

WAP551和WAP561接入點上的工作組網橋配置

目標

本文說明如何在WAP551和WAP561接入點上配置工作組網橋。

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WAP551和WAP561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。要檢視WDS網橋的配置方式，請查閱文章 *Wireless Distribution System(WDS)Bridge Configuration on WAP551 and WAP561 Access Points(WAP551和WAP561接入點上的無線分佈系統(WDS)網橋配置)*。

適用裝置

- WAP551
- WAP561

軟體版本

- v1.0.4.2

配置工作組網橋

附註：為了能夠啟用工作組網橋群集，必須在WAP中啟用。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 *WAP551/WAP561上的無線電設定*一文。

步驟1.登入到Web配置實用程式並選擇**Wireless > Work Group Bridge**。將開啟「工作組橋」頁：

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:

MAC Acl Mode:

步驟2.在「工作組橋接模式」欄位中，選中**Enable**以啟用工作組橋接功能。

WorkGroup Bridge

Refresh

WorkGroup Bridge Mode: Enable

Radio Setting Per Interface

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

Radio: Radio 1 Radio 2

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

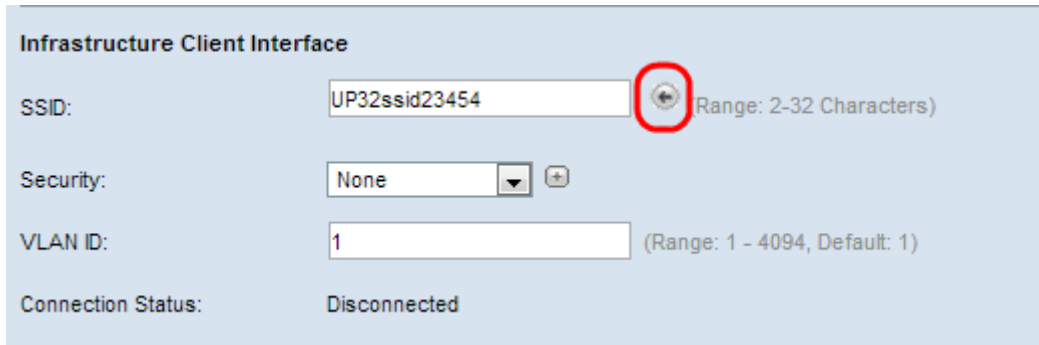
VLAN ID: (Range: 1 - 4094, Default: 1)

Connection Status: Disconnected

步驟3.僅對於WAP561需要此步驟。按一下**Radio1**或**Radio 2**單選按鈕選擇其中一個單選介面

。對於只有一個無線電介面的WAP551，忽略此步驟。要瞭解設定了哪個無線電並使用什麼引數查詢無線電設定。要配置這些設定，請參閱WAP551/WAP561上的無線電設定一文。

步驟4.在SSID欄位中，輸入基礎設施客戶端介面或上游接入點(AP)的服務集識別符號(SSID)名稱。



Infrastructure Client Interface

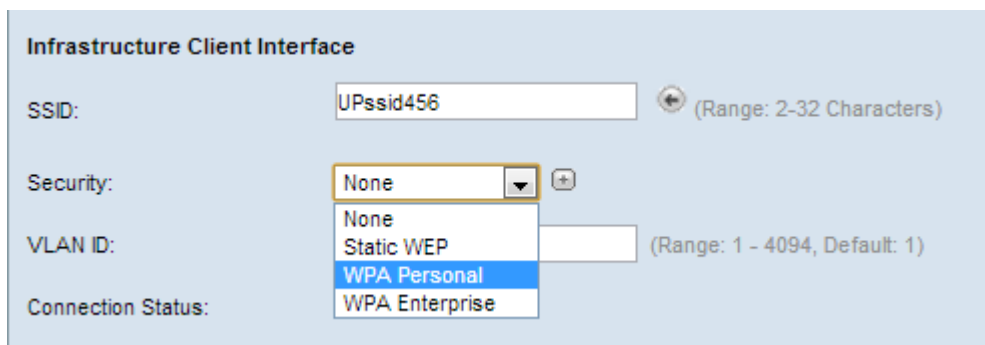
SSID: UP32ssid23454 (Range: 2-32 Characters)

Security: None

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

Connection Status: Disconnected

提示：您還可以點選SSID欄位旁邊的箭頭圖示掃描類似的鄰居SSID。僅當在欺詐AP檢測中啟用了AP檢測（預設情況下已禁用）時，才會啟用此選項。請參閱WAP561和WAP551上的欺詐接入點(AP)檢測文章，以啟用欺詐接入點檢測。



Infrastructure Client Interface

SSID: UPssid456 (Range: 2-32 Characters)

Security: None

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

Connection Status: Disconnected

步驟5.從Infrastructure Client Interface部分Security欄位的下拉選單中，選擇要作為上游WAP裝置（基礎架構客戶端介面）上的客戶端工作站進行身份驗證的安全型別。下面給出了可能的選擇。

·無 — 開啟或無安全保護。這是預設值。如果選擇此選項，請跳至配置VLAN ID和接入點介面部分。

·靜態WEP — 靜態WEP是最小的安全性，最多可支援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。

·WPA Personal — WPA Personal比WEP更先進，可以支援長度為8到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。

·WPA企業 - WPA企業是最高級和建議的安全產品。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的加密方法是AES。

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6.根據您在步驟5中選擇的選項，按一下其中一個選項鍊接並遵循相應的步驟。如果選擇「無」，則無需配置任何這些過程。

The screenshot shows a configuration page with two main sections: "Infrastructure Client Interface" and "Access Point Interface".

Infrastructure Client Interface:

- SSID: Infrastructure Client SSID (Range: 2-32 Characters)
- Security: None
- VLAN ID: 102 (Range: 1 - 4094, Default: 1)
- Connection Status: Disconnected

Access Point Interface:

- Status: Enable
- SSID: Access Point SSID (Range: 2-32 Characters)
- SSID Broadcast: Enable
- Security: None
- MAC Filtering: Local
- MAC Acl Mode: Accept
- VLAN ID: 1 (Range: 1 - 4094, Default: 1)

A "Save" button is located at the bottom left of the interface.

步驟7.在VLAN ID欄位中，輸入基礎設施客戶端介面的VLAN ID。

步驟8.在Status欄位中，選中**Enable**以在接入點介面上啟用橋接。

步驟9.在SSID欄位中，輸入接入點介面的服務集識別符號(SSID)名稱。

步驟10. (可選) 如果要廣播下游SSID (接入點介面SSID)，請選中SSID Broadcast欄位中的**Enable**。預設情況下啟用。

步驟11.從Security下拉選單中選擇安全型別，以便向WAP裝置 (接入點介面) 驗證下遊客戶端站點的身份。可能的值為：

- 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12到步驟15。跳到步驟16。

- 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。按照[配置靜態WEP](#)部分操作。跳至步驟16。

- 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)」。

Access Point Interface

Status: Enable

SSID: (Range: 2-32 Characters)

SSID Broadcast: Enable

Security:

WPA Versions: WPA WPA2

Cipher Suites: TKIP CCMP (AES)

Key: (Range: 8-63 Characters)

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

MAC Filtering:

MAC Acl Mode:

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

時間分配器：僅在步驟11中選擇了WPA個人後，才執行步驟12到步驟15。

步驟12.選中相應的框以選擇WPA版本。您可以在具有不同WPA版本的不同WAP客戶端中選擇WPA和WPA2。

步驟13.勾選適當的方塊以選擇密碼套件。您同時選擇TKIP和CCMP(AES)。

步驟14.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15.在Broadcast Key Refresh Rate欄位中輸入所需的金鑰刷新間隔。這是為所有WAP客戶端刷新組金鑰的間隔。

步驟16.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：

- 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17.在VLAN ID欄位中，輸入接入點客戶端介面的VLAN ID。

注意：要允許橋接資料包，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18.按一下**Save**以儲存設定。

[配置靜態WEP](#)

如果選擇將靜態WEP配置為您的身份驗證安全型別，請執行以下步驟。

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

- SSID: UPssid456 (Range: 2-32 Characters)
- Security: Static WEP
- Transfer Key Index: 1
- Key Length: 128 bits (selected)
- Key Type: Hex (selected)
- WEP Keys: (Required: 26)
- 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欄位的下拉選單中選擇一個鍵索引。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欄位中，選擇64位元單選或按鈕或128位元單選按鈕。這指定使用的金鑰長度。

步驟3.按一下ASCII單選按鈕或HEX單選按鈕，在「金鑰型別」欄位中選擇金鑰型別。WEP金鑰通常為十六進位制。

This is a close-up view of the WEP configuration section from the previous screenshot. The 'WEP Keys: (Required: 26)' text is circled in red. Below it are four input fields labeled 1, 2, 3, and 4, each containing a series of dots representing a key.

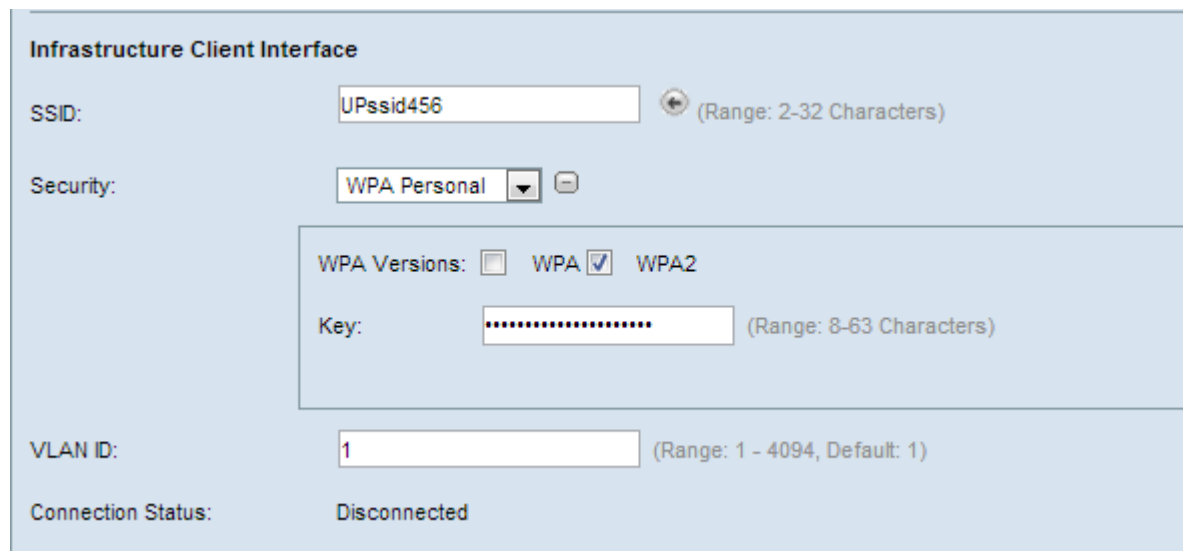
步驟4.在WEP Key欄位的下方四個欄位中最多輸入四個WEP金鑰，分別標籤為1、2、3和4。

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。

按一下[here](#)以繼續設定。

配置WPA個人

如果選擇將WPA個人配置為身份驗證安全型別，請執行以下步驟。



The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is 'UPssid456' with a range of 2-32 characters. The Security is set to 'WPA Personal'. Under 'WPA Versions', 'WPA' is selected with a checkmark, and 'WPA2' is unselected. The Key field is filled with dots, with a range of 8-63 characters. The VLAN ID is '1' with a range of 1-4094 and a default of 1. The Connection Status is 'Disconnected'.

步驟1.檢查WPA或WPA2以選擇WPA的版本。通常只有在所涉及的WAP都不支援WPA2時才選擇WPA。否則，建議使用WPA 2。

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。

按一下[here](#)以繼續設定。

配置WPA企業

如果選擇將WPA Enterprise配置為身份驗證安全型別，請執行以下步驟。

Infrastructure Client Interface

SSID: Infrastructure Client SSID (Range: 2-32 Characters)

Security: WPA Enterprise

WPA Versions: WPA WPA2

EAP Method: PEAP TLS

Username:

Password:

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

Connection Status: Disconnected

步驟1. 如果您選擇WPA企業，請選中WPA或WPA2以選擇WPA的版本。通常只有在網橋系統中的所有WPA都不支援WPA2時，才會選擇WPA。WPA 2更先進，建議使用。

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。執行步驟3到步驟5。

·TLS — 通過交換數位證書進行身份驗證。需要您執行步驟3至步驟7。

Infrastructure Client Interface

SSID: Infrastructure Client SSID (Range: 2-32 Characters)

Security: WPA Enterprise

WPA Versions: WPA WPA2

EAP Method: PEAP TLS

Username: Admin_Sr

Password:

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

步驟3. 無論您在步驟1中選擇了哪種方法，均可在使用者名稱欄位中輸入使用者名稱。

步驟4. 無論您在步驟1中選擇了哪種方法，均可在「密碼」欄位中輸入密碼。

步驟5. 如果您已選擇PEAP，請按一下 [此處](#) 繼續配置。如果您已選擇TLS，請轉至步驟6。

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6.如果您選擇TLS，請按一下HTTP或TFTP單選按鈕，在兩個傳輸模式之間選擇下載用於TLS驗證的證書檔案。

·HTTP — 通過Web伺服器或PC下載。

Transfer Method: HTTP TFTP

Filename: mini_httpd (2).pfx

— 選擇檔案 — 按一下以選擇證書檔案。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 — 從檔案伺服器下載。需要執行步驟。

Transfer Method: HTTP TFTP

Filename:

TFTP Server IPv4 Address:

— 檔名 — 在檔名欄位中輸入證書檔案的名稱。

- TFTP伺服器IPv4地址 — 輸入TFTP伺服器的IP地址。

注意： Certificate File Transfer欄位顯示WAP中是否存在證書， Certificate Expiration Date欄位顯示當前證書的到期日期。

步驟7.按一下**Upload**。

按一下[here](#)以繼續設定。