

# WAP551 및 WAP561 액세스 포인트의 작업 그룹 브리지 구성

## 목표

이 문서에서는 WAP551 및 WAP561 액세스 포인트에서 작업 그룹 브리지를 구성하는 방법에 대해 설명합니다.

작업 그룹 브리지 기능을 사용하면 WAP(Wireless Access Point)에서 원격 클라이언트와 작업 그룹 브리지 모드에 연결된 무선 LAN 간의 트래픽을 연결할 수 있습니다. 원격 인터페이스와 연결된 WAP 디바이스를 액세스 포인트 인터페이스라고 하며, 무선 LAN과 연결된 디바이스를 인프라 인터페이스라고 합니다. WDS 기능은 WAP551 및 WAP 561의 기본 브리지 솔루션이므로 WDS 기능을 사용할 수 없는 경우 이 기능을 사용하는 것이 좋습니다. 작업 그룹 브리지 기능을 사용하면 WDS 브리지 기능이 작동하지 않습니다. WDS 브리지가 구성된 방법을 보려면 *WAP551 및 WAP561 액세스 포인트의 WDS(Wireless Distribution System) Bridge Configuration(WDS) 브리지를 참조하십시오.*

## 적용 가능한 디바이스

- WAP551
- WAP561

## 소프트웨어 버전

- v1.0.4.2

## 작업 그룹 브리지 구성

**참고:**작업 그룹 브리지 클러스터링을 활성화하려면 WAP에서 활성화해야 합니다. 비활성화된 경우 단일 지점 설정을 비활성화해야 합니다. 그러면 클러스터링이 활성화됩니다. 워크그룹 브리지에 참여하는 모든 WAP 장치는 라디오, IEEE 802.11 모드, 채널 대역폭 및 채널에 대한 공통 설정을 가져야 합니다(오디오는 권장되지 않음). 모든 디바이스에서 이 설정이 동일한지 확인하려면 라디오 설정을 조회합니다. 이러한 설정을 구성하려면 *WAP551/WAP561의 라디오 설정을 참조하십시오.*

1단계. 웹 구성 유틸리티에 로그인하고 **무선 > 작업 그룹 브리지**를 선택합니다. **작업 그룹 브리지** 페이지가 열립니다.

## 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:

2단계. Work Group Bridge Mode(작업 그룹 브리지 모드) 필드에서 **Enable(활성화)**을 선택하여 작업 그룹 브리지 기능을 활성화합니다.

## 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

3단계. 이 단계는 WAP561에만 필요합니다. **Radio1** 또는 **Radio 2** 라디오 버튼을 클릭하여 라디오 인터페이스 중 하나를 선택합니다.라디오 인터페이스가 하나만 있는 WAP551에 대해 이 단계를 무시합니다.어떤 라디오가 설정되었는지 그리고 어떤 매개변수가 라디오 설정을 조회하는지 알아보려면 라디오 설정을 구성하려면 WAP551/WAP561의 라디오 설정을 참조하십시오.

4단계. SSID 필드에 인프라 클라이언트 인터페이스 또는 업스트림 액세스 포인트(AP)의 SSID(Service Set Identifier) 이름을 입력합니다.

**팁:**SSID 필드 옆의 화살표 아이콘을 클릭하여 유사한 인접 디바이스 SSID를 검색할 수도 있습니다.이는 비인가 AP 탐지에서 AP 탐지가 활성화된 경우에만 활성화됩니다(기본적으로 비활성화됨). Rogue AP 탐지를 활성화하려면 WAP561 및 WAP551의 AP(Rogue Access Point) 탐지를 참조하십시오.

5단계. Infrastructure Client Interface(인프라 클라이언트 인터페이스) 섹션의 Security(보안) 필드에 있는 드롭다운 목록에서 업스트림 WAP 디바이스(Infrastructure Client Interface)에서 클라이언트 스테이션으로 인증할 보안 유형을 선택합니다.가능한 선택 사항은 아래와 같습니다.

- None — 보안 기능이 없거나 개방적입니다.이것이 기본값입니다.Configure VLAN ID and Access Point Interface(VLAN ID 및 액세스 포인트 인터페이스 구성) 섹션으로 건너뛰도록 선택하면 됩니다.

- 정적 WEP — 고정 WEP는 최소 보안이며 최대 4개의 키 길이 64~128비트를 지원할 수 있습니다.모든 노드에서 동일한 키를 사용해야 합니다.

- WPA Personal — WPA Personal은 WEP에 비해 더 고급이며 8~63자의 키를 지원할 수 있습니다.암호화 방법은 WPA2용 WPA 및 WPA2용 AES(Advanced Encryption Standard)의 RC4입니다. WPA2는 보다 강력한 암호화 표준을 사용하므로 권장됩니다.

- WPA Enterprise — WPA Enterprise는 가장 진보적이고 권장되는 보안입니다.AP는 AES 암호화 표준도 지원할 수 있는 개별 사용자 이름 및 비밀번호로 WAP(Protected Extensible Authentication Protocol)를 사용하여 WAP 아래의 각 무선 사용자에게 권한을 부여합니다.또한 PEAP와 함께 TLS(Transport Layer Security)를 사용합니다. PEAP는 각 사용자와 모든 사용자가 액세스를 위해 추가 인증서를 제공해야 합니다.암호화 방법은 WPA2의 WPA 및

AES(Advanced Encryption Standard)의 RC4입니다.

**참고:**어떤 IEEE 802.11 모드를 선택했는지에 따라 위의 옵션의 사용 가능 여부는 다를 수 있습니다.

6단계. 5단계에서 선택한 옵션에 따라 옵션 링크 중 하나를 클릭하고 적절한 절차를 수행합니다. None(없음)을 선택한 경우 이러한 절차를 구성할 필요가 없습니다.

The screenshot shows a configuration window with two main sections: 'Infrastructure Client Interface' and 'Access Point Interface'.  
In the 'Infrastructure Client Interface' section, the SSID is 'Infrastructure Client SSID', Security is 'None', VLAN ID is '102', and Connection Status is 'Disconnected'.  
In the 'Access Point Interface' section, Status is 'Enable', SSID is 'Access Point SSID', SSID Broadcast is 'Enable', Security is 'None', MAC Filtering is 'Local', MAC Acl Mode is 'Accept', and VLAN ID is '1'.  
A 'Save' button is located at the bottom left of the interface.

**7단계.** VLAN ID 필드에 인프라 클라이언트 인터페이스의 VLAN ID를 입력합니다.

8단계. Status(상태) 필드에서 **Enable(활성화)**을 선택하여 액세스 포인트 인터페이스에서 브리징을 활성화합니다.

9단계. SSID 필드에 액세스 포인트 인터페이스의 SSID(Service Set Identifier) 이름을 입력합니다.

10단계(선택 사항) 다운스트림 SSID(Access Point Interface SSID)를 브로드캐스트하려면 SSID Broadcast 필드에서 Enable(활성화)을 선택합니다.기본적으로 활성화되어 있습니다.

11단계. Security(보안) 드롭다운 목록에서 WAP 디바이스(Access Point Interface)에 대한 다운스트림 클라이언트 스테이션을 인증할 보안 유형을 선택합니다.가능한 값은 다음과 같습니다.

- None — 보안 기능이 없거나 개방적입니다.이것이 기본값입니다.이 옵션을 선택한 경우 12단계부터 15단계까지 건너뛴니다.16단계로 이동합니다.

- 정적 WEP — 고정 WEP는 최소 보안이며 최대 4개의 키 길이 64~128비트를 지원할 수 있

습니다. 고정 [WEP 구성](#) 섹션을 따릅니다. 16단계로 건너뛰니다.

·WPA Personal — WPA Personal은 WEP에 비해 더 고급이며 8~63자의 키를 지원할 수 있습니다. 암호화 방법은 TKIP(Temporal Key Integrity Protocol) 또는 CCMP(Block Chaining Message Authentication Code Protocol)가 있는 Counter Cipher Mode입니다. CCMP를 사용하는 WPA2는 64비트 RC4 표준만 사용하는 TKIP와 비교하여 더 강력한 암호화 표준인 AES(고급 암호화 표준)가 있으므로 권장됩니다.

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)

시간 절약: 11단계에서 WPA Personal을 선택한 경우에만 12단계부터 15단계까지 수행합니다.

12단계. WPA 버전을 선택하려면 해당 확인란을 선택합니다. 서로 다른 WAP 클라이언트에서 WPA 버전과 WPA2를 모두 선택할 수 있습니다.

13단계. 적절한 확인란을 선택하여 암호 그룹을 선택합니다. TKIP 및 CCMP(AES)를 모두 선택합니다.

14단계. 키 필드에 공유 WPA 키를 입력합니다. 키에는 영숫자, 대문자 및 소문자, 특수 문자가 포함될 수 있습니다.

15단계. Broadcast Key Refresh Rate 필드에 원하는 키 새로 고침 간격을 입력합니다. 모든 WAP 클라이언트에 대해 그룹 키를 새로 고쳐야 하는 간격입니다.

16단계. MAC Filtering 드롭다운 목록에서 액세스 포인트 인터페이스에 대해 구성할 MAC 필터링 유형을 선택합니다. 활성화되면 사용자는 사용하는 클라이언트의 MAC 주소를 기반으로 WAP에 대한 액세스 권한을 부여받거나 거부됩니다. 가능한 값은 다음과 같습니다.

·Disabled(비활성화됨) — 모든 클라이언트가 업스트림 네트워크에 액세스할 수 있습니다. 이것이 기본값입니다.

·로컬 — 업스트림 네트워크에 액세스할 수 있는 클라이언트 세트는 로컬로 정의된 MAC 주소 목록에 지정된 클라이언트로 제한됩니다.

·Radius — 업스트림 네트워크에 액세스할 수 있는 클라이언트 집합은 RADIUS 서버의 MAC 주소 목록에 지정된 클라이언트로 제한됩니다.

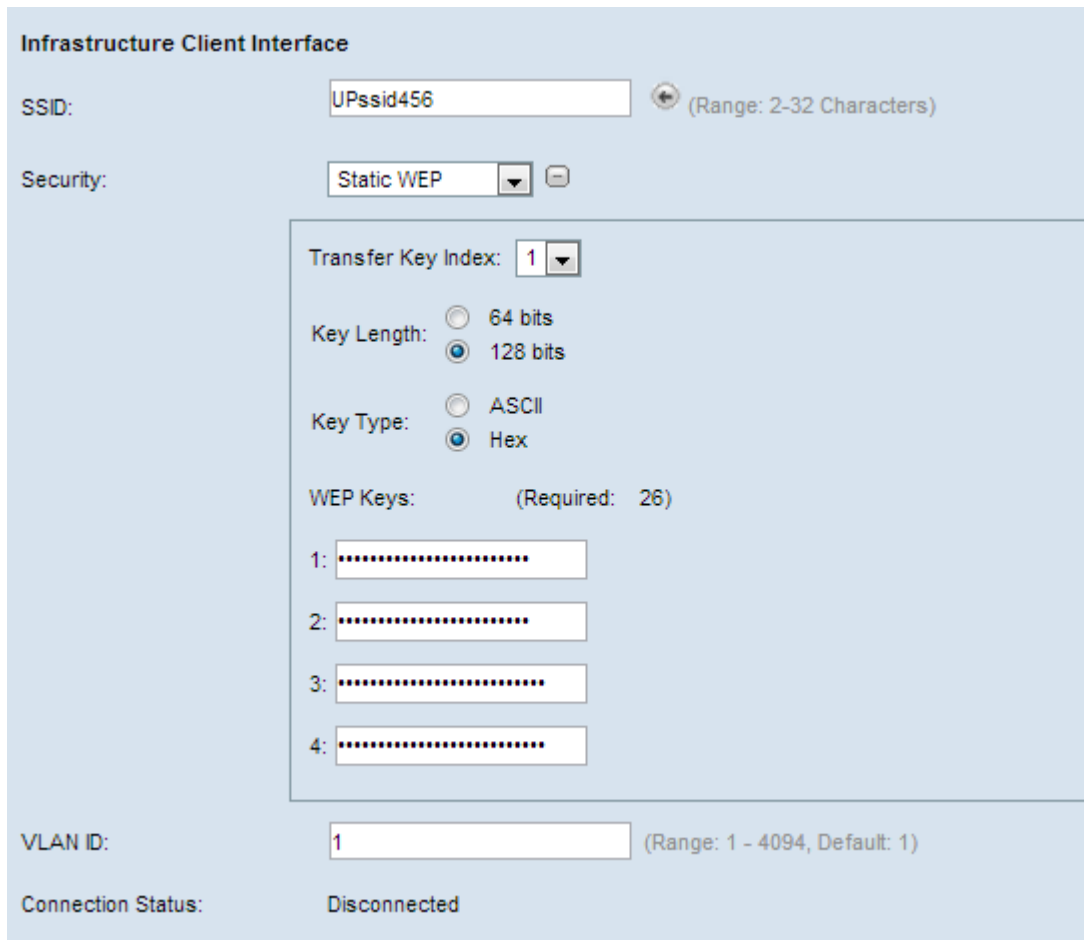
17단계. VLAN ID 필드에 액세스 포인트 클라이언트 인터페이스의 VLAN ID를 입력합니다.

**참고:** 패킷 브리징을 허용하려면 액세스 포인트 인터페이스 및 유선 인터페이스의 VLAN 컨피그레이션이 인프라 클라이언트 인터페이스의 VLAN 컨피그레이션과 일치해야 합니다.

18단계. 설정을 저장하려면 **저장**을 클릭합니다.

## 고정 WEP 구성

인증 보안 유형으로 고정 WEP를 구성하도록 선택한 경우 다음 단계를 수행합니다.



The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID is 'UPssid456'. The Security is set to 'Static WEP'. The Transfer Key Index is '1'. The Key Length is '128 bits'. The Key Type is 'Hex'. There are four WEP Key fields, each containing a series of dots. The VLAN ID is '1'. The Connection Status is 'Disconnected'.

1단계. 고정 WEP를 선택하면 일부 추가 필드가 나타납니다. Transfer Key Index 필드의 드롭 다운 목록에서 키 인덱스를 선택합니다. 사용 가능한 값은 1, 2, 3 및 4입니다. 기본값은 1입니다. 키 인덱스는 다른 WLAN에 대해 다릅니다. 고정 WLAN에 연결된 장치는 동일한 키 인덱스를 가져야 합니다. 이 키는 통신을 위해 데이터를 암호화하는 데 사용됩니다.

2단계. Key Length(키 길이) 필드에서 **64비트** 라디오 또는 버튼 또는 **128비트** 라디오 버튼을 선택합니다. 이는 사용된 키의 길이를 지정합니다.

3단계. **ASCII** 라디오 버튼 또는 **HEX** 라디오 버튼을 클릭하여 Key Type 필드에서 키 유형을 선택합니다. WEP 키는 일반적으로 16진수입니다.

Security: Static WEP

Transfer Key Index: 1

Key Length:  64 bits  128 bits

Key Type:  ASCII  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

4단계. WEP 키 필드 아래에 1,2,3 및 4로 표시된 다음 4개 필드에 최대 4개의 WEP 키를 입력합니다. 키로 입력된 문자열입니다. 키의 길이는 키의 길이와 유형에 따라 달라집니다. 필수 길이는 WEP 키 필드 옆에 표시됩니다. WEP 키 문자열은 모든 WAP 노드(AP 및 클라이언트)에서 일치해야 하며 같은 필드에 있어야 합니다. 즉, 문자열 1이 하나의 디바이스에서 키 1인 경우, 문자열 1도 작업 그룹 브리지의 다른 디바이스에서 키 1이어야 합니다.

컨피그레이션을 계속하려면 [여기](#)를 클릭하십시오.

## [WPA 개인 구성](#)

인증 보안 유형으로 WPA 개인을 구성하도록 선택한 경우 다음 단계를 수행합니다.

Infrastructure Client Interface

SSID:  (Range: 2-32 Characters)

Security: WPA Personal

WPA Versions:  WPA  WPA2

Key:  (Range: 8-63 Characters)

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

Connection Status: Disconnected

1단계. **WPA** 또는 **WPA2**를 선택하여 WPA 버전을 선택합니다. 일반적으로 WPA는 관련된 WAP가 WPA2를 지원하지 않는 경우에만 선택됩니다. 그렇지 않으면 WPA 2가 권장됩니다.

2단계. 키 필드에 공유 WPA 키를 입력합니다. 키에는 영숫자, 대문자 및 소문자, 특수 문자가 포함될 수 있습니다.

컨피그레이션을 계속하려면 [여기](#)를 클릭하십시오.

## [WPA 엔터프라이즈 구성](#)

WPA Enterprise를 인증 보안 유형으로 구성하도록 선택한 경우 다음 단계를 수행합니다.

Infrastructure Client Interface

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

Security: WPA Enterprise

WPA Versions:  WPA  WPA2

EAP Method:  PEAP  TLS

Username: [Empty]

Password: [Empty]

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

Connection Status: Disconnected

1단계. WPA Enterprise를 선택한 경우 WPA 또는 **WPA2**를 선택하여 WPA 버전을 선택합니다. 일반적으로 WPA는 브리지 시스템의 WAP가 WPA2를 지원하지 않는 경우에만 선택됩니다. WPA 2는 보다 진보적이고 권장되는 것입니다.

2단계. 적절한 라디오 버튼을 클릭하여 두 EAP 방법 중에서 선택합니다.

·PEAP — 보호된 EAP.TLS에 의존하지만 모든 클라이언트에 디지털 인증서를 설치하지 않습니다.대신 사용자 이름과 비밀번호를 통해 인증을 제공합니다.3단계부터 5단계까지 진행합니다.

·TLS — 디지털 인증서 교환을 통한 인증3단계부터 7단계까지 수행해야 합니다.

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: [Masked]

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

3단계. 1단계에서 선택한 방법에 관계없이 Username(사용자 이름) 필드에 사용자 이름을 입력합니다.



4단계. 1단계에서 선택한 방법에 관계없이 비밀번호 필드에 비밀번호를 입력합니다.

5단계. PEAP를 선택한 경우 [여기](#)를 클릭하여 구성을 계속 진행합니다. TLS를 선택한 경우 6단계로 이동합니다.

Infrastructure Client Interface

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

Security: WPA Enterprise

WPA Versions:  WPA  WPA2

EAP Method:  PEAP  TLS

Identity: Admin\_Sr

Private Key: .....

Certificate File Present: yes

Certificate Expiration Date: Dec 26 22:09:59 2019

Transfer Method:  HTTP  TFTP

Certificate File: Choose File No file chosen

Upload

6단계. TLS를 선택한 경우 **HTTP** 또는 **TFTP** 라디오 버튼을 클릭하여 두 전송 모드 중에서 선택하여 TLS 인증을 위한 인증서 파일을 다운로드합니다.

·HTTP — 웹 서버 또는 PC에서 다운로드합니다.

Transfer Method:  HTTP  TFTP

Filename: Choose File mini\_httpd (2).pfx

Upload

- 파일 선택 — 인증서 파일을 선택하려면 클릭합니다. 확장명이 .pem, .pfx인 인증서 형식 파일이어야 합니다. 그렇지 않으면 파일 업로드가 실패합니다.

·TFTP — 파일 서버에서 다운로드합니다. 단계를 수행해야 합니다.

Transfer Method:  HTTP  
 TFTP

Filename:

TFTP Server IPv4 Address:

- Filename — Filename 필드에 인증서 파일의 이름을 입력합니다.

- TFTP 서버 IPv4 주소 — TFTP 서버의 IP 주소를 입력합니다.

**참고:** Certificate File Transfer(인증서 파일 전송) 필드는 WAP에 인증서가 있는지 여부를 표시하며 Certificate Expiration Date(인증서 만료 날짜) 필드는 현재 인증서의 만료 날짜를 표시합니다.

7단계. Upload(업로드)를 클릭합니다.

컨피그레이션을 계속하려면 [여기](#)를 클릭하십시오.