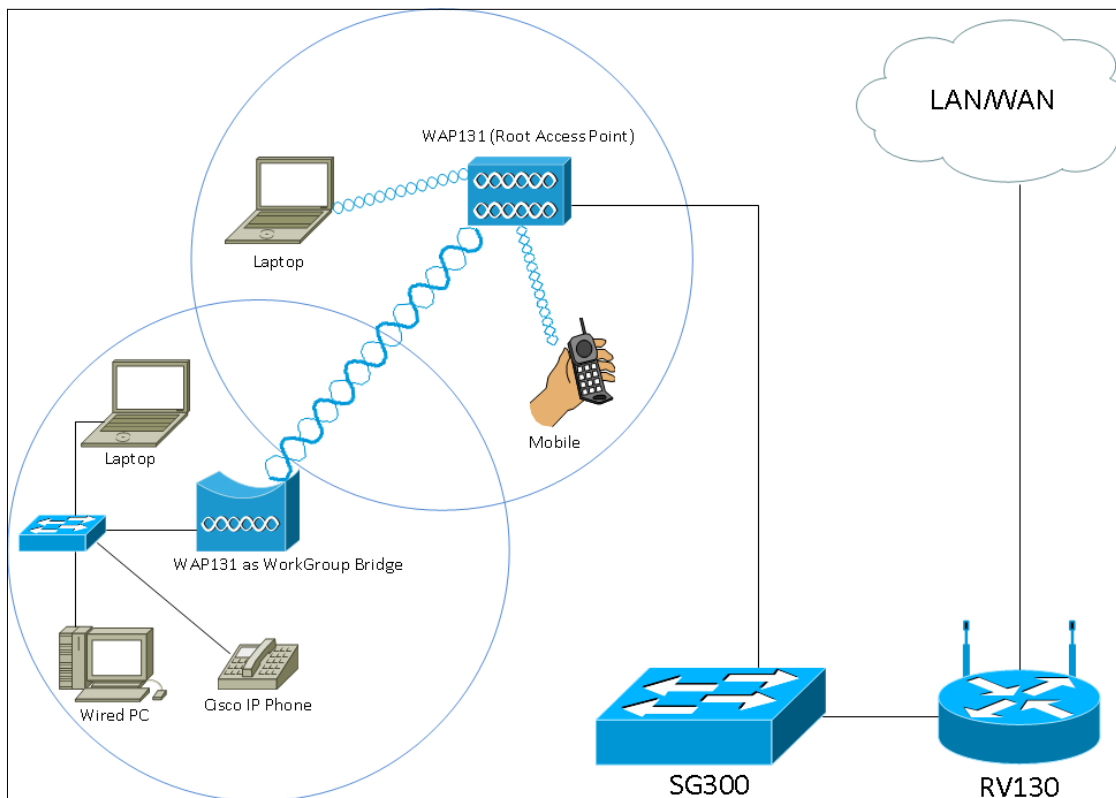


# Konfigurieren der WorkGroup Bridge am WAP131 Access Point

## Ziel

Die Workgroup Bridge-Funktion ermöglicht dem Wireless Access Point (WAP) die Überbrückung des Datenverkehrs zwischen einem Remote-Client und dem Wireless LAN, das mit dem Workgroup Bridge-Modus verbunden ist. Das der Remote-Schnittstelle zugeordnete WAP-Gerät wird als Access Point-Schnittstelle bezeichnet, und das dem WLAN zugeordnete Gerät wird als Infrastruktur-Schnittstelle bezeichnet. Obwohl das Wireless Distribution System (WDS) die bevorzugte Bridge-Lösung für den WAP131 ist, wird der Workgroup Bridge Mode empfohlen, wenn die WDS-Funktion nicht verfügbar ist.



**Hinweis:** Wenn die Workgroup Bridge-Funktion aktiviert ist, funktioniert die WDS Bridge-Funktion nicht. Weitere Informationen zur Konfiguration der WDS Bridge finden Sie im Artikel [Configuring Wireless Distribution System \(WDS\) Bridge on the WAP131 and WAP351](#).

In diesem Dokument wird erläutert, wie die Workgroup Bridge auf dem WAP131 Access Point konfiguriert wird.

## Anwendbare Geräte

WAP131

## Softwareversion

·1,0/3,4

# Arbeitsgruppen-Bridge konfigurieren

**Hinweis:** Um die Workgroup Bridge zu aktivieren, muss das Clustering im WAP aktiviert sein. Wenn das Clustering deaktiviert ist, müssen Sie die Single-Point-Einrichtung deaktivieren, um das Clustering zu aktivieren. Alle WAP-Geräte, die an der Workgroup Bridge teilnehmen, müssen die folgenden Einstellungen aufweisen:

- Radio
- IEEE 802.11-Modus
- Kanalbandbreite
- Kanal (Auto nicht empfohlen)

Um sicherzustellen, dass diese Einstellungen auf allen Geräten gleich sind, überprüfen Sie die Funkeinstellungen. Informationen zum Konfigurieren dieser Einstellungen finden Sie im Artikel [Konfigurieren der grundlegenden Wireless-Funkeinstellungen für die WAP131- und WAP351-Zugangspunkte](#).

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Wireless > WorkGroup Bridge** aus. Die Seite *WorkGroup Bridge* wird geöffnet:

WorkGroup Bridge Mode:  Enable

---

**Radio Setting Per Interface**

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

---

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

---

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 2: Aktivieren Sie das Kontrollkästchen **Enable (Aktivieren)** im Feld *WorkGroup Bridge Mode (Arbeitsgruppen-Bridge-Modus)*, um die Workgroup Bridge-Funktion zu aktivieren.

WorkGroup Bridge Mode:  Enable

---

**Radio Setting Per Interface**

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

## Funkeinstellungen

Schritt 1: Wählen Sie die Funkschnittstelle für die Arbeitsgruppenbrücke aus. Wenn Sie eine Funkeinheit als Arbeitsgruppen-Bridge konfigurieren, bleibt die andere Funkeinheit betriebsbereit. Die Funkschnittstellen entsprechen den Funkfrequenzbändern des WAP131. Der WAP131 ist für die Übertragung auf zwei verschiedenen Funkschnittstellen ausgestattet. Die Konfiguration der Einstellungen für eine Funkschnittstelle hat keine Auswirkungen auf

die andere.

WorkGroup Bridge Mode:  Enable

---

**Radio Setting Per Interface**

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  Radio 2 (5 GHz)

## Infrastruktur-Client-Schnittstelle

Schritt 1: Geben Sie den Namen Service Set Identifier (SSID) in das Feld *SSID ein*. Die SSID muss 2-32 Zeichen lang sein.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 2: Wählen Sie in der Dropdown-Liste *Security* (Sicherheit) den Sicherheitstyp aus, um eine Client-Station auf dem Upstream-WAP-Gerät zu authentifizieren.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:    
None  
WPA Personal  
WPA Enterprise

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Die verfügbaren Optionen sind wie folgt definiert:

- Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Wenn Sie diese Option wählen, fahren Sie mit [Schritt 14 fort](#).
- WPA Personal: WPA Personal unterstützt Schlüssel mit einer Länge von 8-63 Zeichen. Die Verschlüsselungsmethode ist RC4 für WPA und Advanced Encryption Standard (AES) für WPA2. WPA2 wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard verfügt. Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 3 fort](#).
- WPA Enterprise (WPA-Enterprise): WPA Enterprise ist fortschrittlicher als WPA Personal und stellt die empfohlene Sicherheit für die Authentifizierung dar. Es verwendet PEAP (Protected Extensible Authentication Protocol) und TLS (Transport Layer Security). Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 5 fort](#).

## WPA Personal

**Schritt 3:** Aktivieren Sie das Kontrollkästchen **WPA-TKIP** oder **WPA2-AES**, um zu bestimmen, welche Art von WPA-Verschlüsselung die Infrastruktur-Client-Schnittstelle verwendet. Wenn alle Wireless-Geräte WPA2 unterstützen, legen Sie die Sicherheit des Infrastruktur-Client für WPA2-AES fest. Wenn einige Ihrer Wireless-Geräte, wie PDAs und andere kleine Wireless-Netzwerkgeräte, nur eine Verbindung mit WPA-TKIP herstellen, wählen Sie WPA-TKIP aus.

The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is 'TestClient SSID'. The Security is set to 'WPA Personal'. Under 'WPA Versions', the 'WPA2-AES' checkbox is checked and highlighted with a red circle. The Key field is empty. The VLAN ID is '1'. The Connection Status is 'Disconnected'.

**Schritt 4:** Geben Sie den WPA-Verschlüsselungsschlüssel im Feld *Schlüssel ein*. Der Schlüssel muss 8 bis 63 Zeichen lang sein. Fahren Sie mit [Schritt 14 fort](#).

The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is 'TestClient SSID'. The Security is set to 'WPA Personal'. Under 'WPA Versions', the 'WPA2-AES' checkbox is checked. The Key field is filled with eight dots and highlighted with a red circle. The VLAN ID is '1'. The Connection Status is 'Disconnected'.

## WPA-Enterprise

**Schritt 5:** Aktivieren Sie das Kontrollkästchen **WPA-TKIP** oder **WPA2-AES**, um zu bestimmen, welche Art von WPA-Verschlüsselung die Infrastruktur-Client-Schnittstelle verwendet. Wenn alle Wireless-Geräte WPA2 unterstützen, legen Sie die Sicherheit des Infrastruktur-Client für WPA2-AES fest. Wenn einige Ihrer Wireless-Geräte nur eine Verbindung mit WPA-TKIP herstellen können, aktivieren Sie die Kontrollkästchen **WPA-TKIP** und **WPA2-AES**. In dieser Konfiguration werden die WPA2-Geräte mit WPA2 und die WPA-Geräte mit WPA verbunden.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Username:

Password:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 6: Wählen Sie im Feld *EAP-Methode* entweder das Optionsfeld **PEAP** oder **TLS**. Das Protected Extensible Authentication Protocol (PEAP) gibt jedem Wireless-Benutzer individuelle Benutzernamen und Kennwörter für den WAP an, die AES-Verschlüsselungsstandards unterstützen. Für Transport Layer Security (TLS) muss jedem Benutzer ein zusätzliches Zertifikat für den Zugriff zugewiesen werden. Wenn Sie PEAP auswählen, fahren Sie mit [Schritt 14 fort](#).

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Username:

Password:


VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 7: Geben Sie den Benutzernamen und das Kennwort in das Feld *Benutzername* und *Kennwort* ein.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:  

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Username:

Password:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 8: Wählen Sie im Feld *Übertragungsmethode* entweder die Optionsschaltflächen **HTTP** oder **TFTP** aus. Trivial File Transfer Protocol (TFTP) ist eine vereinfachte, unsichere Version von File Transfer Protocol (FTP). Er wird hauptsächlich zur Verteilung von Software oder zur Authentifizierung von Geräten zwischen Unternehmensnetzwerken verwendet. Hypertext Transfer Protocol (HTTP) bietet ein einfaches Challenge-Response-Authentifizierungs-Framework, das von einem Client zur Bereitstellung eines Authentifizierungs-Frameworks verwendet werden kann. Wenn Sie **TFTP** auswählen, fahren Sie mit [Schritt 11 fort](#).

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  
 TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Filename:  mini\_httpd.pem

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

**Hinweis:** Wenn auf dem WAP bereits eine Zertifikatsdatei vorhanden ist, werden das Feld *Zertifikatsdatei* vorhanden und das Feld *Zertifikatsablaufdatum* bereits mit den entsprechenden Informationen ausgefüllt. Andernfalls sind sie leer.

## HTTP

Schritt 9: Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Zertifikatsdatei zu suchen und auszuwählen. Die Datei muss über die entsprechende Zertifikatsdateierweiterung verfügen (z. B. .pem oder .pfx), ansonsten wird die Datei nicht akzeptiert.



### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:	<input checked="" type="checkbox"/> WPA-TKIP <input type="checkbox"/> WPA2-AES
EAP Method:	<input type="radio"/> PEAP <input checked="" type="radio"/> TLS
Identity	<input type="text" value="Admin_Sr"/>
Private Key	<input type="text" value="••••••••"/>
Certificate File Present:	<input type="text"/>
Certificate Expiration Date:	<input type="text"/>
Transfer Method:	<input checked="" type="radio"/> HTTP <input type="radio"/> TFTP
Filename	<input type="button" value="Browse..."/> mini_httpd.pem
<input type="button" value="Upload"/>	


VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 10: Klicken Sie auf **Hochladen**, um die ausgewählte Zertifikatsdatei hochzuladen.  
Fahren Sie mit [Schritt 14 fort](#).

### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:  

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP

TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP

TFTP

Filename  mini\_httpd.pem

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Das Feld *Zertifikatdatei* vorhanden und *Zertifikatsablaufdatum* wird automatisch aktualisiert.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Filename:  mini\_httpd.pem

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

## TFTP

[Schritt 11](#): Geben Sie den Dateinamen der Zertifikatsdatei im Feld *Dateiname ein*.

### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP

TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP

TFTP

Filename

TFTP Server IPv4 Address:


VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 12: Geben Sie die Adresse des TFTP-Servers in das Feld *IPv4-Adresse des TFTP-Servers* ein.

### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:  

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP

TLS

Identity

Private Key

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP

TFTP

Filename

TFTP Server IPv4 Address:


VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Schritt 13: Klicken Sie auf die Schaltfläche **Hochladen**, um die angegebene Zertifikatsdatei hochzuladen.

### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:  

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP

TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP

TFTP

Filename:

TFTP Server IPv4 Address:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

Das Feld "Zertifikatsdatei vorhanden" und das Feld "Zertifikatsablaufdatum" werden automatisch aktualisiert.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

Filename:

TFTP Server IPv4 Address:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

[Schritt 14](#): Geben Sie die VLAN-ID für die Infrastruktur-Client-Schnittstelle ein.

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

## Access Point-Schnittstelle

Schritt 1: Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Status*, um Bridging für die Access Point-Schnittstelle zu aktivieren.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 2: Geben Sie im Feld *SSID* den Service Set Identifier (SSID) für den Access Point ein. Die SSID-Länge muss zwischen 2 und 32 Zeichen betragen.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 3: (Optional) Wenn Sie die Downstream-SSID nicht übertragen möchten, deaktivieren Sie das Kontrollkästchen **Aktivieren** im Feld SSID-Broadcast. Es ist standardmäßig aktiviert.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 4: Wählen Sie aus der Dropdown-Liste *Security* (Sicherheit) den Sicherheitstyp aus, der Downstream-Client-Stationen für das WAP-Gerät authentifizieren soll.



**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Die verfügbaren Optionen sind wie folgt definiert:

·Keine - Offen oder keine Sicherheit. Dies ist der Standardwert. Fahren Sie mit [Schritt 10 fort](#), wenn Sie diese Option auswählen.

·WPA Personal: WPA Personal unterstützt Schlüssel mit einer Länge von 8 bis 63 Zeichen. Die Verschlüsselungsmethode ist entweder Temporal Key Integrity Protocol (TKIP) oder Counter Cipher Mode mit Block Chaining Message Authentication Code Protocol (CCMP). WPA2 mit CCMP wird empfohlen, da es über einen leistungsfähigeren Verschlüsselungsstandard, Advanced Encryption Standard (AES), verfügt, als das TKIP, das nur einen 64-Bit-RC4-Standard verwendet.

Schritt 5: Überprüfen Sie die gewünschten WPA-Versionen im Feld *WPA-Versionen*. In der Regel wird WPA nur dann ausgewählt, wenn einige der beteiligten WAPs WPA2 nicht unterstützen. Andernfalls wird WPA2 empfohlen. WPA2-AES ist immer aktiviert.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 6: Geben Sie den gemeinsamen WPA-Schlüssel in das Feld *Schlüssel ein*. Der Schlüssel muss 8 bis 63 Zeichen lang sein und kann alphanumerische Zeichen, Groß- und Kleinbuchstaben sowie Sonderzeichen enthalten.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  ⓘ

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)

MAC Filtering:  ▼

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 7: Geben Sie die Rate in der *Aktualisierungsrate für den Sendeschlüssel* ein. Die Rate muss zwischen 0 und 86400 liegen, wobei der Wert 0 die Funktion deaktiviert. Der Standardwert ist 300.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  ⓘ

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)

MAC Filtering:  ▼

VLAN ID:  (Range: 1 - 4094, Default: 1)

Schritt 8: Wählen Sie aus der Dropdown-Liste *MAC Filtering (MAC-Filterung)* den Typ aus, den Sie für die Access Point-Schnittstelle konfigurieren möchten. Wenn diese Funktion aktiviert ist, wird Benutzern basierend auf der MAC-Adresse des Clients, den sie verwenden, der Zugriff auf den WAP gewährt oder verweigert.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  ⓘ

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)

MAC Filtering:  ▼

VLAN ID:  (Range: 1 - 4094, Default: 1)

Die verfügbaren Optionen sind wie folgt definiert:

- Disabled (Deaktiviert): Alle Clients können auf das Upstream-Netzwerk zugreifen. Dies ist der Standardwert.
- Local (Lokal): Die Clients, die auf das Upstream-Netzwerk zugreifen können, sind auf die Clients beschränkt, die in einer lokal definierten MAC-Adressliste angegeben sind.
- RADIUS - Der Client-Satz, der auf das Upstream-Netzwerk zugreifen kann, ist auf die Clients beschränkt, die in einer MAC-Adressliste auf einem RADIUS-Server angegeben sind.

Schritt 9: Geben Sie die VLAN-ID im Feld *VLAN-ID* für die Client-Schnittstelle des Access Points ein.

The screenshot shows the configuration interface for an Access Point. The 'Access Point Interface' section is active. The 'Status' is set to 'Enable'. The 'SSID' is 'TestSSID'. 'SSID Broadcast' is 'Enable'. 'Security' is set to 'WPA Personal'. Under 'WPA Versions', both 'WPA-TKIP' and 'WPA2-AES' are checked. The 'Key' is masked with dots. 'Broadcast Key Refresh Rate' is set to '300' seconds. 'MAC Filtering' is set to 'Disabled'. The 'VLAN ID' field is highlighted with a red rectangle and contains the value '1'.

**Hinweis:** Um das Bridging von Paketen zu ermöglichen, sollte die VLAN-Konfiguration für die Access Point-Schnittstelle und die kabelgebundene Schnittstelle mit der der Infrastruktur-Client-Schnittstelle übereinstimmen.

**Schritt 10:** Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

WorkGroup Bridge Mode:  Enable

### Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

### Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:

VLAN ID:  (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

### Access Point Interface

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

VLAN ID:  (Range: 1 - 4094, Default: 1)