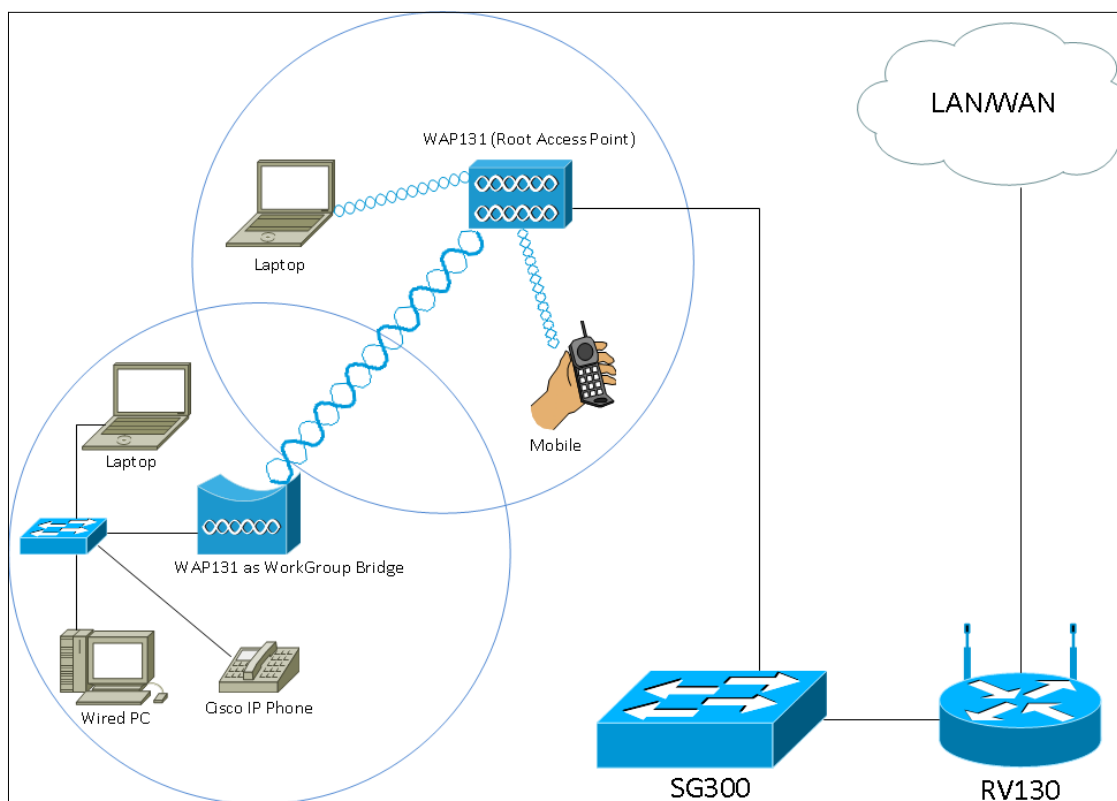


# Configurare WorkGroup Bridge sul punto di accesso WAP131

## Obiettivo

La funzionalità Bridge per gruppi di lavoro consente al punto di accesso wireless (WAP) di collegare il traffico tra un client remoto e la LAN wireless connessa alla modalità bridge per gruppi di lavoro. Il dispositivo WAP associato all'interfaccia remota è noto come interfaccia del punto di accesso, mentre quello associato alla LAN wireless è definito interfaccia di infrastruttura. Sebbene il sistema WDS (Wireless Distribution System) sia la soluzione bridge preferita per WAP131, la modalità Bridge per gruppi di lavoro è consigliata quando la funzionalità WDS non è disponibile.



**Nota:** Quando la funzionalità Bridge di gruppo di lavoro è attivata, la funzionalità Bridge di Servizi di distribuzione Windows non funziona. Per informazioni sulla configurazione di WDS Bridge, fare riferimento all'articolo [Configurazione di Wireless Distribution System \(WDS\) Bridge su WAP131 e WAP351](#).

L'obiettivo di questo documento è spiegare come configurare Workgroup Bridge sul punto di accesso WAP131.

## Dispositivi interessati

·WAP131

## Versione del software

·1.0.3.4

## Configura bridge per gruppi di lavoro

**Nota:** Per abilitare Workgroup Bridge, è necessario abilitare il clustering nel WAP. Se il clustering è disabilitato, è necessario disabilitare la configurazione del punto singolo per abilitarlo. Tutte le periferiche WAP che fanno parte di Workgroup Bridge devono avere le impostazioni seguenti identiche:

- Radio

Modalità IEEE 802.11

- Larghezza di banda del canale

Canale (impostazione automatica non consigliata)

Per verificare che queste impostazioni siano uguali in tutte le periferiche, cercare le impostazioni radio. Per configurare queste impostazioni, consultare l'articolo [Configurazione delle impostazioni base della radio wireless sui punti di accesso WAP131 e WAP351](#).

Passaggio 1. Accedere all'utilità Configurazione Web e scegliere **Wireless > WorkGroup Bridge**. Viene visualizzata la pagina *WorkGroup Bridge*:

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)

Passaggio 2. Selezionare la casella di controllo **Abilita** nel campo *Modalità bridge gruppo di lavoro* per abilitare la funzionalità bridge di gruppo di lavoro.

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)

## Impostazioni radio

Passaggio 1. Selezionare l'interfaccia radio per il bridge per gruppi di lavoro. Quando si configura una radio come bridge per gruppi di lavoro, l'altra radio rimane operativa. Le interfacce radio corrispondono alle bande di radiofrequenza del WAP131. Il WAP131 è predisposto per trasmettere su due diverse interfacce radio. La configurazione delle impostazioni per un'interfaccia radio non influirà sull'altra.

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)

## Interfaccia client infrastruttura

Passaggio 1. Immettere il nome SSID (Service Set Identifier) nel campo *SSID*. L'SSID deve avere una lunghezza compresa tra 2 e 32 caratteri.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:   ▼

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

Connection Status: Disconnected

Passaggio 2. Scegliere il tipo di protezione per autenticare una stazione client sul dispositivo WAP upstream dall'elenco a discesa *Protezione*.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:   ▼

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

Connection Status: Disconnected

Le opzioni disponibili sono definite come segue:

- Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questa opzione, andare al [passaggio 14](#).

- WPA Personal: WPA Personal supporta chiavi di lunghezza compresa tra 8 e 63 caratteri. Il metodo di crittografia è RC4 per WPA e AES (Advanced Encryption Standard) per WPA2. WPA2 è consigliato perché ha uno standard di crittografia più potente. Se si sceglie questa opzione, andare al [Passaggio 3](#).

- WPA Enterprise: WPA Enterprise è più avanzato di WPA Personal e rappresenta la protezione consigliata per l'autenticazione. Utilizza PEAP (Protected Extensible Authentication Protocol) e TLS (Transport Layer Security). Se si sceglie questa opzione, andare al [Passaggio 5](#).

## Personale WPA

[Passaggio 3](#). Selezionare la casella di controllo **WPA-TKIP** o **WPA2-AES** per determinare il tipo di crittografia WPA che verrà utilizzato dall'interfaccia client dell'infrastruttura. Se tutte le apparecchiature wireless supportano WPA2, impostare la sicurezza del client dell'infrastruttura per WPA2-AES. Se alcuni dispositivi wireless, ad esempio PDA e altri dispositivi di rete wireless di piccole dimensioni, si connettono solo con WPA-TKIP, selezionare WPA-TKIP.

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

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

Connection Status: Disconnected

Passaggio 4. Inserire la chiave di cifratura WPA nel campo *Chiave*. La chiave deve avere una lunghezza compresa tra 8 e 63 caratteri. Andare al [passo 14](#).

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

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

Connection Status: Disconnected

## WPA - Enterprise

[Passaggio 5](#). Selezionare la casella di controllo **WPA-TKIP** o **WPA2-AES** per determinare il tipo di crittografia WPA che verrà utilizzato dall'interfaccia client dell'infrastruttura. Se tutte le apparecchiature wireless supportano WPA2, impostare la protezione client dell'infrastruttura per WPA2-AES. Se alcune periferiche wireless possono connettersi solo con WPA-TKIP, selezionare entrambe le caselle di controllo **WPA-TKIP** e **WPA2-AES**. In questa configurazione, le periferiche WPA2 si connetteranno a WPA2 e le periferiche WPA si connetteranno a WPA.

**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

Passaggio 6. Nel campo *Metodo EAP*, selezionare il pulsante di opzione **PEAP** o **TLS**. Il protocollo PEAP (Protected Extensible Authentication Protocol) fornisce a ciascun utente wireless in base al protocollo WAP nomi utente e password individuali che supportano gli standard di crittografia AES. TLS (Transport Layer Security) richiede che ogni utente disponga di un certificato aggiuntivo per poter accedere. Se si seleziona PEAP, andare al [passo 14](#).

**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

Passaggio 7. Immettere il nome utente e la password nei campi *Nome utente* e *Password*.

**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

Passaggio 8. Selezionare i pulsanti di opzione **HTTP** o **TFTP** nel campo *Metodo di trasferimento*. Il protocollo TFTP (Trivial File Transfer Protocol) è una versione semplificata e non protetta del protocollo FTP (File Transfer Protocol). Viene utilizzato principalmente per distribuire software o autenticare dispositivi tra le reti aziendali. Il protocollo HTTP (Hypertext Transfer Protocol) fornisce un semplice framework di autenticazione in attesa/risposta che può essere utilizzato da un client per fornire il framework di autenticazione. Se si seleziona **TFTP**, andare al [punto 11](#).

**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

**Nota:** Se un file di certificato è già presente nel WAP, i campi *File di certificato presente* e *Data scadenza certificato* saranno già compilati con le informazioni pertinenti. In caso contrario, saranno vuote.


## HTTP

Passaggio 9. Fare clic sul pulsante **Sfogli**a per individuare e selezionare un file di certificato. Il file deve avere l'estensione corretta (ad esempio .pem o .pfx), altrimenti non verrà accettato.



### 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="text" value="mini_httpd.pem"/> <input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	


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

Connection Status: Disconnected

Passaggio 10. Fare clic su **Upload** per caricare il file di certificato selezionato. Andare al [passo 14](#).

### 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

I campi *File certificato presente* e *Data scadenza certificato* verranno aggiornati automaticamente.

**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

[Passaggio 11](#). Immettere il nome del file del certificato nel campo *Nome file*.

### 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

Passaggio 12. Immettere l'indirizzo del server TFTP nel campo *Indirizzo IPv4 server TFTP*.

### 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 type="radio"/> HTTP <input checked="" type="radio"/> TFTP
Filename	<input type="text" value="mini_httpd.pem"/>
TFTP Server IPv4 Address:	<input type="text" value="192.168.1.20"/>
<input type="button" value="Upload"/>	


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

Connection Status: Disconnected

Passaggio 13. Fare clic sul pulsante **Upload** per caricare il file di certificato specificato.

### 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

I campi *File certificato presente* e *Data scadenza certificato* verranno aggiornati automaticamente.

**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

[Passaggio 14](#). Immettere l'ID VLAN per l'interfaccia client dell'infrastruttura.

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

Connection Status: Disconnected

## Access Point Interface

Passaggio 1. Selezionare la casella di controllo **Abilita** nel campo *Stato* per abilitare il bridging nell'interfaccia del punto di accesso.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

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

Passaggio 2. Inserire l'SSID (Service Set Identifier) del punto di accesso nel campo *SSID*. La lunghezza SSID deve essere compresa tra 2 e 32 caratteri.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

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

Passaggio 3. (Facoltativo) Se non si desidera trasmettere l'SSID downstream, deselegnare la casella di controllo **Abilita** nel campo Trasmissione SSID. È attivata per impostazione predefinita.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:

MAC Filtering:

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

Passaggio 4. Scegliere il tipo di protezione per autenticare le stazioni client downstream sul dispositivo WAP dall'elenco a discesa *Protezione*.



**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security: None ▼ (+)

MAC Filtering: None  
WPA Personal

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

Le opzioni disponibili sono definite come segue:

- Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questa opzione, andare al [passaggio 10](#).

- WPA Personal: WPA Personal e supporta chiavi di lunghezza compresa tra 8 e 63 caratteri. Il metodo di crittografia è TKIP (Temporal Key Integrity Protocol) o CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). Si consiglia WPA2 con CCMP in quanto offre uno standard di crittografia più potente, AES (Advanced Encryption Standard) rispetto al TKIP che utilizza solo uno standard RC4 a 64 bit.

Passaggio 5. Controllare le versioni WPA desiderate dal campo *Versioni WPA*. In genere, WPA viene scelto solo se alcuni dei WAP interessati non supportano WPA2; in caso contrario, si consiglia WPA2. WPA2-AES è sempre abilitato.

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security: WPA Personal ▼ (-)

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: Disabled ▼

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

Passaggio 6. Immettere la chiave WPA condivisa nel campo *Chiave*. La chiave deve contenere da 8 a 63 caratteri e può includere caratteri alfanumerici, maiuscoli e minuscoli e caratteri speciali.

**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)

Passaggio 7. Inserire il tasso nel campo *Frequenza di aggiornamento chiave trasmissione*. La velocità deve essere compresa tra 0 e 86400, con un valore pari a 0 per disattivare la funzionalità. Il valore predefinito è 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)

Passaggio 8. Selezionare il tipo di filtro MAC che si desidera configurare per l'interfaccia del punto di accesso dall'elenco a discesa *Filtro MAC*. Quando questa opzione è abilitata, agli utenti viene concesso o negato l'accesso al WAP in base all'indirizzo MAC del client utilizzato.

**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)

Le opzioni disponibili sono definite come segue:

·Disattivato: tutti i client possono accedere alla rete upstream. Questo è il valore predefinito.

·Locale: l'insieme di client che possono accedere alla rete upstream è limitato ai client specificati in un elenco di indirizzi MAC definito localmente.

·RADIUS: l'insieme di client che possono accedere alla rete upstream è limitato ai client specificati in un elenco indirizzi MAC su un server RADIUS.

Passaggio 9. Immettere l'ID VLAN nel campo *VLAN ID* per l'interfaccia client del punto di accesso.

The screenshot shows the configuration interface for an Access Point Interface. The 'Status' is set to 'Enable'. The 'SSID' is 'TestSSID'. 'SSID Broadcast' is 'Enable'. 'Security' is 'WPA Personal'. Under 'WPA Versions', '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 'Disabled'. The 'VLAN ID' field is highlighted with a red box and contains the value '1'.

**Nota:** Per consentire il bridging dei pacchetti, la configurazione VLAN dell'interfaccia del punto di accesso e dell'interfaccia cablata deve corrispondere a quella dell'interfaccia del client dell'infrastruttura.

[Passaggio 10](#). Fare clic su **Salva** per salvare le modifiche.

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)