

# Configurazione di Work Group Bridge sui punti di accesso WAP121 e WAP321

## 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. È consigliabile utilizzare questa funzionalità quando non è possibile utilizzare la funzionalità Servizi di distribuzione Windows, poiché la funzionalità Servizi di distribuzione Windows è una soluzione di bridge preferita per WAP121 e WAP321. Quando la funzionalità di bridge per gruppi di lavoro è abilitata, la funzionalità di bridge Servizi di distribuzione Windows non funziona. Per informazioni sulla configurazione di WDS Bridge, fare riferimento all'articolo *Configurazione del bridge WDS (Wireless Distribution System) sui punti di accesso WAP121 e WAP321*.

In questo articolo viene spiegato come configurare il bridge di gruppi di lavoro sui punti di accesso WAP121 e WAP321.

## Dispositivi interessati

- WAP121
- WAP321

## Versione del software

- 1.0.3.4

## Configura bridge per gruppi di lavoro

**Nota:** Per abilitare il bridge per gruppi di lavoro, è necessario abilitare il clustering nel WAP. Se è disattivata, è necessario disabilitare Single Point Setup che a sua volta abilita il clustering. Tutti i dispositivi WAP che fanno parte del bridge di gruppi di lavoro devono avere impostazioni comuni per radio, modalità IEEE 802.11, larghezza di banda del canale e canale (audio non consigliato). 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 WAP121 e WAP321*.

Passaggio 1. Accedere all'Utilità Configurazione punto di accesso e scegliere **Wireless > Bridge per gruppi di lavoro**. Viene visualizzata la pagina *WorkGroup Bridge*:

## 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)

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

## 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)

Passaggio 3. Immettere il nome SSID (Service Set Identifier) nel campo *SSID* per l'interfaccia client dell'infrastruttura.


**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
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest
08:00:27:00:00:00	(Non Broadcasting)
08:00:27:00:00:00	WPSU-Guest

**Suggerimento:** Per analizzare gli SSID adiacenti simili, è inoltre possibile fare clic sull'icona **Arrow** accanto al campo *SSID*. Questa opzione è abilitata solo se il rilevamento dell'access point è abilitato nel rilevamento dell'access point non autorizzato che è disabilitato per impostazione predefinita. Per abilitare il rilevamento dei punti di accesso non autorizzati, consultare l'articolo *Rogue AP Detection sui punti di accesso WAP121 e WAP321*.

Passaggio 4. Selezionare il tipo di protezione per autenticare una stazione client sul dispositivo WAP upstream (Interfaccia client infrastruttura) dall'elenco a discesa *Protezione*. I valori possibili sono:

### WorkGroup Bridge

Refresh

WorkGroup Bridge Mode:  Enable

---

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security: 


- None
- Static WEP
- WPA Personal
- WPA Enterprise
 (+)

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

Connection Status:

---

**Access Point Interface**

Status:  Enable

SSID:  (Range: 2-32 Characters)

SSID Broadcast:  Enable

Security:  (+)

MAC Filtering:

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

Save

·Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questa opzione, andare al passaggio 5.

·WEP statico: WEP statico è la sicurezza minima e può supportare fino a 4 chiavi di lunghezza compresa tra 64 e 128 bit. La stessa chiave deve essere utilizzata in tutti i nodi. Per la configurazione di WEP statici, passare a [WEP statici](#).

·WPA Personal: WPA Personal è più avanzato rispetto a WEP e può supportare 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. Per la configurazione di WPA Personal, vedere [WPA Personal for Client Interface](#).

·WPA Enterprise: WPA Enterprise è la protezione più avanzata e consigliata. Utilizza il protocollo PEAP (Protected Extensible Authentication Protocol), in cui ogni singolo utente wireless in WAP è autorizzato con nomi utente e password individuali che supportano persino gli standard di crittografia AES. Utilizza anche Transport Layer Security (TLS) oltre a PEAP, in cui ogni utente deve fornire un certificato aggiuntivo per ottenere l'accesso. Il metodo di crittografia è RC4 per WPA e Advanced Encryption Standard (AES) per WPA2. Per la configurazione dell'organizzazione WPA, andare a [WPA Enterprise](#).

**Nota:** A seconda della modalità scelta per IEEE 802.11, la disponibilità delle opzioni

precedenti può variare.

Passaggio 5. Immettere l'ID VLAN nel campo *ID VLAN* per l'interfaccia client dell'infrastruttura.

### 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)

Passaggio 6. Selezionare **Enable** nel campo *Status* (Stato) per abilitare il bridging sull'interfaccia del punto di accesso.

### 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)

Passaggio 7. Inserire l'SSID (Service Set Identifier) nel nome del campo *SSID* dell'interfaccia del punto di accesso.

Passaggio 8. (Facoltativo) Se si desidera trasmettere il SSID downstream, selezionare **Abilita** nel campo *Trasmissione SSID* da trasmettere. È attivata per impostazione predefinita.

Passaggio 9. Scegliere il tipo di protezione per autenticare le stazioni client downstream sul dispositivo WAP (Access Point Interface) dall'elenco a discesa Protezione. I valori possibili sono:



## 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

·Nessuno — Aperto o senza protezione. Questo è il valore predefinito. Se si sceglie questa opzione, ignorare il passaggio 10.

·WEP statico: WEP statico è la sicurezza minima e può supportare fino a 4 chiavi di lunghezza compresa tra 64 e 128 bit. Per la configurazione di WEP statici, passare a [WEP statici](#)

·WPA Personal: WPA Personal è più avanzato rispetto a WEP e può supportare 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. Per la configurazione di WPA Personal, vedere [WPA Personal for Access Point Interface](#).

Passaggio 10. 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. I valori possibili sono:



### 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:  (Dropdown menu with options: Disabled, Local, RADIUS)

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

Save

·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 11. Immettere l'ID VLAN nel campo ID VLAN per l'interfaccia client del punto di accesso.

### 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)

**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 12. Fare clic su **Save** per salvare le impostazioni.

## [WEP statico](#)

**Infrastructure Client Interface**

SSID:  (Range: 2-32 Characters)

Security:

Transfer Key Index:

Key Length:  64 bits  128 bits

Key Type:  ASCII  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

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

Connection Status: **Disconnected**

Passaggio 1. Quando si sceglie WEP statico, vengono visualizzati alcuni campi aggiuntivi. Dall'elenco a discesa nel campo *Indice chiave di trasferimento*, scegliere un indice di chiave. I valori disponibili sono 1, 2, 3 e 4. Il valore predefinito è 1. L'indice della chiave è diverso per le diverse WLAN. I dispositivi collegati a una particolare WLAN devono avere lo stesso indice di chiave. Questa chiave viene utilizzata per crittografare i dati per la comunicazione.

Passaggio 2. Nel campo *Lunghezza chiave*, scegliere il pulsante di opzione **64 bit** o **128 bit**. Specifica la lunghezza della chiave utilizzata.

Passaggio 3. Fare clic sul pulsante di opzione desiderato nel campo *Tipo di chiave*. Le chiavi WEP sono in genere in formato esadecimale.

- ASCII - ASCII (American Standard Code for Information Interchange) è uno schema di codifica dei caratteri basato sull'alfabeto inglese codificato in 128 caratteri specificati.

- HEX — HEX (esadecimale) è un sistema numerico posizionale con base 16. Utilizza 16 simboli distinti da 0 a 9 per numeri da 0 a 9 e A,B,C,D,E,F per rappresentare valori da 10 a 15. Ogni valore esadecimale rappresenta quattro cifre binarie.

Passaggio 4. Inserire fino a quattro chiavi WEP nei quattro campi successivi contrassegnati come 1, 2, 3 e 4 sotto il campo *Chiave WEP*. Si tratta di una stringa immessa come chiave. La lunghezza della chiave varia in base alla lunghezza e al tipo della chiave. La lunghezza richiesta è indicata accanto al campo Chiave WEP. Le stringhe della chiave WEP devono corrispondere in tutti i nodi WAP (AP e Client) e devono trovarsi nello stesso campo. Ciò significa che se la stringa 1 è la chiave 1 in un dispositivo, la stringa 1 deve essere la chiave 1 anche negli altri dispositivi del bridge per gruppi di lavoro.

## [WPA Personal per interfaccia client](#)

**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

Passaggio 1. Controllare le versioni WPA desiderate dal campo *Versioni WPA*. In genere, WPA viene scelto solo se alcuni dei WAP nel sistema bridge non supportano WPA2. WPA2 è il più avanzato e consigliato.

- WPA - Se la rete dispone di stazioni client che supportano la versione originale di WPA.
- WPA2: se tutte le stazioni client della rete supportano WPA2. Questa versione del protocollo offre la migliore protezione per lo standard IEEE 802.11i.

Passaggio 2. Immettere la chiave WPA condivisa nel campo *Chiave*. La chiave può includere caratteri alfanumerici, maiuscoli e minuscoli e caratteri speciali.

## [WPA Personal for Access Point Interface](#)

Security:

WPA Versions:  WPA  WPA2

Cipher Suites:  TKIP  CCMP (AES)

Key:  (Range: 8-63 Characters)

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

Passaggio 1. Controllare le versioni WPA desiderate dal campo *Versioni WPA*. Di solito, WPA viene scelto solo se alcuni dei WAP interessati non supportano WPA2; in caso contrario, si consiglia WPA2.

- WPA - Se la rete dispone di stazioni client che supportano la versione originale di WPA.
- WPA2: se tutte le stazioni client della rete supportano WPA2. Questa versione del protocollo offre la migliore protezione per lo standard IEEE 802.11i.

**Nota:** Se la rete è una combinazione di client di WPA e WPA2, selezionare entrambe le caselle di controllo. Ciò consente l'associazione e l'autenticazione delle stazioni client WPA e WPA2, ma utilizza il più affidabile WPA2 per i client che lo supportano.

Passaggio 2. Scegliere le suite di cifratura desiderate dal campo *Suite di cifratura*.

·TKIP: il protocollo TKIP (Temporal Key Integrity Protocol) utilizza solo uno standard RC4 a 64 bit.

·CCMP (AES)— Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) è il protocollo di sicurezza utilizzato da AES (Advanced Encryption Standard). Si consiglia WPA2 con CCMP in quanto offre uno standard di crittografia più potente.

**Nota:** Potete scegliere uno dei due o entrambi. I client TKIP e AES possono essere associati al dispositivo WAP.

Passaggio 3. Immettere la chiave WPA condivisa nel campo *Chiave*. La chiave può includere caratteri alfanumerici, maiuscoli e minuscoli e caratteri speciali.

Passaggio 4. Inserire il tasso nel campo *Tasso di aggiornamento chiave trasmissione*.

## WPA - Enterprise

The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID field is set to 'test'. The Security dropdown is set to 'WPA Enterprise'. Under 'WPA Versions', both 'WPA' and 'WPA2' are selected. The 'EAP Method' is set to 'PEAP'. There are empty fields for 'Username' and 'Password'. The 'VLAN ID' is set to '1'. The 'Connection Status' is 'Disconnected'.

Passaggio 1. Controllare le versioni WPA desiderate nel campo *Versioni WPA*. Di solito WPA viene scelto solo se alcuni dei WAP nel sistema bridge non supportano WPA2. WPA2 è il più avanzato e consigliato.

·WPA - Se la rete dispone di stazioni client che supportano la versione originale di WPA.

·WPA2: se tutte le stazioni client della rete supportano WPA2. Questa versione del protocollo offre la migliore protezione per lo standard IEEE 802.11i.

**Nota:** Se la rete è una combinazione di client di WPA e WPA2, selezionare entrambe le caselle di controllo. Ciò consente l'associazione e l'autenticazione delle stazioni client WPA e WPA2, ma utilizza il più affidabile WPA2 per i client che lo supportano.

Passaggio 2. Fare clic sul pulsante di opzione appropriato per scegliere tra i due metodi EAP.

·PEAP — Protected EAP. Si basa su TLS ma evita l'installazione di certificati digitali su ogni client. Fornisce invece l'autenticazione tramite un nome utente e una password. Se si

sceglie questa opzione, passare a [PEAP \(Protected Extensible Authentication Protocol\)](#).

·TLS: autenticazione tramite scambio di certificati digitali. Se si sceglie questa opzione, passare a [TLS \(Transport Layer Security\)](#).

### [PEAP \(Protected Extensible Authentication Protocol\)](#)

The screenshot shows the 'Infrastructure Client Interface' configuration window. It includes the following fields and options:

- SSID:** A text box containing 'test' with a help icon and '(Range: 2-32 Characters)'.
- Security:** A dropdown menu set to 'WPA Enterprise' with a minus icon.
- WPA Versions:** Radio buttons for 'WPA' (checked) and 'WPA2' (unchecked).
- EAP Method:** Radio buttons for 'PEAP' (checked) and 'TLS' (unchecked).
- Username:** A text box containing 'Admin\_Sr'.
- Password:** A text box with masked characters '.....'.
- VLAN ID:** A text box containing '1' with a help icon and '(Range: 1 - 4094, Default: 1)'.

Passaggio 1. Inserire un nome utente nel campo *Nome utente*.

Passaggio 2. Immettere una password nel campo *Password*.

### [TLS \(Transport Layer Security\)](#)

**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

Passaggio 1. Scegliere la modalità di trasferimento per scaricare un file di certificato per l'autenticazione TLS.

·HTTP: scaricare il certificato da un server Web del PC. Se si sceglie questa opzione, passare a [HTTP](#).

·TFTP - Se si desidera scaricare il certificato da un file server. Se si sceglie questa opzione, passare al protocollo [TFTP](#).

## [HTTP](#)

Transfer Method:  HTTP  TFTP

Filename:  mini\_httpd (2).pfx

Passaggio 1. Fare clic su **Scegli file** per selezionare un file di certificato. Deve essere un file di tipo certificato con estensione .pem, .pfx, ecc. In caso contrario, il caricamento del file non riuscirà.

## [TFTP](#)



Transfer Method:  HTTP  
 TFTP

Filename

TFTP Server IPv4 Address:

Passaggio 1. Immettere il nome del file di certificato nel campo *Nome file*.

Passaggio 2. Immettere l'indirizzo IP del server TFTP.

**Nota:** Nel campo Trasferimento file certificato viene indicato se è presente un certificato in WAP e nel campo Data scadenza certificato viene visualizzata la data di scadenza del certificato corrente.

Passaggio 3. Fare clic su **Upload** per caricare il file nel dispositivo.