

Werkgroepbridge instellen op WAP121 en WAP321 access points

Doel

De werkgroepbridge-functie stelt het Wireless Access Point (WAP) in staat om verkeer tussen een externe client en de draadloze LAN-unit te overbruggen die met de werkgroepbridge-modus is verbonden. Het WAP-apparaat dat aan de externe interface is gekoppeld, wordt bekend als een access point interface en het apparaat dat aan de draadloze LAN-interface is gekoppeld, wordt een infrastructuur-interface genoemd. Deze functie wordt aanbevolen wanneer de WDS-functie niet kan worden gebruikt omdat de WDS-functie een voorkeursbrugoplossing is voor WAP121 en WAP321. Wanneer de werkgroepbridge-functie is ingeschakeld, werkt de WDS-bridge-functie niet. Om te zien hoe WDS Bridge wordt geconfigureerd, raadpleegt u de *configuratie* van de *artikelen* *Wireless Distribution System (WDS) op WAP121 en WAP321 access points*.

Dit artikel legt uit hoe u de werkgroepbridge op WAP121- en WAP321-access points kunt configureren.

Toepasselijke apparaten

- WAP121
- WAP321

Softwareversie

- 1.0.3.4

Werkgroepbridge configureren

Opmerking: Om werkgroepbridge in staat te stellen, moet clustering in WAP zijn ingeschakeld. Als het uitgeschakeld is, moet u Single Point Setup uitschakelen die clustering mogelijk maakt. Alle WAP-apparaten die aan de Workgroup bridge deelnemen, moeten beschikken over gemeenschappelijke instellingen voor radio, IEEE 802.11-modus, kanaalbandbreedte en kanaal (audio niet aanbevolen). Om er zeker van te zijn dat deze instellingen in alle apparaten hetzelfde zijn, raadpleegt u de radio-instellingen. Om deze instellingen te configureren raadpleegt u het artikel *Configuratie van fundamentele draadloze radio-instellingen op WAP121 en WAP321 access points*.

Stap 1. Meld u aan bij het hulpprogramma Access Point Configuration en kies **Wireless > Workgroup Bridge**. De pagina *Werkgroepbridge* wordt geopend:

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)

Stap 2. Controleer het veld *Work Group* Bridge Mode in het veld *Work Group Brug Mode* in om de functie Workgroup bridge te kunnen inschakelen.

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


Stap 3. Voer de naam van de Service Set Identifier (SSID) in het veld *SSID* voor client-interface in.

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

Tip: U kunt ook op het pictogram **Arrow** naast het veld *SSID* klikken om voor soortgelijke buurtSSID's te scannen. Dit is alleen ingeschakeld als AP Detectie is ingeschakeld in de detectie van AP-schurk, die standaard uitgeschakeld wordt. Raadpleeg het artikel *Woorddetectie van AP-herkenning op WAP121 en WAP321 access points* om detectie van AP-afstanden mogelijk te maken.

Stap 4. Kies het type beveiliging om een client-station op het upstream WAP-apparaat (Infrastructuur-clientinterface) te authentifieren uit de vervolgkeuzelijst *Beveiliging*. De mogelijke waarden zijn:

WorkGroup Bridge

WorkGroup Bridge Mode: Enable

Infrastructure Client Interface

SSID: (Range: 2-32 Characters)

Security: (+)

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)

- Geen — Open of geen beveiliging. Dit is de standaardwaarde. Als u dit kiest, slaat u over op Stap 5.
- Statische EFN — Statische EFN is de minimale beveiliging en kan tot 4 sleutels van lengte 64 tot 128 bits ondersteunen. In alle knooppunten moet dezelfde toets worden gebruikt. Voor configuratie voor statische medeplichtigheid, ga naar [Static-li](#).
- Persoonlijk WAP - Persoonlijk ben geavanceerd in vergelijking met EVN en kan sleutels van lengte 8-63 tekens ondersteunen. De coderingsmethode is RC4 voor WAP en Advanced Encryption Standard (AES) voor WAP2. WAP2 wordt aanbevolen omdat deze een krachtigere coderingsstandaard heeft. Voor het configureren van de persoonlijk naam van WAP, ga naar [WAP Persoonlijk voor Clientinterface](#).
- WAP Enterprise — WAP Enterprise is de meest geavanceerde en aanbevolen beveiliging. Het maakt gebruik van Protected Extensible Authentication Protocol (PEAP), waarin elke draadloze gebruiker onder WAP is geautoriseerd met individuele gebruikersnamen en wachtwoorden die zelfs AES-encryptie-standaarden kunnen ondersteunen. Het maakt ook gebruik van TMS (Transport Layer Security, TLS) naast PEAP, waarin elke gebruiker ook een aanvullend certificaat moet verstrekken om toegang te krijgen. De coderingsmethode is RC4 voor WAP en Advanced Encryption Standard (AES) voor WAP2. Ga voor configuratie van de WAP-onderneming naar [WAP Enterprise](#).

Opmerking: Op basis van de keuze van de IEEE 802.11-modus kan de beschikbaarheid van de bovenstaande opties verschillen.

Stap 5. Voer de VLAN-id in het veld *VLAN-id* in voor de interface van de infrastructuurclient.

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)

Stap 6. Controleer **het** veld *Status inschakelen* om overbrugging op de interface van het access point mogelijk te maken.

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)

Stap 7. Voer de Service Set-id (SSID) in in de veldnaam *van SSID* voor de interface van het access point.

Stap 8. (Optioneel) Als u de downstreamSSID wilt uitzenden, controleert u op *SSID Broadcast*-veld **inschakelen** om te worden uitgezonden. Deze functie is standaard ingeschakeld.

Stap 9. Kies het type beveiliging om downloads van clientstations naar het WAP-apparaat (Access Point Interface) te controleren in de vervolgkeuzelijst Beveiligingsinstellingen. De mogelijke waarden zijn:

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

- Geen — Open of geen beveiliging. Dit is de standaardwaarde. Stap 10 als u dit kiest.
- Statische EFN — Statische EFN is de minimale beveiliging en kan tot 4 sleutels van lengte 64 tot 128 bits ondersteunen. Voor configuratie voor statische EFN, ga naar [Static-EFN](#)
- Persoonlijk WAP - Persoonlijk ben geavanceerd in vergelijking met EVN en kan sleutels van lengte 8 tot 63 tekens ondersteunen. De coderingsmethode is ofwel het TKIP-protocol (Temporal Key Integrity Protocol) of de Cmin-modus voor tegenstanders met Block Chaining Message Verifier Code Protocol (CCMP). WAP2 met CCMP wordt aanbevolen omdat deze een krachtiger coderingsstandaard heeft, Advanced Encryption Standard (AES) in vergelijking met de TKIP die alleen een 64-bits RC4-standaard gebruikt. Voor het configureren van de persoonlijk naam van WAP, ga naar [WAP Persoonlijk voor de interface van het access point](#).

Stap 10. Kies het type MAC-filtering dat u wilt configureren voor de interface van het access point in de vervolgkeuzelijst *MAC-filtering*. Indien ingeschakeld, worden gebruikers toegang tot de WAP verleend of geweigerd op basis van het MAC-adres van de client die zij gebruiken. De mogelijke waarden zijn:

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

- Uitgeschakeld — Alle klanten hebben toegang tot het stroomopwaarts netwerk. Dit is de standaardwaarde.
- Lokaal — De reeks klanten die tot het upstreamnetwerk kunnen toegang hebben is beperkt tot de klanten die in een lokaal gedefinieerde MAC-adreslijst zijn gespecificeerd.
- Straal — De reeks klanten die tot het upstreamnetwerk kunnen toegang hebben is beperkt tot de klanten die in een MAC-adreslijst op een RADIUS-server zijn gespecificeerd.

Stap 1. Voer de VLAN-id in het veld VLAN-id in voor de interface van de access point client.

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)

Opmerking: Om het overbruggen van pakketten toe te staan, zou de configuratie van VLAN voor de interface van het toegangspunt en de bekabelde interface die van de interface van de infrastructuurclient moeten passen.

Stap 12. Klik op **Opslaan** om de instellingen op te slaan.

[Statische Wi](#)

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**

Stap 1. Wanneer u Statische Wi kiest, verschijnen sommige extra velden. Kies in de vervolgkeuzelijst in het veld *Transfer Key Index* een belangrijke index. Beschikbare waarden zijn 1,2,3 en 4. De standaardwaarde is 1. De key index is anders voor verschillende WLAN. De apparaten die zijn aangesloten op een prioritair WLAN moeten dezelfde sleutelindex hebben. Deze toets wordt gebruikt om gegevens voor communicatie te versleutelen.

Stap 2. Kies in het veld *Key Length* de radioknop van **64 bits** of **128 bits**. Geeft de lengte van de gebruikte toets aan.

Stap 3. Klik het gewenste keuzerondje aan in het veld *toetstype*. De sleutels van het gebruik zijn meestal hex.

- ASCII — ASCII (American Standard Code for Information Interchange) is een tekencoderingsschema dat is gebaseerd op het Engelse alfabet dat is gecodeerd in 128 gespecificeerde tekens.
- HEX — HEX (Hexadecimaal) is een positioneel numeriek systeem met basis 16. Het gebruikt 16 verschillende symbolen 0-9 voor 0 tot 9 getallen en A,B,C,D,E,F om waarden van 10 tot 15 te vertegenwoordigen. Elk hexadecimaal vertegenwoordigt vier binaire cijfers.

Stap 4. Voer maximaal vier sleutels van EFN in in de volgende vier velden die als 1,2,3 en 4 gemarkeerd zijn onder het veld *van de sleutel van EFN*. Dit is een string die als de sleutel is ingevoerd. De lengte van de toets varieert afhankelijk van de lengte en het type van de toets. De gewenste lengte wordt naast het veld Gigabit-toets aangegeven. De de zeer belangrijke koorden van de van de EVN moeten in alle knopen van de WAP (AP en Clients) aan elkaar passen en moeten plaats in het zelfde gebied zijn. Dit betekent dat als string 1 belangrijk is in één apparaat, string 1 ook belangrijk 1 moet zijn in de andere apparaten in de werkgroepbridge.

WAP Persoonlijk voor clientinterface

Infrastructure Client Interface

SSID: test (Range: 2-32 Characters)

Security: WPA Personal

WPA Versions: WPA WPA2

Key: (Range: 8-63 Characters)

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

Connection Status: Disconnected

Stap 1. Controleer de gewenste WAP-versies in het veld *WAP-versies*. Gewoonlijk wordt WAP alleen geselecteerd als sommige WAP's in het brugsysteem geen WAP2 ondersteunen. WAP2 is het meest geavanceerde en aanbevolen.

- WAP — Als het netwerk clientstations heeft die de oorspronkelijke versie van WAP ondersteunen.
- WAP2 — Als alle clientstations op de netwerkondersteuning van WAP2. Deze protocolversie biedt de beste beveiliging volgens de standaard IEEE 802.11i.

Stap 2. Voer de gedeelde WAP-toets in het veld *Key in*. De toets kan alfanumerieke tekens, hoofdletters en kleine tekens en speciale tekens bevatten.

WAP Persoonlijk voor access point interface

Security: WPA Personal

WPA Versions: WPA WPA2

Cipher Suites: TKIP CCMP (AES)

Key: (Range: 8-63 Characters)

Broadcast Key Refresh Rate: 300 (Range: 0-86400)

Stap 1. Controleer de gewenste WAP-versies in het veld *WAP-versies*. WAP is doorgaans alleen geselecteerd als sommige van de betrokken WAP's geen ondersteuning bieden voor WAP2; Anders wordt WAP2 aanbevolen.

- WAP — Als het netwerk clientstations heeft die de oorspronkelijke versie van WAP ondersteunen.
- WAP2 — Als alle clientstations op de netwerkondersteuning van WAP2. Deze protocolversie biedt de beste beveiliging volgens de standaard IEEE 802.11i.

Opmerking: Als het netwerk een mix is van klanten van WAP en WAP2, controleer beide van de controlevakjes. Dit laat zowel WAP- als WAP2 clientstations associëren en authenticeren,

maar gebruikt de robuustere WAP2 voor klanten die dit ondersteunen.

Stap 2. Kies het gewenste algoritme uit het veld *Cipher Suites*.

- TKIP — Temporal Key Integrity Protocol (TKIP) gebruikt slechts een 64-bits RC4-standaard.
- CCMP (AES)— Counter Cipher Mode met Block Chaining Message Verification Code Protocol (CCMP) is het beveiligingsprotocol dat wordt gebruikt door AES (Advanced Encryption Standard). WAP2 met CCMP wordt aanbevolen omdat dit een krachtiger coderingsstandaard heeft.

Opmerking: U kunt kiezen of beide. Zowel TKIP- als AES-clients kunnen worden gekoppeld aan het WAP-apparaat.

Stap 3. Voer de gedeelde WAP-toets in het veld *Key in*. De toets kan alfanumerieke tekens, hoofdletters en kleine tekens en speciale tekens bevatten.

Stap 4. Voer het tarief in het veld *Broadcast Key Refresh Rate* in.

WAP-onderneming

The screenshot shows the 'Infrastructure Client Interface' configuration page. The SSID field contains 'test'. The Security dropdown is set to 'WPA Enterprise'. Below this, there are checkboxes for 'WPA Versions': 'WPA' is unchecked and 'WPA2' is checked. The 'EAP Method' section has 'PEAP' selected with a radio button and 'TLS' unselected. There are empty input fields for 'Username' and 'Password'. The 'VLAN ID' field contains '1'. The 'Connection Status' is 'Disconnected'.

Stap 1. Controleer de gewenste WAP-versies in het veld *WAP-versies*. WAP is meestal alleen geselecteerd als sommige WAP's in het brugsysteem geen WAP2 ondersteunen. WAP2 is het meest geavanceerde en aanbevolen.

- WAP — Als het netwerk clientstations heeft die de oorspronkelijke versie van WAP ondersteunen.
- WAP2 — Als alle clientstations op de netwerkondersteuning van WAP2. Deze protocolversie biedt de beste beveiliging volgens de standaard IEEE 802.11i.

Opmerking: Als het netwerk een mix is van klanten van WAP en WAP2, controleer dan de beide controlevakjes. Dit laat zowel WAP- als WAP2 clientstations associëren en authenticeren, maar gebruikt de robuustere WAP2 voor klanten die dit ondersteunen.

Stap 2. Klik op de juiste radioknop om te kiezen tussen de twee MAP-methoden.

- GOEDKOPE — beschermde MAP. Het maakt gebruik van TLS, maar vermijdt de installatie van digitale certificaten op elke cliënt. In plaats daarvan biedt het authenticatie door een gebruikersnaam en wachtwoord. Als u dit kiest, gaat u naar [PEAP \(Beschermd Extensible Authentication Protocol\)](#).
- TLS — Verificatie door uitwisseling van digitale certificaten. Als u dit kiest, gaat u naar [TLS \(Vervoerlaag beveiliging\)](#).

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

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

- SSID:** A text input field containing 'test' with a character count indicator '(Range: 2-32 Characters)'.
- Security:** A dropdown menu set to 'WPA Enterprise'.
- WPA Versions:** Two radio buttons: 'WPA' (checked) and 'WPA2' (unchecked).
- EAP Method:** Two radio buttons: 'PEAP' (checked) and 'TLS' (unchecked).
- Username:** A text input field containing 'Admin_Sr'.
- Password:** A password input field with masked characters '.....'.
- VLAN ID:** A text input field containing '1' with a character count indicator '(Range: 1 - 4094, Default: 1)'.

Stap 1. Voer een gebruikersnaam in het veld *Gebruikersnaam in*.

Stap 2. Voer een wachtwoord in het veld *Wachtwoord in*.

[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

Stap 1. Kies de overdrachtmodus om een certificaatbestand voor TLS-verificatie te downloaden.

- HTTP — Als u het certificaat wilt downloaden van een webserver van PC. Als je dit kiest, ga dan naar [HTTP](#).
- TFTP — Als u het certificaat wilt downloaden van een bestandserver. Als je dit kiest, ga dan naar [TFTP](#).

[HTTP](#)

Transfer Method: HTTP TFTP

Filename: mini_httpd (2).pfx

Stap 1. Klik op **Kies bestand** om een certificaatbestand te selecteren. Dit moet een bestand zijn met een certificaat als bestandsextensie .pem, .pfx enzovoort. Anders wordt het uploaden van bestanden niet geslaagd.

[TFTP](#)

Transfer Method: HTTP
 TFTP

Filename

TFTP Server IPv4 Address:

Stap 1. Voer de naam van het certificaatbestand in het veld *Bestandsnaam* in.

Stap 2. Voer het IP-adres van de TFTP-server in.

Opmerking: Het veld Bestandsoverdracht van het certificaat toont aan of er een certificaat in de WAP aanwezig is en het veld Verloopdatum van het certificaat toont de verloopdatum van het huidige certificaat.

Stap 3. Klik op **Upload** om bestand naar het apparaat te uploaden.