

# 在WAP121和WAP321接入點上配置工作組網橋

## 目標

工作組橋接功能使無線接入點(WAP)能夠橋接遠端客戶端與連線到工作組橋接模式的無線LAN之間的流量。與遠端介面關聯的WAP裝置稱為接入點介面，與無線LAN關聯的裝置稱為基礎設施介面。當WDS功能無法使用時，建議使用此功能，因為WDS功能是WAP121和WAP321的首選網橋解決方案。啟用工作組網橋功能時，WDS網橋功能不工作。要瞭解WDS網橋的配置方式，請參閱 *WAP121和WAP321接入點上的無線分佈系統(WDS)網橋配置* 一文。

本文說明如何在WAP121和WAP321接入點上配置工作組網橋。

## 適用裝置

- WAP121
- WAP321

## 軟體版本

- 1.0.3.4

## 配置工作組網橋

**附註：**要啟用工作組網橋，必須在WAP中啟用集群。如果禁用該設定，則需要禁用單點設定，這又會啟用集群。參與工作組網橋的所有WAP裝置必須具有無線電、IEEE 802.11模式、通道頻寬和通道（不建議使用音訊）的通用設定。要確保所有裝置中的這些設定相同，請查詢無線電設定。要配置這些設定，請參閱 *在WAP121和WAP321接入點上配置基本無線無線電設定* 一文。

步驟1.登入到Access Point Configuration Utility，然後選擇**Wireless > Work Group Bridge**。將開啟 *WorkGroup Bridge* 頁面：

## WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

### 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)

步驟2.在 *WorkGroup Bridge Mode* 欄位中選中 **Enable**，以啟用工作組網橋功能。

## WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

### 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)

步驟3. 在基礎設施客戶端介面的SSID欄位中輸入服務集識別符號(SSID)名稱。

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode:  Enable

---

**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)

Save

MAC Address	SSID
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	(Non Broadcasting)
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	(Non Broadcasting)
00:0C:29:00:00:00	WPSU-Guest
00:0C:29:00:00:00	(Non Broadcasting)
00:0C:29:00:00:00	WPSU-Guest

**提示：**您還可以按一下SSID欄位旁邊的箭頭圖示來掃描類似的鄰居SSID。僅當在預設情況下禁用的欺詐AP檢測中啟用了AP檢測時，才會啟用此選項。請參閱在WAP121和WAP321接入點上檢測無管理AP文章，以啟用無管理AP檢測。

步驟4.從Security下拉選單選擇對上游WAP裝置（基礎設施客戶端介面）上的客戶端工作站進行身份驗證的安全型別。可能的值為：

**WorkGroup Bridge**

Refresh

WorkGroup Bridge Mode:  Enable

---

**Infrastructure Client Interface**

SSID: test (Range: 2-32 Characters)

Security: None (+)  
None  
Static WEP  
WPA Personal  
WPA Enterprise

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

Connection Status:

---

**Access Point Interface**

Status:  Enable

SSID: Access Point SSID (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security: None (+)

MAC Filtering: Disabled

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

Save

·無 — 開啟或無安全保護。這是預設值。如果選擇此選項，請跳至步驟5。

·靜態WEP — 靜態WEP是最小的安全性，最多可以支援4個長度為64到128位的金鑰。必須在所有節點中使用相同的金鑰。有關靜態WEP的配置，請轉至[靜態WEP](#)。

·WPA個人 — WPA個人比WEP更先進，可以支援長度為8-63個字元的金鑰。WPA的加密方法是RC4,WPA2的加密方法是「高級加密標準」(AES)。建議使用WPA2，因為它的加密標準更強大。要配置WPA個人，請轉至[WPA個人客戶端介面](#)。

·WPA企業版 — WPA企業版是最高級且推薦的安全產品。它使用受保護的可擴展身份驗證協定(PEAP)，其中WAP下的每個無線使用者都使用單個使用者名稱和密碼進行授權，這些使用者名稱和密碼甚至可以支援AES加密標準。除了PEAP以外，它還使用傳輸層安全(TLS)，其中每位使用者都需要提供額外的證書才能獲得訪問許可權。WPA的加密方法是RC4,WPA2的高級加密標準(AES)。要配置WPA企業，請轉至[WPA企業](#)。

**附註：**根據所選擇的IEEE 802.11模式，上述選項的可用性可能會有所不同。

步驟5.在VLAN ID欄位中輸入基礎設施客戶端介面的VLAN ID。

## WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

### 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)

步驟6.在 *Status* 欄位中選中 **Enable**，以在接入點介面上啟用橋接。

### WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

#### 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)

步驟7.在接入點介面的SSID欄位名稱中輸入服務集識別符號(SSID)。

步驟8. ( 可選 ) 如果要廣播下游SSID，請選中要廣播的SSID Broadcast欄位中的Enable。預設情況下啟用。

步驟9.從Security下拉選單中選擇安全型別，以向WAP裝置 ( 接入點介面 ) 驗證下游客戶端站點的身份。可能的值為：

### WorkGroup Bridge

Refresh

WorkGroup Bridge Mode:  Enable

---

#### 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)

Save

·無 — 開啟或無安全保護。這是預設值。如果選擇此項，請跳過步驟10。

·靜態WEP — 靜態WEP是最小的安全性，最多可以支援4個長度為64到128位的金鑰。有關靜態WEP的配置，請轉至[靜態WEP](#)

·WPA個人 — WPA個人比WEP更先進，可以支援長度為8到63個字元的金鑰。加密方法是臨時金鑰完整性協定(TKIP)或具有塊鏈消息驗證代碼協定(CCMP)的計數器密碼模式。建議使用具有CCMP的WPA2，因為它具有比僅使用64位RC4標準的TKIP更強大的加密標準「高級加密標準(AES)」。要配置WPA個人，請轉至[WPA個人用於接入點介面](#)。

步驟10.從MAC Filtering下拉選單中選擇要為接入點介面配置的MAC過濾型別。啟用時，系統會根據使用者使用的客戶端的MAC地址授予或拒絕使用者訪問WAP。可能的值為：



### WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

#### 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:  (Dropdown menu showing Disabled, Local, RADIUS)

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

- 已禁用 — 所有客戶端都可以訪問上游網路。這是預設值。
- 本地 — 可以訪問上游網路的客戶端集僅限於本地定義的MAC地址清單中指定的客戶端。
- Radius — 可存取上游網路的使用者端組限制在RADIUS伺服器的MAC位址清單中指定的使用者端。

步驟11.在VLAN ID欄位中輸入接入點客戶端介面的VLAN ID。

### WorkGroup Bridge

WorkGroup Bridge Mode:  Enable

---

#### 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)

**附註：**為了允許橋接資料包，接入點介面和有線介面的VLAN配置應與基礎設施客戶端介面的VLAN配置相匹配。

步驟12.按一下**Save**以儲存設定。

## [靜態WEP](#)

The screenshot shows the 'Infrastructure Client Interface' with the following configuration details:

- SSID:** test (Range: 2-32 Characters)
- Security:** Static WEP
- Transfer Key Index:** 1
- Key Length:** 128 bits (selected)
- Key Type:** Hex (selected)
- WEP Keys:** (Required: 26)
- WEP Key 1:** [Redacted]
- WEP Key 2:** [Redacted]
- WEP Key 3:** [Redacted]
- WEP Key 4:** [Redacted]
- VLAN ID:** 1 (Range: 1 - 4094, Default: 1)
- Connection Status:** Disconnected

步驟1.選擇靜態WEP時，會顯示一些附加欄位。從 *Transfer Key Index* 欄位的下拉清單中，選擇鍵索引。可用值為1、2、3和4。預設值為1。不同WLAN的金鑰索引不同。連線到特定WLAN的裝置必須具有相同的金鑰索引。此金鑰用於加密資料以進行通訊。

步驟2.在 *Key Length* 字段中，選擇64位單選按鈕或128位單選按鈕。這指定使用的金鑰長度。

步驟3.在 *Key Type* 欄位中點選所需的單選按鈕。WEP金鑰通常為十六進位制。

- ASCII - ASCII (美國資訊交換標準碼) 是一種基於英文字母編碼為128個指定字元的字元編碼方案。

- 十六進位制 — 十六進位制 (十六進位制) 是一個以16為基數的位置數字系統。它使用16個不同的符號0-9表示0到9的數字，使用A、B、C、D、E、F表示10到15之間的值。每個十六進位制表示四個二進位制數字。

步驟4.在 *WEP Key* (WEP金鑰) 欄位下接下來的四個欄位中最多輸入四個WEP金鑰，分別標籤為1、2、3和4。這是一個輸入為金鑰的字串。金鑰的長度因金鑰的長度及型別而異。所需的長度在WEP金鑰欄位旁邊指示。所有WAP節點 (AP和客戶端) 中的WEP金鑰字串必須匹配，並且必須位於同一欄位中。這意味著如果字串1在一個裝置中是金鑰1，則字串1還必須是工作組網橋中其他裝置中的金鑰1。

## [WPA個人客戶端介面](#)

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA  WPA2

Key:  (Range: 8-63 Characters)

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

Connection Status: Disconnected

步驟1.從WPA Versions欄位檢查所需的WPA版本。通常，只有在網橋系統中的某些WAP不支援WPA2時，才會選擇WPA。WPA2是更高級且建議使用的協定。

- WPA — 如果網路具有支援原始版本WPA的客戶端工作站。
- WPA2 — 如果網路上的所有客戶端站都支援WPA2。此協定版本根據IEEE 802.11i標準提供最佳安全性。

步驟2.在金鑰欄位中輸入共用WPA金鑰。金鑰可以包括字母數字字元、大小寫字元和特殊字元。

### 適用於存取點介面的WPA個人版

Security:

WPA Versions:  WPA  WPA2

Cipher Suites:  TKIP  CCMP (AES)

Key:  (Range: 8-63 Characters)

Broadcast Key Refresh Rate:  (Range: 0-86400)

步驟1.從「WPA版本」欄位檢查所需的WPA版本。通常，只有當所涉及的某些WAP不支援WPA2時，才會選擇WPA;否則，建議使用WPA2。

- WPA — 如果網路具有支援原始版本WPA的客戶端工作站。
- WPA2 — 如果網路上的所有客戶端站都支援WPA2。此協定版本根據IEEE 802.11i標準提供最佳安全性。

**附註：**如果網路是WPA和WPA2客戶端的組合，請選中兩個覈取方塊。這允許WPA和WPA2客戶端工作站進行關聯和身份驗證，但是對於支援它的客戶端使用更強大的WPA2。

步驟2.從密碼套件(Cipher Suites)欄位中選擇所需的密碼套件。

- TKIP — 臨時金鑰完整性協定(TKIP)僅使用64位RC4標準。
- CCMP(AES) — 使用區塊鏈訊息驗證碼通訊協定(CCMP)的計數器密碼模式是AES (進階加

密標準) 使用的安全通訊協定。建議使用帶有CCMP的WPA2，因為它具有更強大的加密標準。

**附註：**可以選擇其中之一，也可以選擇兩者。TKIP和AES客戶端都可以與WAP裝置關聯。

步驟3.在**金鑰欄位**中輸入**共用WPA金鑰**。金鑰可以包括字母數字字元、大小寫字元和特殊字元。

步驟4.在**Broadcast Key Refresh Rate欄位**中輸入**速率**。

## WPA企業版

Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA  WPA2

EAP Method:  PEAP  TLS

Username:

Password:

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

Connection Status: Disconnected

步驟1.在**WPA Versions欄位**中檢查所需的**WPA版本**。通常只有在網橋系統中的某些WAP不支援WPA2時，才會選擇WPA。WPA2更先進，建議使用。

·WPA — 如果網路具有支援原始版本WPA的客戶端工作站。

·WPA2 — 如果網路上的所有客戶端站都支援WPA2。此協定版本根據IEEE 802.11i標準提供最佳安全性。

**附註：**如果網路是WPA和WPA2客戶端的組合，則選中兩個覈取方塊。這允許WPA和WPA2客戶端工作站進行關聯和身份驗證，但是對於支援它的客戶端使用更強大的WPA2。

步驟2.按一下相應的單選按鈕選擇兩個EAP方法。

·PEAP — 受保護的EAP。它依賴TLS，但避免在每個客戶端上安裝數位證書。相反，它通過使用者名稱和密碼提供身份驗證。如果選擇此選項，請轉到[PEAP \(受保護的可擴展身份驗證協定\)](#)。

·TLS — 通過交換數位證書進行身份驗證。如果選擇此選項，請轉至[TLS \(傳輸層安全\)](#)。

## PEAP (受保護的可擴展身份驗證協定)

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA  WPA2

EAP Method:  PEAP  TLS

Username:

Password:

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

步驟1. 在 *Username* 欄位中輸入使用者名稱。

步驟2. 在 *Password* 欄位中輸入密碼。

### [TLS \(傳輸層安全\)](#)

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

WPA Versions:  WPA  WPA2

EAP Method:  PEAP  TLS

Identity:

Private Key:

Certificate File Present:

Certificate Expiration Date:

Transfer Method:  HTTP  TFTP

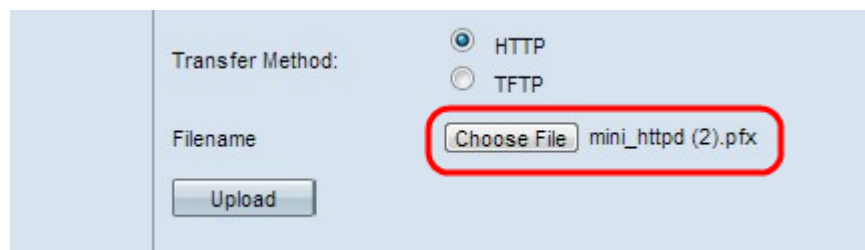
Certificate File:  No file chosen

步驟1. 選擇傳輸模式下載用於TLS驗證的證書檔案。

·HTTP — 如果要從PC的Web伺服器下載證書。如果選擇此選項，請轉到[HTTP](#)。

·TFTP — 如果您要從檔案伺服器下載證書。如果您選擇此項，請前往[TFTP](#)。

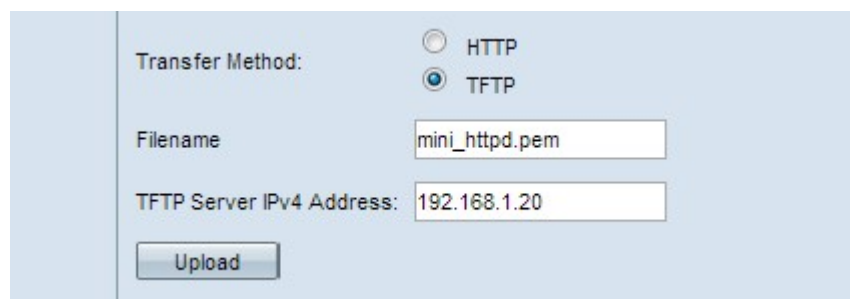
## [HTTP](#)



The screenshot shows a configuration window for the HTTP transfer method. Under the heading "Transfer Method:", the "HTTP" radio button is selected. Below this, the "Filename" field contains the text "mini\_httpd (2).pfx". A red rectangular box highlights the "Choose File" button and the filename text. At the bottom of the form is an "Upload" button.

步驟1。按一下**Choose file**以選擇憑證檔案。必須是副檔名為.pem、.pfx等的證書型別檔案。否則，檔案上傳將失敗。

## [TFTP](#)



The screenshot shows a configuration window for the TFTP transfer method. Under the heading "Transfer Method:", the "TFTP" radio button is selected. Below this, the "Filename" field contains the text "mini\_httpd.pem". The "TFTP Server IPv4 Address" field contains the text "192.168.1.20". At the bottom of the form is an "Upload" button.

步驟1.在*Filename*欄位中輸入證書檔案的名稱。

步驟2.輸入TFTP伺服器的IP地址。

**附註：** Certificate File Transfer欄位顯示WAP中是否存在憑證，Certificate Expiration Date欄位顯示現有憑證的到期日期。

步驟3.按一下**Upload**以上傳檔案至裝置。