen verwendeten RADIUS-Server konfigurieren. Sie können bis zu vier global verfügbare IPv4- oder IPv6-RADIUS-Server konfigurieren. Dabei müssen Sie jedoch auswählen, ob der RADIUS-Client im Hinblick auf die globalen Server im IPv4- oder IPv6-Modus betrieben wird. Einer der Server fungiert immer als primärer Server, während die anderen als Backup-Server fungieren.

HINWEIS Neben der Verwendung der globalen RADIUS-Server können Sie außerdem die einzelnen VAPs für die Verwendung einer Gruppe bestimmter RADIUS-Server konfigurieren. Informationen hierzu finden Sie auf der Seite **Netzwerke**.

So konfigurieren Sie globale RADIUS-Server:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **System Security** > **RADIUS Server** aus.

SCHRITT 2 Geben Sie die folgenden Parameter ein:

- **Server IP Address Type**: Die vom RADIUS-Server verwendete IP-Version.

  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 des in diesem Feld ausgewählten Adresstyps her.

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

  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.

- **Server IP Address (2** bis **4)** oder **Server IPv6 Address (2** bis **4)**: Bis zu drei IPv4- oder IPv6-Adressen für RADIUS-Backup-Server.

  Wenn die Authentifizierung beim primären Server fehlschlägt, wird der Vorgang nacheinander mit den konfigurierten Backup-Servern wiederholt.

- **Key 1**: Der gemeinsame geheime Schlüssel, den das WAP-Gerät für die Authentifizierung gegenüber dem primären RADIUS-Server verwendet.

  Sie können 1 bis 64 alphanumerische Standardzeichen und Sonderzeichen verwenden. Beim Schlüssel wird zwischen Groß- und Kleinschreibung unterschieden, und der Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Der eingegebene Text wird in Form von Sternchen angezeigt.

- **Key (2** bis **4)**: Der RADIUS-Schlüssel, der den konfigurierten RADIUS-Backupservern 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.

- **Enable RADIUS Accounting**: Ermöglicht das Verfolgen und Messen der von einem bestimmten Benutzer verwendeten Ressourcen, beispielsweise Systemzeit, Menge der gesendeten und empfangenen Daten usw.

  Wenn Sie RADIUS-Benutzerkonten aktivieren, gilt dies für den primären RADIUS-Server und alle Backup-Server.

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

802.1X Supplicant

Durch die IEEE 802.1X-Authentifizierung erhält der Access Point Zugriff auf ein geschütztes drahtgebundenes Netzwerk. Sie können den Access Point im drahtgebundenen Netzwerk als 802.1X-Supplicant (Client) aktivieren. Sie können einen Benutzernamen und ein Kennwort konfigurieren, die mit dem MD5-Algorithmus verschlüsselt werden, um dem Access Point die Authentifizierung mit 802.1X zu ermöglichen.

In Netzwerken mit portbasierter IEEE 802.1X-Netzwerkzugangskontrolle erhält ein Supplicant nur dann Zugriff auf das Netzwerk, wenn der 802.1X-Authentifikator den Zugriff gewährt. Wenn im Netzwerk 802.1X verwendet wird, müssen Sie im WAP-Gerät 802.1X-Authentifizierungsinformationen konfigurieren, damit diese dem Authentifikator bereitgestellt werden können.

Die Seite **802.1X Supplicant** ist in drei Bereiche unterteilt: **Supplicant Configuration**, **Certificate File Status** und **Certificate File Upload**.

Im Bereich **Supplicant Configuration** können Sie den 802.1X-Betriebsstatus und Basiseinstellungen konfigurieren.

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **System Security** > **802.1X Supplicant** aus.

SCHRITT 2 Klicken Sie auf **Aktualisieren**, um den Bereich **Certificate File Status** zu aktualisieren.

SCHRITT 3 Geben Sie die folgenden Parameter ein:

- **Administrative Mode**: Aktiviert die 802.1X-Supplicant-Funktion.
- **EAP Method**: Der Algorithmus, der zum Verschlüsseln von Benutzernamen und Kennwörtern für die Authentifizierung verwendet wird

- **MD5**: Eine in RFC 3748 definierte Hash-Funktion, die grundlegende Sicherheit bietet
- **PEAP**: Ein Protokoll (Protected Extensible Authentication Protocol), das durch Kapselung in einem TLS-Tunnel mehr Sicherheit als MD5 bietet
- **TLS**: Transport Layer Security, ein in RFC 5216 definierter offener Standard, der hohe Sicherheit bietet

- **Username**: Diesen Benutzernamen verwendet das WAP-Gerät für Antworten auf Anfragen eines 802.1X-Authentifikators. Der Benutzername kann aus 1 bis 64 Zeichen bestehen. Zulässig sind druckbare ASCII-Zeichen, das heißt Groß- und Kleinbuchstaben, Ziffern und alle Sonderzeichen mit Ausnahme von Fragezeichen.
- **Password**: Dieses MD5-Kennwort verwendet das WAP-Gerät für Antworten auf Anfragen eines 802.1X-Authentifikators. Das Kennwort kann aus 1 bis 64 Zeichen bestehen. Zulässig sind druckbare ASCII-Zeichen, das heißt Groß- und Kleinbuchstaben, Ziffern und alle Sonderzeichen mit Ausnahme von Fragezeichen.

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

HINWEIS Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

Im Bereich **Certificate File Status** wird angezeigt, ob ein aktuelles Zertifikat vorhanden ist:

- **Certificate File Present**: Gibt an, ob das HTTP-SSL-Zertifikatdatei vorhanden ist. Wenn die Datei vorhanden ist, wird im Feld **Ja** angezeigt. Die Standardeinstellung lautet **Nein**.
- **Certificate Expiration Date**: Gibt an, wann das HTTP-SSL-Zertifikat abläuft. Möglich ist ein gültiges Datum.

Im Bereich **Certificate File Upload** können Sie eine Zertifikatdatei in das WAP-Gerät hochladen:

SCHRITT 1 Wählen Sie für **Transfer Method** die Option **HTTP** oder **TFTP** aus.

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

> **HINWEIS** Informationen zum Konfigurieren der HTTP- und HTTPS-Servereinstellungen finden Sie unter **HTTP/HTTPS Service**.

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

SCHRITT 3 Klicken Sie auf **Upload**.

Daraufhin wird ein Bestätigungsfenster angezeigt, gefolgt von einem Fortschrittsbalken, aus dem der Status des Uploads hervorgeht.

Password Complexity

Sie können Anforderungen für die Komplexität der Kennwörter konfigurieren, die für den Zugriff auf das Konfigurationsdienstprogramm für das WAP-Gerät verwendet werden. Komplexe Kennwörter erhöhen die Sicherheit allgemein.

So konfigurieren Sie die Anforderungen für die Kennwortkomplexität:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **System Security** > **Password Complexity** aus.

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

SCHRITT 3 Konfigurieren Sie die folgenden Parameter:

- **Password Minimum Character Class**: Die Mindestanzahl an Zeichenklassen, die in der Kennwortzeichenfolge enthalten sein müssen. Folgende vier Zeichenklassen sind möglich: Großbuchstaben, Kleinbuchstaben, Zahlen und auf einer Standardtastatur verfügbare Sonderzeichen.
- **Password Different From Current**: Wählen Sie diese Option aus, damit Benutzer nach Ablauf des aktuellen Kennworts ein anderes Kennwort eingeben müssen. Wenn diese Option nicht ausgewählt ist, können Benutzer nach Ablauf eines Kennworts wieder das gleiche Kennwort eingeben.

- **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**.
- **Password Aging Support**: Wählen Sie diese Option aus, damit Kennwörter nach einem konfigurierten Zeitraum 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 Complexity

Wenn Sie VAPs im WAP-Gerät konfigurieren, können Sie eine Methode für die sichere Authentifizierung von Clients auswählen. Wenn Sie das WPA-Personal-Protokoll (das auch als WPA Pre-Shared Key oder WPA-PSK bezeichnet wird) als Sicherheitsmethode für einen VAP auswählen, können Sie auf der Seite **WPA-PSK Complexity** die Komplexitätsanforderungen für den beim Authentifizierungsprozess verwendeten Schlüssel konfigurieren. Komplexere Schlüssel bieten höhere Sicherheit.

So konfigurieren Sie die WPA-PSK-Komplexität:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **System Security** > **WPA-PSK Complexity** 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 Kontrollkästchen deaktivieren, wird keine dieser Einstellungen verwendet. **WPA-PSK Complexity** ist standardmäßig deaktiviert.

SCHRITT 3 Konfigurieren Sie die folgenden Parameter:

- **WPA-PSK Minimum Character Class**: Die Mindestanzahl an Zeichenklassen, die in der Schlüsselzeichenfolge enthalten sein müssen. Folgende vier Zeichenklassen sind möglich: Großbuchstaben, Kleinbuchstaben, Zahlen und auf einer Standardtastatur verfügbare Sonderzeichen. Standardmäßig werden drei Zeichenklassen verwendet.

- **WPA-PSK Different From Current**: Wählen Sie eine der folgenden Optionen aus:
  - **Enable**: Benutzer müssen nach Ablauf des aktuellen Schlüssels einen anderen Schlüssel konfigurieren.
  - **Disable**: Benutzer können nach Ablauf des aktuellen Schlüssels den alten oder vorherigen Schlüssel verwenden.
- **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.

7

Quality of Service für Clients

Dieses Kapitel enthält eine Übersicht über Quality of Service (QoS, Servicequalität) für Clients und Erläuterungen der QoS-Funktionen im Menü **Client QoS**. Das Kapitel umfasst die folgenden Themen:

- **Client QoS Global Settings**
- **ACL**
- **Klassenzuordnung**
- **Richtlinienzuordnung**
- **Client QoS Association**
- **Client QoS Status**

Client QoS Global Settings

Auf der Seite **Client QoS Global Settings** können Sie die Quality of Service-Funktion für das WAP-Gerät aktivieren oder deaktivieren.

Wenn Sie **Client QoS Mode** deaktivieren, werden alle ACLs, Ratenbegrenzungen und DiffServ-Konfigurationen global deaktiviert.

Wenn Sie diesen Modus aktivieren, können Sie auch den Modus **Client QoS** für bestimmte VAPs aktivieren oder deaktivieren. Informationen hierzu finden Sie im Abschnitt zur Einstellung **Client QoS Mode** auf der Seite *Client QoS Association*.

ACL

Bei ACLs handelt es sich um eine Sammlung von Bedingungen zum Zulassen bzw. Verweigern des Zugriffs, die als Regeln bezeichnet werden. Sie bieten Sicherheit, indem sie nicht autorisierte Benutzer blockieren und autorisierten Benutzern den Zugriff auf bestimmte Ressourcen gewähren. Mit ACLs können Sie ungerechtfertigte Zugriffsversuche auf Netzwerkressourcen blockieren.

Das WAP-Gerät unterstützt bis zu 50 IPv4-, IPv6- und MAC-ACLs.

IP-ACLs klassifizieren Verkehr für Layer 3 und 4.

Jede ACL besteht aus zehn Regeln, die auf den vom WAP-Gerät gesendeten oder empfangenen Verkehr angewendet werden. Jede Regel gibt an, ob der Inhalt eines bestimmten Felds verwendet werden soll, um den Zugriff auf das Netzwerk zuzulassen oder zu verweigern. Regeln können auf verschiedenen Kriterien basieren und für ein oder mehrere Felder in einem Paket gelten, beispielsweise für die IP-Quell- oder IP-Zieladresse, den Quell- oder Zielport oder das im Paket enthaltene Protokoll.

HINWEIS Am Ende jeder erstellten Regel ist implizit eine Verweigerung vorgesehen. Um die Verweigerung des gesamten Verkehrs zu verhindern, sollten Sie unbedingt in der ACL eine Zulassungsregel hinzufügen, die den Verkehr zulässt.

Bei MAC-ACLs handelt es sich um Layer-2-ACLs. Sie können die Regeln so konfigurieren, dass Felder eines Frames überprüft werden, beispielsweise die MAC-Quelladresse oder -Zieladresse, die VLAN-ID oder die Class of Service. Wenn ein Frame am Port des WAP-Geräts eingeht oder diesen verlässt (abhängig davon, ob die ACL in ein- oder ausgehender Richtung angewendet wird), überprüft das WAP-Gerät den Frame und gleicht die ACL-Regeln mit dem Frame-Inhalt ab. Wenn der Inhalt mit einer der Regeln übereinstimmt, wird der Frame zugelassen oder verweigert.

Konfigurieren Sie auf der Seite **ACL Configuration** ACLs und Regeln, und wenden Sie dann die Regeln auf einen angegebenen VAP an.

Diese Schritte dienen als allgemeine Beschreibung für das Konfigurieren von ACLs:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Client QoS** > **ACL** aus.

SCHRITT 2 Geben Sie einen Namen für die ACL an.

SCHRITT 3 Wählen Sie den Typ der hinzuzufügenden ACL aus.

SCHRITT 4 Fügen Sie die ACL hinzu.

SCHRITT 5 Fügen Sie der ACL neue Regeln hinzu.

SCHRITT 6 Konfigurieren Sie die Übereinstimmungskriterien für die Regeln.

SCHRITT 7 Wenden Sie auf der Seite **Client QoS Association** die ACL auf einen oder mehrere VAPs an.

Diese Schritte dienen als detaillierte Beschreibung für das Konfigurieren von ACLs:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Client QoS** > **ACL** aus.

SCHRITT 2 Geben Sie diese Parameter ein, um eine neue ACL zu erstellen:

- **ACL Name**: Ein Name zur Identifizierung der ACL. Der ACL-Name kann 1 bis 31 alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: Bindestrich, Unterstrich, umgekehrter Schrägstrich und Doppelpunkt. Leerzeichen sind nicht zulässig.
- **ACL Type**: Der Typ der zu konfigurierenden ACL:
  - IPv4
  - IPv6
  - MAC

  IPv4- und IPv6-ACLs steuern den Zugriff auf Netzwerkressourcen auf der Grundlage von Layer-3- und Layer-4-Kriterien. MAC-ACLs steuern den Zugriff auf der Grundlage von Layer-2-Kriterien.

SCHRITT 3 Klicken Sie auf **Add ACL**.

Auf der Seite werden zusätzliche Felder zum Konfigurieren der ACL angezeigt.

SCHRITT 4 Konfigurieren Sie die Regelparameter:

- **ACL Name - ACL Type**: Die mit der neuen Regel zu konfigurierende ACL. Die Liste enthält alle ACLs, die Sie im Abschnitt **ACL Configuration** hinzugefügt haben.
- **Rule**: Die auszuführende Aktion:
  - Wählen Sie **New Rule** aus, um eine neue Regel für die ausgewählte ACL zu konfigurieren.

- Wenn bereits Regeln vorhanden sind (auch wenn diese zur Verwendung mit anderen ACLs erstellt wurden), können Sie die Regelnummer auswählen, um die Regel der ausgewählten ACL hinzuzufügen oder die Regeln zu ändern.

Wenn für eine ACL mehrere Regeln vorhanden sind, werden die Regeln in der Reihenfolge auf das Paket bzw. den Frame angewendet, in der Sie sie der ACL hinzugefügt haben. Die letzte Regel sieht implizit die Verweigerung des gesamten Verkehrs vor.

- **Action**: Gibt an, ob die ACL-Regel eine Aktion zulässt oder verweigert.

  Wenn Sie **Permit** auswählen, lässt die Regel für sämtlichen den Regelkriterien entsprechenden Verkehr zu, dass dieser beim WAP-Gerät eingeht oder das WAP-Gerät verlässt (abhängig von der ausgewählten ACL-Richtung). Verkehr, der nicht den Kriterien entspricht, wird gelöscht.

  Wenn Sie **Deny** auswählen, verhindert die Regel für sämtlichen den Regelkriterien entsprechenden Verkehr, dass dieser beim WAP-Gerät eingeht oder das WAP-Gerät verlässt (abhängig von der ausgewählten ACL-Richtung). Nicht den Kriterien entsprechender Verkehr wird weitergeleitet, sofern es sich nicht um die letzte Regel handelt. Da sich am Ende jeder ACL eine Regel befindet, die implizit den gesamten Verkehr verweigert, wird nicht ausdrücklich zugelassener Verkehr gelöscht.

- **Match Every Packet**: Wenn Sie die Option auswählen, gleicht die Regel, die das Zulassen oder Verweigern vorsieht, den Frame oder das Paket unabhängig vom Inhalt ab.

  Wenn Sie dieses Feld auswählen, können Sie keine weiteren Übereinstimmungskriterien konfigurieren. Die Option **Match Every Packet** ist für neue Regeln standardmäßig ausgewählt. Sie müssen die Option deaktivieren, um andere Übereinstimmungsfelder zu konfigurieren.

Konfigurieren Sie für IPv4-ACLs die folgenden Parameter:

- **Protocol**: Wählen Sie das Feld **Protocol** aus, um eine Layer-3- oder Layer-4-Übereinstimmungsbedingung zu verwenden, die auf dem Wert des Felds **IP Protocol** in IPv4-Paketen oder dem Feld **Next Header** in IPv6-Paketen basiert.

  Wenn Sie **Protocol** ausgewählt haben, wählen Sie eine der folgenden Optionen aus:

  - **Select From List**: Wählen Sie eines dieser Protokolle aus: IP, ICMP, IGMP, TCP oder UDP.

- **Match to Value**: Geben Sie eine von IANA zugewiesene Standardprotokoll-ID von 0 bis 255 ein. Wählen Sie diese Methode aus, um ein Protokoll anzugeben, dessen Name in **Select From List** nicht aufgeführt ist.

- **Source IP Address**: Gibt an, dass die IP-Quelladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Geben Sie eine IP-Adresse in das entsprechende Feld ein, um dieses Kriterium anzuwenden.

- **Wild Card Mask**: Die Platzhaltermaske für die IP-Quelladresse.

  Die Platzhaltermaske bestimmt, welche Bits verwendet und welche Bits ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit wichtig ist. Die Platzhaltermaske 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn **Source IP Address** aktiviert ist.

  Eine Platzhaltermaske ist im Grunde das Gegenteil einer Subnetzmaske. Wenn Sie beispielsweise die Kriterien mit einer einzelnen Hostadresse abgleichen möchten, verwenden Sie die Platzhaltermaske 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (beispielsweise 192.168.10.0/24) abgleichen möchten, verwenden Sie die Platzhaltermaske 0.0.0.255.

- **Source Port**: Schließt einen Quellport in die Übereinstimmungsbedingungen für die Regel ein. Der Quellport wird im Datagramm-Header identifiziert.

  Wenn Sie **Source Port** ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.

  - **Select From List**: Das dem Quellport entsprechende Schlüsselwort, das abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Jedes dieser Schlüsselwörter wird in die entsprechende Portnummer umgewandelt.

  - **Match to Port**: Die IANA-Portnummer, die mit dem im Datagramm-Header identifizierten Quellport abgeglichen werden soll. Möglich sind Ports im Bereich von 0 bis 65535. Dazu gehören drei verschiedene Porttypen:

    0 bis 1023: Allgemein bekannte Ports

    1024 bis 49151: Registrierte Ports

    49152 bis 65535: Dynamische und/oder private Ports

- **Destination IP Address**: Gibt an, dass die IP-Zieladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Geben Sie eine IP-Adresse in das entsprechende Feld ein, um dieses Kriterium anzuwenden.
- **Wild Card Mask**: Die Platzhaltermaske für die IP-Zieladresse.

  Die Platzhaltermaske bestimmt, welche Bits verwendet und welche Bits ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit wichtig ist. Die Platzhaltermaske 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn **Source IP Address** ausgewählt ist.

  Eine Platzhaltermaske ist im Grunde das Gegenteil einer Subnetzmaske. Wenn Sie beispielsweise die Kriterien mit einer einzelnen Hostadresse abgleichen möchten, verwenden Sie die Platzhaltermaske 0.0.0.0. Wenn Sie die Kriterien mit einem 24-Bit-Subnetz (beispielsweise 192.168.10.0/24) abgleichen möchten, verwenden Sie die Platzhaltermaske 0.0.0.255.
- **Destination Port**: Schließt einen Zielport in die Übereinstimmungsbedingung für die Regel ein. Der Zielport wird im Datagramm-Header identifiziert.

  Wenn Sie **Destination Port** ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.

  - **Select From List**: Wählen Sie das dem Zielport entsprechende Schlüsselwort aus, das abgeglichen werden soll: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Jedes dieser Schlüsselwörter wird in die entsprechende Portnummer umgewandelt.
  - **Match to Port**: Die IANA-Portnummer, die mit dem im Datagramm-Header identifizierten Zielport abgeglichen werden soll. Möglich sind Ports im Bereich von 0 bis 65535. Dazu gehören drei verschiedene Porttypen:

    0 bis 1023: Allgemein bekannte Ports

    1024 bis 49151: Registrierte Ports

    49152 bis 65535: Dynamische und/oder private Ports
- **IP DSCP**: Gleicht Pakete auf der Grundlage des IP-DSCP-Werts ab.

  Wenn Sie **IP DSCP** ausgewählt haben, wählen Sie eine dieser Optionen als Übereinstimmungskriterium aus:

- **Select From List**: DSCP-Werte für **Assured Forwarding (AS)**, **Class of Service (CS)** oder **Expedited Forwarding (EF)**.
- **Match to Value**: Ein benutzerdefinierter DSCP-Wert von 0 bis 63

- **IP Precedence**: Gleicht Pakete auf der Grundlage des Werts für **IP Precedence** ab. Wenn Sie diese Option auswählen, geben Sie für **IP Precedence** einen Wert von 0 bis 7 ein.
- **IP TOS Bits**: Gibt einen Wert für die Verwendung der Type of Service-Bits im IP-Header als Übereinstimmungskriterium an.

  Das IP-TOS-Feld in einem Paket ist definiert als alle acht Bits des Service Type-Oktetts im IP-Header. Der Wert von **IP TOS Bits** ist eine zweistellige hexadezimale Zahl von 00 bis ff.

  Die drei Bits höherer Ordnung stellen den Wert für den IP-Vorrang dar. Die sechs Bits höherer Ordnung stellen den IP-DSCP-Wert (IP Differentiated Services Code Point) dar.
- **IP TOS Mask**: Geben Sie einen Wert für **IP TOS Mask** ein, um die Bitpositionen im Wert **IP TOS Bits** zu identifizieren, die für den Vergleich mit dem IP-TOS-Feld in einem Paket verwendet werden.

  Der Wert von **IP TOS Mask** ist eine zweistellige hexadezimale Zahl von 00 bis FF, die eine umgekehrte Maske (das heißt eine Platzhaltermaske) darstellt. Die Bits mit dem Wert **0** in **IP TOS Mask** geben die Bitpositionen im Wert **IP TOS Bits** an, der für den Vergleich mit dem IP-TOS-Feld eines Pakets verwendet wird. Wenn Sie beispielsweise einen IP-TOS-Wert überprüfen möchten, bei dem die Bits 7 und 5 festgelegt sind und Bit 1 leer ist, wobei Bit 7 am wichtigsten ist, verwenden Sie für **IP TOS Bits** den Wert **0** und für **IP TOS Mask** die Maske **00**.

Konfigurieren Sie für IPv6-ACLs die folgenden Parameter:

- **Protocol**: Wählen Sie das Feld **Protocol** aus, um eine Layer-3- oder Layer-4-Übereinstimmungsbedingung zu verwenden, die auf dem Wert des Felds **IP Protocol** in IPv4-Paketen oder dem Feld **Next Header** in IPv6-Paketen basiert.

  Wenn Sie dieses Feld ausgewählt haben, wählen Sie das Protokoll aus, das anhand des Schlüsselworts oder der Protokoll-ID abgeglichen werden soll.
- **Source IPv6 Address**: Wählen Sie dieses Feld aus, um festzulegen, dass die IPv6-Quelladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Geben Sie eine IPv6-Adresse in das entsprechende Feld ein, um dieses Kriterium anzuwenden.

- **Source IPv6 Prefix Length**: Geben Sie die Präfixlänge der IPv6-Quelladresse ein.
- **Source Port**: Wählen Sie diese Option aus, um einen Quellport in die Übereinstimmungsbedingung für die Regel einzuschließen. Der Quellport wird im Datagramm-Header identifiziert. Wenn Sie diese Option ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.
- **Destination IPv6 Address**: Wählen Sie dieses Feld aus, um festzulegen, dass die IPv6-Zieladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Geben Sie eine IPv6-Adresse in das entsprechende Feld ein, um dieses Kriterium anzuwenden.
- **Destination IPv6 Prefix Length**: Geben Sie die Präfixlänge der IPv6-Zieladresse ein.
- **Destination Port**: Wählen Sie diese Option aus, um einen Zielport in die Übereinstimmungsbedingung für die Regel einzuschließen. Der Zielport wird im Datagramm-Header identifiziert. Wenn Sie diese Option ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.
- **IPv6 Flow Label**: Eine für ein IPv6-Paket eindeutige 20-Bit-Zahl. Die Zahl wird von Endstationen verwendet, um die QoS-Behandlung in Routern anzugeben (Bereich von 0 bis 1048575).
- **IP DSCP**: Gleicht Pakete auf der Grundlage des IP-DSCP-Werts ab. Wenn Sie diese Option ausgewählt haben, wählen Sie eine der folgenden Optionen als Übereinstimmungskriterium aus:
  - **Select From List**: DSCP-Werte für **Assured Forwarding (AS)**, **Class of Service (CS)** oder **Expedited Forwarding (EF)**.
  - **Match to Value**: Ein benutzerdefinierter DSCP-Wert von 0 bis 63

Konfigurieren Sie für eine MAC-ACL die folgenden Parameter:

- **EtherType**: Wählen Sie diese Option aus, um die Übereinstimmungskriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen.

  Wählen Sie ein EtherType-Schlüsselwort aus, oder geben Sie einen EtherType-Wert ein, um die Übereinstimmungskriterien anzugeben.
  - **Select from List**: Wählen Sie einen dieser Protokolltypen aus: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.
  - **Match to Value**: Geben Sie eine benutzerdefinierte Protokoll-ID ein, mit der Pakete abgeglichen werden sollen. Der Wert ist eine vierstellige hexadezimale Zahl im Bereich von 0600 bis FFFF.

- **Class of Service**: Wählen Sie dieses Feld aus, und 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 Address**: Wählen Sie dieses Feld aus, und geben Sie die MAC-Quelladresse ein, die mit einem Ethernet-Frame verglichen werden soll.

- **Source MAC Mask**: Wählen Sie dieses Feld aus, und geben Sie die MAC-Quelladressmaske ein. Geben Sie dabei an, welche Bits in der Quell-MAC mit einem Ethernet-Frame verglichen werden sollen.

  Für jede Bitposition in der MAC-Maske gibt eine 0 an, dass das entsprechende Adressbit wichtig ist. Eine 1 gibt an, dass das Adressbit ignoriert wird. Wenn beispielsweise nur die ersten vier Oktette einer MAC-Adresse verglichen werden sollen, wird die MAC-Maske 00:00:00:00:ff:ff verwendet. Die MAC-Maske 00:00:00:00:00:00 wird verwendet, um alle Adressbits zu überprüfen und eine einzelne MAC-Adresse abzugleichen.

- **Destination MAC Address**: Wählen Sie dieses Feld aus, und geben Sie die MAC-Zieladresse ein, die mit einem Ethernet-Frame verglichen werden soll.

- **Destination MAC Mask**: Geben Sie die MAC-Zieladressmaske ein, um anzugeben, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.

  Für jede Bitposition in der MAC-Maske gibt eine 0 an, dass das entsprechende Adressbit wichtig ist. Eine 1 gibt an, dass das Adressbit ignoriert wird. Wenn beispielsweise nur die ersten vier Oktette einer MAC-Adresse verglichen werden sollen, wird die MAC-Maske 00:00:00:00:ff:ff verwendet. Die MAC-Maske 00:00:00:00:00:00 wird verwendet, um alle Adressbits zu überprüfen und eine einzelne MAC-Adresse abzugleichen.

- **VLAN ID**: Wählen Sie dieses Feld aus, und geben Sie die konkrete VLAN-ID ein, die mit einem Ethernet-Frame verglichen werden soll.

  Dieses Feld befindet sich im ersten bzw. einzigen 802.1Q-VLAN-Tag.

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

HINWEIS Zum Löschen einer ACL stellen Sie sicher, dass die ACL in der Liste **ACL Name-ACL Type** ausgewählt ist, wählen Sie **Delete ACL** aus, und klicken Sie auf **Speichern**.

Klassenzuordnung

Die Client-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.

So fügen Sie eine Klassenzuordnung hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Client QoS** > **Class Map** aus.

SCHRITT 2 Geben Sie in **Class Map Name** einen Klassenzuordnungsnamen ein. Der Name kann 1 bis 31 alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: Bindestrich, Unterstrich, umgekehrter Schrägstrich und Doppelpunkt. Leerzeichen sind nicht zulässig.

SCHRITT 3 Wählen Sie in der Liste **Match Layer 3 Protocol** einen Wert aus:

- **IPv4**: Die Klassenzuordnung gilt nur für IPv4-Verkehr im WAP-Gerät.
- **IPv6**: Die Klassenzuordnung gilt nur für IPv6-Verkehr im WAP-Gerät.

Die Seite **Class Map** wird angezeigt. Sie enthält abhängig vom ausgewählten Layer-3-Protokoll zusätzliche Felder:

Verwenden Sie die Felder im Bereich **Match Criteria Configuration**, um Pakete einer Klasse zuzuordnen. Aktivieren Sie die Kontrollkästchen der einzelnen Felder, die als Kriterien für eine Klasse verwendet werden sollen, und geben Sie Daten in das zugehörige Feld ein. Eine Klasse kann mehrere Übereinstimmungskriterien enthalten.

Welche Felder für Übereinstimmungskriterien verfügbar sind, hängt davon ab, ob es sich um eine IPv4- oder IPv6-Klassenzuordnung handelt.

So konfigurieren Sie eine Klassenzuordnung:

SCHRITT 1 Wählen Sie in der Liste **Class Map Name** die Klassenzuordnung aus.

SCHRITT 2 Konfigurieren Sie die Parameter (wenn Parameter nur für IPv4- oder IPv6-Klassenzuordnungen angezeigt werden, wird darauf hingewiesen):

- **Match Every Packet**: Die Übereinstimmungsbedingung gilt für alle Parameter in einem Layer-3-Paket.

  Wenn diese Option ausgewählt ist, entsprechen alle Layer-3-Pakete der Bedingung.

- **Protocol**: Verwenden Sie eine Layer-3- oder Layer-4-Übereinstimmungsbedingung, die auf dem Wert des Felds **IP Protocol** in IPv4-Paketen oder dem Feld **Next Header** in IPv6-Paketen basiert.

  Wenn Sie dieses Feld ausgewählt haben, wählen Sie das Protokoll aus, das anhand des Schlüsselworts abgeglichen werden soll, oder geben Sie eine Protokoll-ID ein.

  - **Select From List**: Das ausgewählte Protokoll wird abgeglichen: IP, ICMP, IPv6, ICMPv6, IGMP, TCP, UDP.

  - **Match to Value**: 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.

- **Source IP Address** oder **Source IPv6 Address**: Gibt an, dass die IP-Quelladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Aktivieren Sie das Kontrollkästchen, und geben Sie eine IP-Adresse ein.

- **Source IP Mask** (nur IPv4): Die IP-Quelladressmaske.

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.

- **Source IPv6 Prefix Length** (nur IPv6): Die Präfixlänge der IPv6-Quelladresse
- **Destination IP Address** oder **Destination IPv6 Address**: Gibt an, dass die IP-Zieladresse eines Pakets mit der hier aufgeführten Adresse übereinstimmen muss. Geben Sie eine IP-Adresse in das entsprechende Feld ein, um dieses Kriterium anzuwenden.
- **Destination IP Mask** (nur IPv4): Die IP-Zieladressmaske.

  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.
- **Destination IPv6 Prefix Length** (nur IPv6): Die Präfixlänge der IPv6-Zieladresse
- **IPv6 Flow Label** (nur IPv6): Eine für ein IPv6-Paket eindeutige 20-Bit-Zahl. Die Zahl wird von Endstationen verwendet, um die QoS-Behandlung in Routern anzugeben (Bereich von 0 bis 1048575).
- **IP DSCP**: Eine Beschreibung hierzu finden Sie im Abschnitt zu Diensttypfeldern.
- **Source Port**: Schließt einen Quellport in die Übereinstimmungsbedingungen für die Regel ein. Der Quellport wird im Datagramm-Header identifiziert.

Wenn Sie das Feld ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.

- **Select From List**: Gleicht ein dem Quellport zugeordnetes Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

  Jedes dieser Schlüsselwörter wird in die entsprechende Portnummer umgewandelt.

- **Match to Port**: Gleicht die Quellportnummer im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Möglich sind Ports im Bereich von 0 bis 65535. Dazu gehören drei verschiedene Porttypen:

  0 bis 1023: Allgemein bekannte Ports

  1024 bis 49151: Registrierte Ports

  49152 bis 65535: Dynamische und/oder private Ports

- **Destination Port**: Schließt einen Zielport in die Übereinstimmungsbedingung für die Regel ein. Der Zielport wird im Datagramm-Header identifiziert.

  Wenn Sie das Feld ausgewählt haben, wählen Sie den Portnamen aus, oder geben Sie die Portnummer ein.

  - **Select From List**: Gleicht die Zielportnummer im Datagramm-Header mit dem ausgewählten Schlüsselwort ab: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Jedes dieser Schlüsselwörter wird in die entsprechende Portnummer umgewandelt.

  - **Match to Port**: Gleicht den Zielport im Datagramm-Header mit einer angegebenen IANA-Portnummer ab. Möglich sind Ports im Bereich von 0 bis 65535. Dazu gehören drei verschiedene Porttypen:

    0 bis 1023: Allgemein bekannte Ports

    1024 bis 49151: Registrierte Ports

    49152 bis 65535: Dynamische und/oder private Ports

- **EtherType**: Vergleicht die Übereinstimmungskriterien mit dem Wert im Header eines Ethernet-Frames.

  Wählen Sie ein EtherType-Schlüsselwort aus, oder geben Sie einen EtherType-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.
  - **Match to Value**: Gleicht den Ethertype im Datagramm-Header mit einer angegebenen benutzerdefinierten Protokoll-ID ab. Der Wert kann eine vierstellige hexadezimale Zahl im Bereich von 0600 bis FFFF sein.

- **Class of Service**: Ein Wert für die Class of Service-802.1p-Benutzerpriorität, der für die Pakete abgeglichen werden soll. Gültig sind Werte im Bereich von 0 bis 7.
- **Source MAC Address**: Eine MAC-Quelladresse, die mit einem Ethernet-Frame verglichen werden soll
- **Source MAC Mask**: Die MAC-Quelladressmaske, die angibt, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.

  Für jede Bitposition in der MAC-Maske gibt eine 0 an, dass das entsprechende Adressbit wichtig ist. Eine 1 gibt an, dass das Adressbit ignoriert wird. Wenn beispielsweise nur die ersten vier Oktette einer MAC-Adresse verglichen werden sollen, wird die MAC-Maske 00:00:00:00:ff:ff verwendet. Die MAC-Maske 00:00:00:00:00:00 wird verwendet, um alle Adressbits zu überprüfen und eine einzelne MAC-Adresse abzugleichen.
- **Destination MAC Address**: Die MAC-Zieladresse, die mit einem Ethernet-Frame verglichen werden soll
- **Destination MAC Mask**: Die MAC-Zieladressmaske, die angibt, welche Bits in der Ziel-MAC mit einem Ethernet-Frame verglichen werden sollen.

  Für jede Bitposition in der MAC-Maske gibt eine 0 an, dass das entsprechende Adressbit wichtig ist. Eine 1 gibt an, dass das Adressbit ignoriert wird. Wenn beispielsweise nur die ersten vier Oktette einer MAC-Adresse verglichen werden sollen, wird die MAC-Maske 00:00:00:00:ff:ff verwendet. Die MAC-Maske 00:00:00:00:00:00 wird verwendet, um alle Adressbits zu überprüfen und eine einzelne MAC-Adresse abzugleichen.
- **VLAN ID**: Eine VLAN-ID, die für Pakete abgeglichen werden soll. Gültig sind VLAN-IDs im Bereich von 0 bis 4095.

Die folgenden Diensttypfelder werden nur für IPv4 angezeigt. Sie können einen Diensttyp angeben, der für den Abgleich von Paketen mit Klassenkriterien verwendet werden soll.

- **IP DSCP**: Ein DSCP-Wert (Differentiated Services Code Point), der als Übereinstimmungskriterium verwendet werden soll:

- **Select from List**: Eine Liste mit DSCP-Typen
- **Match to Value**: Ein von Ihnen angegebener DSCP-Wert von 0 bis 63

- **IP Precedence** (nur IPv4): Gleicht den Wert des Pakets für **IP Precedence** mit dem Wert des Klassenkriteriums für **IP Precedence** ab. Für **IP Precedence** sind Werte im Bereich von 0 bis 7 möglich.
- **IP TOS Bits** (nur IPv4): 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 drei Bits höherer Ordnung stellen den Wert für **IP Precedence** dar. Die sechs Bits höherer Ordnung stellen den IP-DSCP-Wert (IP Differentiated Services Code Point) dar.

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

HINWEIS Zum Löschen einer Klassenzuordnung wählen Sie diese in der Liste **Class Map Name** 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 **Policy Map**. 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.

So können Sie eine Richtlinienzuordnung hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Client QoS** > **Policy Map** aus.

SCHRITT 2 Geben Sie in **Policy Map Name** einen Richtlinienzuordnungsnamen ein. Der Name kann 1 bis 31 alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: Bindestrich, Unterstrich, umgekehrter Schrägstrich und Doppelpunkt. Leerzeichen sind nicht zulässig.

SCHRITT 3 Klicken Sie auf **Add Policy Map**. Die Seite wird mit zusätzlichen Feldern zum Konfigurieren der Richtlinienzuordnung aktualisiert.

SCHRITT 4 Vergewissern Sie sich im Bereich **Policy Class Definition**, dass die neu erstellte Richtlinienzuordnung in der Liste **Policy Map Name** angezeigt wird.

SCHRITT 5 Wählen Sie in der Liste **Class Map Name** die Klassenzuordnung aus, auf die Sie die Richtlinie anwenden möchten.

SCHRITT 6 Konfigurieren Sie die folgenden Parameter:

- **Police Simple**: 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 dieses Feld auswählen, konfigurieren Sie eines der folgenden Felder:
  - **Committed Rate**: Die vereinbarte Bitrate in KBit/s, der der Verkehr entsprechen muss. Möglich sind Werte im Bereich von 1 bis 1000000 KBit/s.
  - **Committed Burst**: Die vereinbarte Burst-Größe in Byte, der der Verkehr entsprechen muss. Möglich sind Werte im Bereich von 1 bis 204800000 Byte.
- **Send**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom weitergeleitet werden sollen, wenn das Klassenzuordnungskriterium erfüllt ist.
- **Drop**: Gibt an, dass alle Pakete für den zugeordneten Verkehrsstrom gelöscht werden sollen, wenn das Klassenzuordnungskriterium erfüllt ist.
- **Mark Class of Service**: 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.
- **Mark IP DSCP**: Markiert alle Pakete für den zugeordneten Verkehrsstrom mit dem IP-DSCP-Wert, den Sie in der Liste auswählen oder angeben.
  - **Select from List**: Eine Liste mit DSCP-Typen
  - **Match to Value**: Ein von Ihnen angegebener DSCP-Wert. Der Wert ist eine Ganzzahl zwischen 0 und 63.
- **Mark IP Precedence**: 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.

- **Disassociate Class Map**: Entfernt die in der Liste **Class Map Name** ausgewählte Klasse aus der in der Liste **Policy Map Name** ausgewählten Richtlinie.
- **Member Classes**: 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 7 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Löschen einer Richtlinienzuordnung wählen Sie diese in der Liste **Policy Map Name** aus, und klicken Sie auf **Löschen**.

Client QoS Association

Die Seite **Client QoS Association** ermöglicht eine umfassendere Steuerung bestimmter QoS-Aspekte von WLAN-Clients, die Verbindungen mit dem Netzwerk herstellen. Dazu gehört beispielsweise die Menge der Bandbreite, die ein einzelner Client senden und empfangen kann. Zum Steuern der allgemeinen Verkehrskategorien wie beispielsweise HTTP-Verkehr oder Verkehr aus einem bestimmten Subnetz können Sie ACLs konfigurieren und diese einem oder mehreren VAPs zuweisen.

Neben der Steuerung der allgemeinen Verkehrskategorien können Sie mit Client-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.

So konfigurieren Sie die Parameter für die Client-QoS-Zuordnung:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Client QoS** > **Client QoS Association** aus.

SCHRITT 2 Nur für WAP561-Geräte: Wählen Sie die Funkschnittstelle aus, für die Sie die Zuordnung konfigurieren möchten (**Radio 1** oder **Radio 2**).

SCHRITT 3 Wählen Sie in der VAP-Liste den VAP aus, für den Sie Client-QoS-Parameter konfigurieren möchten.

SCHRITT 4 Wählen Sie für **Client QoS Global** die Option **Aktivieren** aus, um die Funktion zu aktivieren.

SCHRITT 5 Konfigurieren Sie die folgenden Parameter für den ausgewählten VAP:

- **Client QoS Mode**: Wählen Sie **Aktivieren** aus, um die Client-QoS-Funktion für den ausgewählten VAP zu aktivieren.
- **Bandwidth Limit Down**: Die maximal zulässige Übertragungsrate vom WAP-Gerät zum Client in Bit pro Sekunde (Bit/s). Gültig sind Werte im Bereich von 0 bis 300 MBit/s.
- **Bandwidth Limit Up**: Die maximal zulässige Übertragungsrate vom Client zum WAP-Gerät in Bit pro Sekunde (Bit/s). Gültig sind Werte im Bereich von 0 bis 300 MBit/s.
- **ACL Type Down**: Der ACL-Typ, der auf Verkehr in ausgehender Richtung (vom WAP-Gerät zum Client) angewendet werden soll. Folgende Optionen sind verfügbar:
  - IPv4: Die ACL untersucht IPv4-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - IPv6: Die ACL untersucht IPv6-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - MAC: Die ACL untersucht Layer-2-Frames auf Übereinstimmungen mit ACL-Regeln.
- **ACL Name Down**: Der Name der ACL, die auf Verkehr in ausgehender Richtung angewendet wird.

  Nach der Vermittlung des Pakets oder Frames an die Ausgangsschnittstelle werden die ACL-Regeln auf eine Übereinstimmung überprüft. Zulässige Pakete bzw. Frames werden gesendet, und verweigerte Pakete oder Frames werden verworfen.
- **ACL Type Up**: Der ACL-Typ, der auf Verkehr in ausgehender Richtung (vom Client zum WAP-Gerät) angewendet wird. Folgende Optionen sind verfügbar:
  - IPv4: Die ACL untersucht IPv4-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - IPv6: Die ACL untersucht IPv6-Pakete auf Übereinstimmungen mit ACL-Regeln.

  - MAC: Die ACL untersucht Layer-2-Frames auf Übereinstimmungen mit ACL-Regeln.

- **ACL Name Up**: Der Name der ACL, die auf an das WAP-Gerät gesendeten Verkehr in eingehender Richtung angewendet wird

  Wenn ein Paket oder Frame vom WAP-Gerät empfangen wird, werden die ACL-Regeln auf eine Übereinstimmung überprüft. Zulässige Pakete bzw. Frames werden verarbeitet, und verweigerte Pakete oder Frames werden verworfen.

- **DiffServ Policy Down**: Der Name der DiffServ-Richtlinie, die auf vom WAP-Gerät gesendeten Verkehr in ausgehender Richtung (vom WAP-Gerät zum Client) angewendet wird

- **DiffServ Policy Up**: Der Name der DiffServ-Richtlinie, die auf an das WAP-Gerät gesendeten Verkehr in eingehender Richtung (vom Client zum WAP-Gerät) angewendet wird

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

Client QoS Status

Auf der Seite **Client QoS Status** werden die Client-QoS-Einstellungen angezeigt, die auf die einzelnen dem WAP-Gerät zurzeit zugeordneten Clients angewendet werden.

Zum Anzeigen der Seite **Client QoS Status** wählen Sie im Navigationsbereich die Option **Client QoS** > **Client QoS Status** aus.

Mit den folgenden Feldern können Sie die Option **Client QoS Status** konfigurieren:

- **Station**: Das Menü **Station** enthält die MAC-Adressen aller Clients, die zurzeit dem WAP-Gerät zugeordnet sind. Zum Anzeigen der auf einen Client angewendeten QoS-Einstellungen wählen Sie in der Liste die entsprechende MAC-Adresse aus.

- **Global QoS Mode**: Gibt an, ob QoS global für das WAP-Gerät aktiviert ist. Diesen Status konfigurieren Sie auf der Seite *Client QoS Association*.

- **Client QoS Mode**: Gibt an, ob QoS für den zugeordneten VAP aktiviert ist. Diesen Status konfigurieren Sie auf der Seite *Client QoS Association*.

- **Bandwidth Limit Down**: Die maximal zulässige Übertragungsrate vom WAP-Gerät zum Client in Bit pro Sekunde (Bit/s). Gültig sind Werte im Bereich von 0 bis 4294967295 Bit/s.
- **Bandwidth Limit Up**: Die maximal zulässige Übertragungsrate vom Client zum WAP-Gerät in Bit pro Sekunde (Bit/s). Gültig sind Werte im Bereich von 0 bis 4294967295 Bit/s.
- **ACL Type Up**: Der ACL-Typ, der auf Verkehr in ausgehender Richtung (vom Client zum WAP-Gerät) angewendet wird. Folgende Optionen sind verfügbar:
  - IPv4: Die ACL untersucht IPv4-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - IPv6: Die ACL untersucht IPv6-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - MAC: Die ACL untersucht Layer-2-Frames auf Übereinstimmungen mit ACL-Regeln.
- **ACL Name Up**: Der Name der ACL, die auf an den WAP gesendeten Verkehr in eingehender Richtung angewendet wird. Wenn ein Paket oder Frame vom WAP empfangen wird, werden die ACL-Regeln auf eine Übereinstimmung überprüft. Zulässige Pakete bzw. Frames werden verarbeitet, und verweigerte Pakete oder Frames werden verworfen.
- **ACL Type Down**: Der ACL-Typ, der auf Verkehr in ausgehender Richtung (vom WAP zum Client) angewendet werden soll. Folgende Optionen sind verfügbar:
  - IPv4: Die ACL untersucht IPv4-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - IPv6: Die ACL untersucht IPv6-Pakete auf Übereinstimmungen mit ACL-Regeln.
  - MAC: Die ACL untersucht Layer-2-Frames auf Übereinstimmungen mit ACL-Regeln.
- **ACL Name Down**: Der Name der ACL, die auf Verkehr in ausgehender Richtung angewendet wird. Nach der Vermittlung des Pakets oder Frames an die Ausgangsschnittstelle werden die ACL-Regeln auf eine Übereinstimmung überprüft. Zulässige Pakete bzw. Frames werden gesendet, und verweigerte Pakete oder Frames werden verworfen.

- **DiffServ Policy Up**: Der Name der DiffServ-Richtlinie, die auf an das WAP-Gerät gesendeten Verkehr in eingehender Richtung (vom Client zum WAP-Gerät) angewendet wird
- **DiffServ Policy Down**: Der Name der DiffServ-Richtlinie, die auf vom WAP-Gerät gesendeten Verkehr in ausgehender Richtung (vom WAP-Gerät zum Client) angewendet wird

8

SNMP-Protokoll

In diesem Kapitel wird beschrieben, wie Sie das SNMP-Protokoll (Simple Network Management Protocol) konfigurieren, um Konfigurationen vorzunehmen und Statistiken zu sammeln.

Das Kapitel umfasst die folgenden Themen:

- **Allgemeine SNMP-Einstellungen**
- **Ansichten**
- **Gruppen**
- **Benutzer**
- **Ziele**

Allgemeine SNMP-Einstellungen

Auf der Seite **General** können Sie SNMP aktivieren und grundlegende Protokolleinstellungen konfigurieren.

So konfigurieren Sie allgemeine SNMP-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **SNMP** > **General** aus.

SCHRITT 2 Wählen Sie für die Einstellung **SNMP** die Option **Enabled** aus. SNMP ist standardmäßig deaktiviert.

SCHRITT 3 Geben Sie in **UDP Port** einen UDP-Port für SNMP-Verkehr an.

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. Gültig sind Werte im Bereich von 1025 bis 65535.

SCHRITT 4 Konfigurieren Sie die folgenden SNMPv2-Einstellungen:

- **Read-only Community**: Ein schreibgeschützter Community-Name für den 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.

- **Read-write Community**: Community-Name mit Lese- und Schreibzugriff, der für SNMP-SET-Anfragen verwendet wird. Gültig sind Werte mit 1 bis 256 alphanumerischen Zeichen und Sonderzeichen.

  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:

  - **All**: Die Gruppe der Stationen, die über SNMP auf das WAP-Gerät zugreifen können, ist nicht beschränkt.

  - **User Defined**: Die Gruppe der zulässigen SNMP-Anfragen ist auf die angegebenen beschränkt.

- **NMS, IPv4 Address/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. Dabei ist *Adresse* eine IP-Adresse und *Maskenlänge* die Anzahl der Maskenbits. Unterstützt

werden die Formate *Adresse/Maske* und *Adresse/Maskenlänge*. 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 Address/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**: Eine globale Community-Zeichenfolge (Community String), die SNMP-Traps zugeordnet ist. Vom Gerät gesendete Traps stellen diese Zeichenfolge als Community-Namen bereit. Gültig sind Werte mit 1 bis 60 alphanumerischen Zeichen und Sonderzeichen.
- **Trap Destination Table**: Eine Liste mit bis zu drei IP-Adressen oder Hostnamen, die SNMP-Traps empfangen sollen. Aktivieren Sie das Kontrollkästchen, und wählen Sie die Option für **Host IP Address Type** (IPv4 oder IPv6) aus, bevor Sie die Option für **Hostname/IP Address** 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. Aktivieren Sie das Kontrollkästchen **Enabled**, und wählen Sie die entsprechende Option für **Host IP Address Type** aus.

Beachten Sie außerdem den Hinweis zu Hostnamen im vorherigen Schritt.

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

HINWEIS Nach dem Speichern der neuen Einstellungen werden die entsprechenden Prozesse möglicherweise beendet und neu gestartet. 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.

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.

Das WAP-Gerät 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 die Option **SNMP** > **Views** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle **SNMPv3 Views** zu erstellen.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen in der neuen Zeile, und klicken Sie auf **Bearbeiten**:

- **View Name**: Geben Sie einen Namen zur Identifizierung der MIB-Ansicht ein. Ansichtsnamen können bis zu 32 alphanumerische Zeichen enthalten.
- **Type**: Wählen Sie aus, ob die Ansichtsunterstruktur oder die Gruppe der Unterstrukturen in der MIB-Ansicht ein- oder ausgeschlossen sein soll.
- **OID**: Geben Sie eine OID-Zeichenfolge für die Unterstruktur ein, die in der Ansicht ein- oder ausgeschlossen sein soll.

  Die Systemunterstruktur beispielsweise geben Sie mit der OID-Zeichenfolge .1.3.6.1.2.1.1 an.
- **Mask**: 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 Views** 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.

Das WAP-Gerät 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 Das WAP-Gerät unterstützt maximal acht Gruppen.

So können Sie eine SNMP-Gruppe hinzufügen und konfigurieren:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **SNMP** > **Groups** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle **SNMPv3 Groups** zu erstellen.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen für die neue Gruppe, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die folgenden Parameter:

- **Group Name**: Ein Name zur Identifizierung der Gruppe. Die Standardgruppennamen lauten **RO** und **RW**.

  Gruppennamen können bis zu 32 alphanumerische Zeichen enthalten.

- **Security Level**: 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.

- **Write Views**: 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.

- **Read Views**: 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 Groups** 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 WAP-Gerät keine SNMPv3-Standardbenutzer. Sie können bis zu acht Benutzer hinzufügen.

So fügen Sie SNMP-Benutzer hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **SNMP** > **Users** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**, um eine neue Zeile in der Tabelle **SNMPv3 Users** zu erstellen.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen in der neuen Zeile, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die folgenden Parameter:

- **User Name**: Ein Name zur Identifizierung des SNMPv3-Benutzers. Benutzernamen können bis zu 32 alphanumerische Zeichen enthalten.
- **Group**: Die Gruppe, der der Benutzer zugeordnet ist. Die Standardgruppen lauten **RWAuth**, **RWPriv** und **RO**. Auf der Seite **SNMP Groups** können Sie zusätzliche Gruppen definieren.
- **Authentication Type**: 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.
  - **None**: Für SNMPv3-Anfragen des Benutzers ist keine Authentifizierung erforderlich.
- **Authentication Pass Phrase** (Wenn Sie den Authentifizierungstyp MD5 angegeben haben): Ein Kennwort, mit dem der SNMP-Agent vom Benutzer gesendete Anfragen authentifizieren kann. Das Kennwort muss aus 8 bis 32 Zeichen bestehen.

- **Encryption Type**: 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.
  - **None**: Für SNMPv3-Anfragen des Benutzers ist kein Datenschutz erforderlich.
- **Encryption Pass Phrase** (Wenn Sie den Datenschutztyp DES angegeben haben): Ein Kennwort, das zum Verschlüsseln der SNMP-Anfragen verwendet werden soll. Das Kennwort muss aus 8 bis 32 Zeichen bestehen.

SCHRITT 5 Klicken Sie auf **Speichern**. Der Benutzer wird der Liste **SNMPv3 Users** 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-Versionen 1 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 Das WAP-Gerät unterstützt maximal acht Ziele.

So fügen Sie SNMP-Ziele hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **SNMP** > **Targets** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**. In der Tabelle wird eine neue Zeile erstellt.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen in der neuen Zeile, und klicken Sie auf **Bearbeiten**.

SCHRITT 4 Konfigurieren Sie die folgenden Parameter:

- **IP Address**: 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.
- **Users**: Geben Sie den Namen des SNMP-Benutzers ein, den Sie dem Ziel zuordnen möchten. Informationen zur Konfiguration der SNMP-Benutzer finden Sie auf der Seite **Benutzer**.

SCHRITT 5 Klicken Sie auf **Speichern**. Der Benutzer wird der Liste **SNMPv3 Targets** hinzugefügt, und die Änderungen werden in der Startkonfiguration gespeichert.

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

9

Captive Portal

In diesem Kapitel 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.

HINWEIS Die Captive Portal-Funktion ist in den WAP5xx-Geräten und im Cisco WAP321-Gerät verfügbar.

Authentifizierte Benutzer müssen anhand einer Datenbank der autorisierten Captive Portal-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 Überprüfungsmethdoen für die einzelnen VAPs oder SSIDs konfiguriert werden. Cisco WAP551- und WAP561-Geräte werden zurzeit gleichzeitig mit einigen für die CP-Authentifizierung konfigurierten VAPs und einigen für normale WLAN-Authentifizierungsverfahren wie beispielsweise WPA oder WPA Enterprise betrieben.

Das Kapitel enthält die folgenden Themen:

- **Globale Captive Portal-Konfiguration**
- **Instanzkonfiguration**
- **Instance Association**
- **Web Portal Customization**
- **Lokale Gruppen**
- **Lokale Benutzer**
- **Authenticated Clients**
- **Failed Authentication Clients**

Globale Captive Portal-Konfiguration

Auf der Seite **Global CP Configuration** können Sie den administrativen Status der CP-Funktion steuern und globale Einstellungen konfigurieren, die sich auf alle im WAP-Gerät konfigurierten Captive Portal-Instanzen auswirken.

So konfigurieren Sie globale CP-Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Captive Portal** > **Global Configuration** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Parameter:

- **Captive Portal Mode**: Aktiviert den CP-Betrieb im WAP-Gerät.
- **Authentication Timeout**: 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.
- **Additional 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 Portnummer zwischen 1025 und 65535 oder **80** ein. Der HTTP-Port und der HTTPS-Port können nicht identisch sein.
- **Additional HTTPS 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.

Im Bereich **Captive Portal Configuration Counters** werden schreibgeschützte CP-Informationen angezeigt:

- **Instance Count**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Instanzen. Es können maximal zwei Instanzen konfiguriert sein.

- **Group Count**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Gruppen. Es können maximal zwei Gruppen konfiguriert sein. Die **Default Group** ist standardmäßig vorhanden und kann nicht gelöscht werden.
- **User Count**: Die Anzahl der zurzeit im WAP-Gerät konfigurierten CP-Benutzer. Es können maximal 128 Benutzer konfiguriert sein.

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

Instanzkonfiguration

Sie können maximal zwei Captive Portal-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, fahren Sie mit **Netzwerke** fort, um einen VAP hinzuzufügen.
- Möchten Sie eine neue Gruppe hinzufügen? Wenn ja, fahren Sie mit **Lokale Gruppen** fort, um eine Gruppe hinzuzufügen.
- Möchten Sie einen neuen Benutzer hinzufügen? Wenn ja, fahren Sie mit **Lokale Benutzer** fort, um einen Benutzer hinzuzufügen.

So erstellen Sie eine CP-Instanz und konfigurieren die Einstellungen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Captive Portal** > **Instance Configuration** aus.

SCHRITT 2 Stellen Sie sicher, dass in der Liste **Captive Port Instances** die Option **Erstellen** ausgewählt ist.

SCHRITT 3 Geben Sie in **Instance Name** einen Instanznamen ein, und klicken Sie auf **Speichern**. Der Instanzname kann 1 bis 32 alphanumerische Zeichen und Unterstriche enthalten.

SCHRITT 4 Wählen Sie in der Liste **Captive Port Instances** den Instanznamen aus.

Daraufhin werden die Felder unter **Captive Portal Instance Parameters** mit zusätzlichen Optionen erneut angezeigt.

SCHRITT 5 Konfigurieren Sie die folgenden Parameter:

- **Instance ID**: Die Instanz-ID. Dieses Feld ist nicht konfigurierbar.
- **Administrative Mode**: Aktiviert und deaktiviert die CP-Instanz.
- **Protocol**: Gibt HTTP oder HTTPS als 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.
- **Verification**: Das Authentifizierungsverfahren, das vom CP zum Überprüfen von Clients verwendet wird:
  - **Guest**: Der Benutzer muss nicht anhand einer Datenbank authentifiziert werden.
  - **Local**: 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.
- **Redirect**: Gibt an, dass das CP den neu authentifizierten Client an die konfigurierte URL umleiten soll. Wenn diese Option deaktiviert ist, sehen die Benutzer nach der erfolgreichen Überprüfung die gebietsschemaspezifische Willkommensseite.
- **Redirect URL**: Geben Sie die URL (einschließlich **http://** oder **https://**) ein, an die der neu authentifizierte Client umgeleitet wird, wenn der URL-Umleitungsmodus aktiviert ist. Die zulässige Anzahl der Zeichen liegt zwischen 0 und 256 Zeichen.
- **Away Timeout**: Gibt an, wie lange ein Benutzer in der Liste der authentifizierten CP-Clients bleibt, nachdem die Zuordnung zum WAP-Gerät aufgehoben wurde. Wenn der in diesem Feld angegebene Zeitraum verstreicht, bevor der Client sich erneut zu authentifizieren versucht, wird der Clienteintrag aus der Liste der authentifizierten Clients entfernt. Möglich sind Werte im Bereich von 0 bis 1440 Minuten. Der Standardwert lautet **60 Minuten**.

HINWEIS Außerdem wird für jeden Benutzer ein Timeout-Wert bei Abwesenheit konfiguriert. Informationen hierzu finden Sie auf der Seite **Lokale 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.

- **Session Timeout**: Die in Sekunden verbleibende Zeit, 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**.
- **Maximum Bandwidth Upstream**: Die maximale Upload-Geschwindigkeit in Megabit pro Sekunde, 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 300 MBit/s. Der Standardwert lautet **0**.
- **Maximum Bandwidth Downstream**: Die maximale Download-Geschwindigkeit in Megabit pro Sekunde, 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 300 MBit/s. Der Standardwert lautet **0**.
- **User Group Name**: 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 Network**: Die vom RADIUS-Server verwendete IP-Version. Sie können zwischen den Adresstypen umschalten, um RADIUS-Adresseinstellungen für IPv4 und IPv6 zu konfigurieren. Das WAP-Gerät stellt jedoch nur Verbindungen mit den RADIUS-Servern des in diesem Feld ausgewählten Adresstyps her.
- **Global RADIUS**: Dieses Feld ist verfügbar, wenn der Überprüfungsmodus **RADIUS** entspricht. Die CP-Instanz verwendet standardmäßig die globalen RADIUS-Einstellungen, die Sie für das WAP-Gerät definieren (siehe **RADIUS-Server**). Sie können jedoch für jede Instanz andere RADIUS-Server konfigurieren. Wenn Sie die globalen RADIUS-Servereinstellungen verwenden möchten, muss das Kontrollkästchen aktiviert sein. Wenn Sie für die CP-Instanz einen separaten RADIUS-Server verwenden möchten, deaktivieren Sie das Kontrollkästchen, und geben Sie in die folgenden Felder **Server IP Address** und **Key** Werte ein.

- **RADIUS Accounting**: Ermöglicht das Verfolgen und Messen der von einem bestimmten Benutzer verwendeten Ressourcen, 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 Address 1** oder **Server IPv6 Address 1**: Die Adresse des primären RADIUS-Servers für diese CP-Instanz. 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 Address 2** bis **4** oder **Server IPv6 Address 2** bis **4**: Bis zu drei IPv4- oder IPv6-Adressen für RADIUS-Backup-Server. Wenn die Authentifizierung beim primären Server fehlschlägt, wird der Vorgang nacheinander mit den konfigurierten Backup-Servern wiederholt.
- **Key 1**: 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 mit dem auf dem RADIUS-Server konfigurierten Schlüssel übereinstimmen. Der eingegebene Text wird mit Sternchen maskiert.
- **Key 2** bis **Key 4**: Der RADIUS-Schlüssel, der den konfigurierten RADIUS-Backup-Servern zugeordnet ist. Der Server an Server-IP-Adresse (IPv6) 2 verwendet **Key 2**, der Server an Server-IP-Adresse (IPv6) 3 verwendet **Key 3** usw.
- **Locale Count**: 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.
- **Delete Instance**: Löscht die aktuelle Instanz.

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

Instance Association

Wenn Sie eine Instanz erstellen, können Sie diese auf der Seite **Instance Association** einem VAP zuordnen. Die Einstellungen für zugeordnete CP-Instanzen gelten für Benutzer, die sich gegenüber dem VAP zu authentifizieren versuchen.

So ordnen Sie eine Instanz einem VAP zu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Captive Portal** > **Instance Association** aus.

SCHRITT 2 Wählen Sie bei WAP561-Geräten die Funkschnittstelle aus, an der Sie eine Instanzzuordnung 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.

Web Portal Customization

Wenn die CP-Instanz einem VAP zugeordnet ist, 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 **Web Portal Customization** können Sie eindeutige Seiten für verschiedene Gebietsschemas im Netzwerk erstellen und den Text und die Bilder auf den Seiten anpassen.

So können Sie eine CP-Authentifizierungsseite erstellen und anpassen:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Captive Portal > Web Portal Customization** aus.

SCHRITT 2 Wählen Sie in der Liste **Captive Portal Web Locale** die Option **Erstellen** aus.

Sie können bis zu drei verschiedene Authentifizierungsseiten mit verschiedenen Gebietsschemas im Netzwerk erstellen.

SCHRITT 3 Geben Sie einen Wert für **Web Locale Name** ein, um diesen der Seite zuzuweisen. Der Name kann 1 bis 32 alphanumerische Zeichen und Unterstriche enthalten.

SCHRITT 4 Wählen Sie in der Liste **Captive Portal Instances** 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 5 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

SCHRITT 6 Wählen Sie in der Liste **Captive Portal Web Locale** das erstellte Gebietsschema aus.

Auf der Seite werden zusätzliche Felder zum Ändern des Gebietsschemas angezeigt. Die Felder **Locale ID** und **Instance Name** können Sie nicht bearbeiten. Die Felder, die Sie bearbeiten können, sind mit Standardwerten gefüllt.

SCHRITT 7 Konfigurieren Sie die folgenden Parameter:

- **Background Image Name**: Das Bild, das als Seitenhintergrund angezeigt werden soll. Sie können auf **Upload/Delete Custom Image** klicken, um Bilder für Captive Portal-Instanzen hochzuladen. Weitere Informationen hierzu finden Sie unter **Hochladen und Löschen von Bildern**.
- **Logo Image Name**: 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 hochgeladen haben, können Sie das Bild in der Liste auswählen.
- **Foreground color**: Der HTML-Code für die Vordergrundfarbe im sechsstelligen Hexadezimalformat. Möglich sind Werte im Bereich von 1 bis 32 Zeichen. Der Standardwert lautet **#999999**.
- **Background color**: Der HTML-Code für die Hintergrundfarbe im sechsstelligen Hexadezimalformat. Möglich sind Werte im Bereich von 1 bis 32 Zeichen. Der Standardwert lautet **#BFBFBF**.
- **Separator**: Der HTML-Code für die Farbe der dicken horizontalen Linie, 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**.

Locale Label: Eine aussagekräftige Beschriftung für das Gebietsschema (1 bis 32 Zeichen). Das Label muss der IANA Language Subtag Registry und dem optionalen Regionscode entsprechen. Beispiele: Englisch: *en*, Französisch: *fr*, Taiwanesisch: *zh-TW*. Standardmäßig ist das Gebietsschema **Englisch** festgelegt.

- **Locale**: Eine Abkürzung für das Gebietsschema (1 bis 32 Zeichen). Der Standardwert lautet **en**.
- **Account Image**: Die Bilddatei, die über dem Anmeldefeld angezeigt werden soll, und eine authentifizierte Anmeldung symbolisiert.
- **Account Label**: Der Text, mit dem Benutzer angewiesen werden, einen Benutzernamen einzugeben. Möglich sind Werte im Bereich von 1 bis 32 Zeichen.
- **User Label**: Das Label des Textfelds für den Benutzernamen. Möglich sind Werte im Bereich von 1 bis 32 Zeichen.
- **Password Label**: Das Label des Textfelds für das Benutzerkennwort. Möglich sind Werte im Bereich von 1 bis 64 Zeichen.
- **Button Label**: 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 **Connect**.
- **Fonts**: 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. Die zulässige Anzahl der Zeichen liegt zwischen 1 und 512 Zeichen. Der Standardwert lautet **MS UI Gothic, Arial, Sans-Serif**.
- **Browser Title**: 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**.
- **Browser Content**: 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**.
- **Content**: 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.**

- **Acceptance Use Policy**: Der Text, der im Feld **Acceptance Use Policy** angezeigt wird. Möglich sind Werte im Bereich von 1 bis 4096 Zeichen. Der Standardwert lautet **Acceptance Use Policy**.
- **Accept Label**: 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. Der Standardwert lautet **Check here to indicate that you have read and accepted the Acceptance Use Policy.**
- **No Accept Text**: Der Text, der in einem Popupfenster angezeigt wird, wenn Benutzer Anmeldeinformationen übermitteln, ohne das Kontrollkästchen **Acceptance Use Policy** zu aktivieren. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet **Error: You must acknowledge the Acceptance Use Policy before connecting!**.
- **Work In Progress Text**: Der Text, der während der Authentifizierung angezeigt wird. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet **Connecting, please be patient.....**
- **Denied Text**: Der Text, der angezeigt wird, wenn die Authentifizierung eines Benutzers fehlschlägt. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet **Error Invalid Credentials, please try again!**.
- **Welcome Title**: Der Text, der angezeigt wird, wenn der Client gegenüber dem VAP authentifiziert wurde. Möglich sind Werte im Bereich von 1 bis 128 Zeichen. Der Standardwert lautet **Congratulations**.
- **Welcome Content**: Der Text, der angezeigt wird, wenn der Client mit dem Netzwerk verbunden ist. Möglich sind Werte im Bereich von 1 bis 256 Zeichen. Der Standardwert lautet **You are now authorized and connected to the network**.
- **Delete Locale**: Löscht das aktuelle Gebietsschema.

SCHRITT 8 Klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

SCHRITT 9 Klicken Sie auf **Preview**, um die aktualisierte Seite anzuzeigen.

HINWEIS Sie können auf **Preview** 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 **Preview** klicken, um die Änderungen anzuzeigen.

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

So laden Sie binäre Grafikdateien in das WAP-Gerät hoch:

SCHRITT 1 Klicken Sie auf der Seite **Web Portal Customization** auf **Upload/Delete Custom Image** neben dem Feld **Background Image Name**, **Logo Image Name** oder **Account Image**.

Die Seite **Web Portal Custom Image** wird angezeigt.

SCHRITT 2 Wählen Sie durch Durchsuchen das Bild aus.

SCHRITT 3 Klicken Sie auf **Upload**.

SCHRITT 4 Klicken Sie auf **Zurück**, um zur Seite **Web Portal Custom Image** zurückzukehren.

SCHRITT 5 Wählen Sie in **Captive Portal Web Locale** das zu konfigurierende Gebietsschema für das Captive Portal-Web aus.

SCHRITT 6 Wählen Sie in den Feldern **Background Image Name**, **Logo Image Name** oder **Account Image** das neu hochgeladene Bild aus.

SCHRITT 7 Klicken Sie auf **Speichern**.

HINWEIS Zum Löschen eines Bilds wählen Sie das Bild auf der Seite **Web Portal Custom Image** in der Liste **Delete Web Customization Image** aus, und klicken Sie auf **Löschen**. Die Standardbilder können Sie nicht löschen.

Lokale Gruppen

Jeder lokale Benutzer wird einer Benutzergruppe zugewiesen. Jede Gruppe wird einer CP-Instanz zugewiesen. Die Gruppe erleichtert das Verwalten der Zuordnung von Benutzern zu CP-Instanzen.

Die integrierte Benutzergruppe **Default** kann nicht gelöscht werden. Sie können bis zu zwei zusätzliche Benutzergruppen erstellen.

So fügen Sie lokale Benutzergruppen hinzu:

SCHRITT 1 Wählen Sie im Navigationsbereich die Option **Captive Portal** > **Local Groups** aus.

SCHRITT 2 Geben in **Group Name** einen Gruppennamen ein, und klicken Sie auf **Speichern**. Die Änderungen werden in der Startkonfiguration gespeichert.

HINWEIS Zum Löschen einer Gruppe wählen Sie die Gruppe in der Liste **Captive Portal Groups** aus, aktivieren Sie das Kontrollkästchen **Delete Group**, und klicken Sie auf **Speichern**.

Lokale Benutzer

Sie können eine Captive Portal-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 **Local Users** 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 im Navigationsbereich die Option **Captive Portal** > **Local Users** aus.

SCHRITT 2 Geben Sie in **User Name** einen Benutzernamen ein, und klicken Sie auf **Speichern**.

Daraufhin werden zusätzliche Felder zum Konfigurieren des Benutzers angezeigt.

SCHRITT 3 Geben Sie die folgenden Parameter ein:

- **User Password**: 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.
- **Show Password as Clear Text**: Wenn diese Option aktiviert ist, wird der eingegebene Text angezeigt. Wenn die Option deaktiviert ist, wird der Text bei der Eingabe nicht maskiert.
- **Away Timeout**: 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.
- **Group Name**: Die zugewiesene Benutzergruppe. Jede CP-Instanz ist für die Unterstützung einer bestimmten Benutzergruppe konfiguriert.
- **Maximum Bandwidth Up**: Die maximale Upload-Geschwindigkeit in Megabit pro Sekunde, 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 300 MBit/s. Der Standardwert lautet **0**.
- **Maximum Bandwidth Down**: Die maximale Download-Geschwindigkeit in Megabit pro Sekunde, 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 300 MBit/s. Der Standardwert lautet **0**.
- **Delete User**: Löscht den aktuellen Benutzer.

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

Authenticated Clients

Die Seite **Authenticated Clients** enthält Informationen zu Clients, die in einer Captive Portal-Instanz authentifiziert wurden.

Zum Anzeigen der Liste der authentifizierten Clients wählen Sie im Navigationsbereich die Option **Captive Portal** > **Authenticated Clients** aus.

- **MAC Address**: Die MAC-Adresse des Clients
- **IP Address**: Die IP-Adresse des Clients
- **User Name**: Der Captive Portal-Benutzername des Clients
- **Protocol**: Das Protokoll, das der Benutzer zum Herstellen der Verbindung verwendet hat (HTTP oder HTTPS)
- **Verification**: Die Methode, die für die Authentifizierung des Benutzers in Captive Portal verwendet wurde. Einer der folgenden Werte ist möglich:
  - **Guest**: Der Benutzer muss nicht anhand einer Datenbank authentifiziert werden.
  - **Local**: 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
- **Radio ID**: Die ID des Funkmoduls. Beim WAP551-Gerät mit einem einzigen Funkmodul wird in diesem Feld **Radio 1** angezeigt. Beim WAP561-Gerät mit zwei Funkmodulen wird in diesem Feld **Radio 1** oder **Radio 2** angezeigt.
- **Captive Portal ID**: Die ID der Captive Portal-Instanz, der der Benutzer zugeordnet ist
- **Session Timeout**: Die in Sekunden verbleibende Zeit, während der die CP-Sitzung gültig ist. Wenn Null erreicht ist, wird der Client deauthentifiziert.
- **Away Timeout**: 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.

- **Received Packets**: Die Anzahl der IP-Pakete, die das WAP-Gerät von der Benutzerstation empfangen hat
- **Transmitted Packets**: Die Anzahl der IP-Pakete, die vom WAP-Gerät an die Benutzerstation gesendet wurden
- **Received Bytes**: Die Anzahl der Bytes, die das WAP-Gerät von der Benutzerstation empfangen hat
- **Transmitted Bytes**: Die Anzahl der Bytes, die vom WAP-Gerät an die Benutzerstation gesendet wurden

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

Failed Authentication Clients

Auf der Seite **Failed Authenticated Clients** werden Informationen zu Clients angezeigt, die erfolglos versucht haben, sich im Captive Portal zu authentifizieren.

Zum Anzeigen einer Liste der Clients, bei denen die Authentifizierung fehlgeschlagen ist, wählen Sie im Navigationsbereich die Option **Captive Portal** > **Failed Authentication Clients** aus.

- **MAC Address**: Die MAC-Adresse des Clients
- **IP Address**: Die IP-Adresse des Clients
- **User Name**: Der Captive Portal-Benutzername des Clients
- **Verification**: Die Methode, die für die Authentifizierung des Benutzers im Captive Portal verwendet wurde. Einer der folgenden Werte ist möglich:
  - **Guest**: Der Benutzer muss nicht anhand einer Datenbank authentifiziert werden.
  - **Local**: 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

- **Radio ID**: Die ID des Funkmoduls. Beim WAP551-Gerät mit einem einzigen Funkmodul wird in diesem Feld **Radio 1** angezeigt. Beim WAP561-Gerät mit zwei Funkmodulen wird in diesem Feld **Radio 1** oder **Radio 2** angezeigt.
- **Captive Portal ID**: Die ID der Captive Portal-Instanz, der der Benutzer zugeordnet ist
- **Failure Time**: 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.

10

Single Point Setup

In diesem Kapitel wird beschrieben, wie Sie Single Point Setup für mehrere WAP-Geräte konfigurieren.

Das Kapitel enthält die folgenden Themen:

Übersicht über Single Point Setup

Die WAP551- und WAP561-Geräte unterstützen Single Point Setup. Mit Single Point Setup können Sie WLAN-Services 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.

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 WAP551- und WAP561-Geräten, jedoch keine anderen Modelle im gleichen 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-Begrenzungen 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)
WAP5xx	16	480 960 für das WAP561 mit Doppelfunkfeld	1024 2048 für das WAP561 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. 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 WAP551-Geräte nur mit anderen Cisco WAP551- oder WAP561-Geräten in einem Cluster angeordnet werden.

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

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

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

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

HINWEIS Zwei Geräte, die sich im gleichen Single Point Setup befinden sollen, müssen nicht über gleich viele Funkmodule verfügen, jedoch sollten die Funkmodule die gleichen Funktionen unterstützen.

Single Point Setup für APs mit einem oder zwei Funkmodulen

Ein Single Point Setup kann eine Mischung aus APs mit einem und mit zwei Funkmodulen enthalten. Wenn die Konfiguration eines Geräts mit einem einzigen Funkmodul im Cluster geändert wird, verbreitet das Gerät die Änderung an das erste Funkmodul aller Mitglieder. Die Konfiguration des zweiten Funkmoduls eines APs mit zwei Funkmodulen ist nicht betroffen.

Wenn ein Single Point Setup nur APs mit einem einzigen Funkmodul enthält und ein Gerät mit zwei Funkmodulen dem Cluster beitritt, wird bei Geräten nur **Radio 1** des Geräts mit zwei Funkmodulen mit der Single Point Setup-Konfiguration konfiguriert. **Radio 2** des Geräts bleibt so wie vor dem Beitritt zum Cluster. Wenn das Single Point Setup jedoch bereits mindestens ein Gerät mit zwei Funkmodulen enthält, wird das zweite Funkmodul des dem Cluster beitretenden Geräts mit den Clustereinstellungen konfiguriert.

Wenn ein WAP-Gerät 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.)

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.

Allgemeine Konfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden	
Captive Portal	Password Complexity
Client QoS	User Accounts
Email Alert	QoS
HTTP/HTTP-Service (mit Ausnahme der Konfiguration von SSL-Zertifikaten)	**Radio Settings** einschließlich **TSpec Settings** (mit Ausnahmen)
Log Settings	Rogue AP Detection
MAC Filtering	Scheduler
Management Access Control	**SNMP General** und **SNMPv3**
Networks	WPA-PSK Complexity
Time Settings	

Funkkonfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden
Mode
Fragmentation Threshold
RTS Threshold
Rate Sets
Primary Channel
Protection

Funkkonfigurationseinstellungen und -parameter, die in Single Point Setup verbreitet werden
Fixed Multicast Rate
Broadcast or Multicast Rate Limiting
Channel Bandwidth
Short Guard Interval Supported

Funkkonfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden
Channel
Beacon Interval
DTIM Period
Maximum Stations
Transmit Power

Andere Konfigurationseinstellungen und -parameter, die nicht in Single Point Setup verbreitet werden	
Bandwidth Utilization	Port Settings
Bonjour	VLAN und IPv4
IPv6 Address	WDS Bridge
IPv6 Tunnel	WPS
Packet Capture	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.

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 das WAP-Gerät standardmäßig deaktiviert. Wenn die Option deaktiviert ist, wird die Schaltfläche **Enable Single Point Setup** angezeigt. Wenn Single Point Setup aktiviert ist, wird die Schaltfläche **Disable Single Point Setup** 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.

- **Location**: Geben Sie eine Beschreibung für den physischen Standort des Access Points ein, beispielsweise **Rezeption**. Das Feld für den Standort ist optional.
- **Cluster Name**: 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 **Enable Single Point Setup**.

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.

Wenn Single Point Setup aktiviert ist, bildet das WAP-Gerät 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:

- **Location**: Beschreibung des physischen Standorts des Access Points
- **MAC Address**: 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 Address**: 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.

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 **Cluster name** auf den gleichen Namen fest, der für die Cluster-Mitglieder konfiguriert ist.

SCHRITT 4 (Optional) Geben Sie in das Feld **Location** eine Beschreibung für den physischen Standort des Access Points ein, beispielsweise **Rezeption.**

SCHRITT 5 Klicken Sie auf **Enable Single Point Setup**.

Der Access Point tritt automatisch dem Single Point Setup bei.

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 **Disable Single Point Setup**.

Im Statusfeld **Single Point Setup** für den Access Point wird jetzt **Disabled** angezeigt.

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.

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)

Sessions

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 **Sessions** 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 **Display** ein Element aus, und klicken Sie auf **Go**. 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 im Navigationsbereich die Option **Single Point Setup > Sessions** aus.

Die folgenden Daten werden für jede WLAN-Clientsitzung mit Single Point Setup angezeigt.

- **AP Location**: Der Standort des Access Points.

  Der Standort wird von dem Standort abgeleitet, den Sie auf der Seite **Administration > System Settings** angegeben haben.

- **User MAC**: Die MAC-Adresse des WLAN-Clients.

  Eine MAC-Adresse ist eine Hardwareadresse, mit der jeder Knoten eines Netzwerks eindeutig identifiziert wird.

- **Idle**: 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.

- **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.

- **Receive Total**: Die Gesamtanzahl der Pakete, die der WLAN-Client während der aktuellen Sitzung empfangen hat

- **Transmit Total**: Die Gesamtanzahl der Pakete, die während dieser Sitzung an den WLAN-Client gesendet wurden

- **Error Rate**: 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**.

Channel Management

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 das WAP-Gerät 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.

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** > **Channel Management** aus.

Auf der Seite **Channel Management** 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 **Channel** auf der Seite **Wireless > Radio** 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 **Stop**.

Es werden keine Kanalverwendungszuordnungen oder Kanalneuzuweisungen vorgenommen. Nur manuelle Aktualisierungen wirken sich auf die Kanalzuweisung aus.

Wenn die Kanalverwaltung aktiviert ist, werden auf der Seite die Tabellen **Current Channel Assignations** und **Proposed Channel Assignments** angezeigt.

Die Tabelle **Current Channel Assignments** 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.

- **Location**: Der physische Standort des Geräts
- **IP Address**: Die IP-Adresse für den Access Point
- **Radio interface**: Gibt an, ob das Gerät über **Radio 1** (WLAN0) oder **Radio 2** (WLAN1) beigetreten ist. **Radio 2** ist nur für WAP561-Geräte relevant.
- **Wireless Radio**: Die MAC-Adresse des Funkmoduls
- **Band**: Das Band, über das der Access Point sendet
- **Channel**: Der Funkkanal, über den dieser Access Point zurzeit sendet
- **Locked**: 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 **Up** (funktionsfähig) oder **Down** (nicht funktionsfähig).

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 **Current Channel Assignments** und **Proposed Channel Assignments** der gleiche Kanal angezeigt. Gesperrte Geräte behalten die aktuellen Kanäle bei.

Die Tabelle **Proposed Channel Assignments** 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 **Proposed Channel Assignments** wie in der Tabelle **Current Channel Assignations** 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.

Im Bereich **Advanced settings** 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:

- **Change channels if interference is reduced by at least**: 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.

- **Determine if there is better set of channels every**: 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 **Wireless Neighborhood** 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 Sie nach Fehlern. Unerwartete Änderungen des Abdeckungsmusters sind in der farblich codierten Tabelle auf einen Blick erkennbar.

Zum Anzeigen von benachbarten Geräten wählen Sie im Navigationsbereich die Option **Single Point Setup** > **Wireless Neighborhood** aus. 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 Detection** aus.

Für jeden benachbarten Access Point werden die folgenden Informationen angezeigt:

- **Display Neighboring APs**: Wählen Sie eines der folgenden Optionsfelder aus, um die Ansicht zu ändern:
  - **In cluster**: Nur benachbarte WAP-Geräte, die Mitglieder des Clusters sind
  - **Not in cluster**: Nur benachbarte WAP-Geräte, die nicht Mitglieder des Clusters sind
  - **Both**: Zeigt alle benachbarten WAP-Geräte an (Cluster-Mitglieder und Nichtmitglieder).

  HINWEIS Bei einem erkannten AP, der auch Cluster-Mitglied ist, werden mit **In cluster** nur die SSIDs des Standard-VAPs (VAP0) angezeigt. Für Nichtstandard-VAPs im AP wird **Not in 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.
- **Neighbors**: 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.

Die Farbe des Balkens gibt die Signalstärke an:

- Dunkelblauer Balken: Ein dunkelblauer Balken und ein hoher Signalstärkewert (beispielsweise 50) weisen darauf hin, dass von dem benachbarten Gerät mit der über der jeweiligen Spalte genannten IP-Adresse eine gute Signalstärke erkannt wird.
- Hellblauer Balken: Ein hellblauer Balken und ein niedrigerer Signalstärkewert (beispielsweise 20 oder niedriger) weisen darauf hin, dass von dem benachbarten Gerät mit der über der jeweiligen Spalte genannten IP-Adresse eine mittlere oder niedrige Signalstärke erkannt wird.
- Weißer Balken: Ein weißer Balken und die Zahl 0 weisen darauf hin, dass ein benachbartes Gerät, das von einem der Cluster-Mitglieder erkannt wurde, von dem Gerät mit der über der jeweiligen Spalte genannten IP-Adresse nicht erkannt wird.
- Hellgrauer Balken: Ein hellgrauer Balken ohne Signalstärkewert weist darauf hin, dass kein Signal von dem Nachbarn erkannt wurde. Möglicherweise wurde der Nachbar jedoch von anderen Mitgliedern des Clusters erkannt.
- Dunkelgrauer Balken: Ein dunkelgrauer Balken ohne Signalstärkewert weist auf das WAP-Gerät selbst hin, das der oben angegebenen IP-Adresse entspricht. Die Signalstärke Null wird angezeigt, da die eigene Signalstärke des Geräts nicht gemessen wird.

Zum Anzeigen von Details zu einem Cluster-Mitglied klicken Sie oben auf der Seite auf die IP-Adresse eines Mitglieds.

Unter der Liste **Neighbors** werden die folgenden Details für das Gerät angezeigt.

- **SSID**: Die SSID (Netzwerkadresse) für den benachbarten Access Point
- **MAC Address**: Die MAC-Adresse des benachbarten Access Points
- **Channel**: 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 Interval**: Das vom Access Point verwendete Beacon-Intervall
- **Beacon Age**: Datum und Uhrzeit des letzten von diesem Access Point empfangenen Beacons

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 and Statistics > Log** klicken.

Weitere Informationen finden Sie unter:

- **Tabelle mit Ursachencodes für Deauthentifizierungen**

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.

Ursachencode	Bedeutung
6	Es wurde ein Klasse-2-Frame von einer nicht authentifizierten STA empfangen.
7	Es wurde ein Klasse-3-Frame von einer nicht zugeordneten STA empfangen.
8	Die Zuordnung wurde aufgehoben, da die sendende STA den BSS (Basic Service Set) verlassen hat oder verlässt.
9	Die STA, die die (erneute) Zuordnung anfordert, ist gegenüber der antwortenden STA nicht authentifiziert.
10	Die Zuordnung wurde aufgehoben, da die Informationen im Power Capability-Element nicht akzeptabel sind.
11	Die Zuordnung wurde aufgehoben, da die Informationen im Supported Channels-Element nicht akzeptabel sind.
12	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 sollen, den Cisco Access Point WAP551 und WAP561 optimal zu nutzen.

Support	
Cisco Small Business Support-Community	www.cisco.com/go/smallbizsupport
Cisco Small Business-Support und -Ressourcen	www.cisco.com/go/smallbizhelp
Telefonischer Kundensupport	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business-Firmwaredownloads	www.cisco.com/go/smallbizfirmware Klicken Sie auf einen der Links, um Firmware für Cisco Small Business-Produkte herunterzuladen. Eine Anmeldung ist nicht erforderlich. Downloads für alle anderen Cisco Small Business-Produkte, einschließlich Netzwerkspeichersystemen, stehen im Download-Bereich von Cisco.com unter www.cisco.com/go/software zur Verfügung (Registrierung/Anmeldung erforderlich).
Open Source-Anfragen zu Cisco Small Business	www.cisco.com/go/smallbiz_opensource_request
Produktdokumentation	
Cisco Small Business Wireless-N-Access Point WAP551 und WAP561 – Kurzanleitung und Administratorhandbuch	http://www.cisco.com/go/100_wap_resources oder http://www.cisco.com/go/300_wap_resources

Cisco Small Business	
Cisco Partner Central für Small Business (Partneranmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Cisco Small Business-Homepage	www.cisco.com/smb

78-20594-01