

Bekabelde WGB-clients (Workgroup Bridge) configureren met NAT

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Draadloze LAN-controller](#)

[Werkgroepbrug](#)

[Router](#)

[Draadloze LAN-controller](#)

[Werkgroepbrug](#)

[Router](#)

Inleiding

Dit document beschrijft de configuratie van bekabelde clients achter Network Access Translation om toegang te krijgen tot het netwerk via Workgroup Bridge.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- Concepten en configuratie van de 9800 Wireless LAN Controller (WLC)
- Concepten en configuratie van werkgroepbridge (WGB)
- Concepten en configuratie van Network Access Control (NAT)
- Schakelen tussen concepten en configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 9800-CL WLC Cisco IOS® XE 26.1.1
- WGB WP-WIFI6-B geïntegreerd in 1821 router versie 26.1.1
- Catalyst IR1821 Rugged Router, Cisco IOS 17.15.4
- 9300 Switch, Cisco IOS 17.15.4

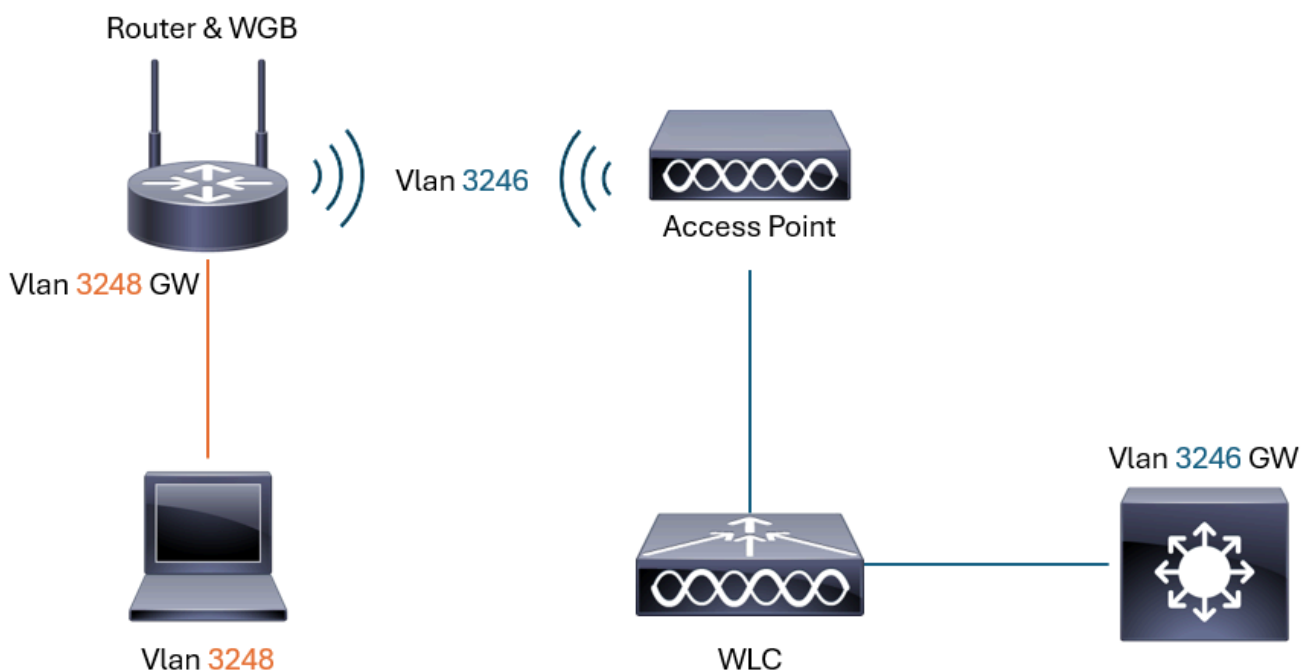
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Er zijn WGB-implementaties die vereisen dat de bekabelde clients achter de WGB zich in een ander vLAN bevinden dan de WGB en tegelijkertijd dat vLAN niet bestaat in de WGB, WLC of in de netwerkapparaten achter de WLC.

In dit scenario biedt het gebruik van NAT de configuratie en flexibiliteit die nodig zijn om de bekabelde clients te laten communiceren met het netwerk (toepassingen, internet, servers, enzovoort) achter de WLC.

Netwerkdigram



Configureren

Draadloze LAN-controller

In dit gedeelte wordt de basisconfiguratie van de WLAN-, WLAN-beleidsprofiel- en beleidstag uitgelegd om de SSID (Service Set Identifier) uit te zenden waarmee de WGB verbinding maakt.



Waarschuwing: elke configuratiewijziging op deze parameters in de productie kan leiden tot het verbreken van de verbinding met een draadloze client.

Stap 1. De SSID configureren.

Stap 1.1. Navigeer naar Configuration > Tags & Profiles > WLAN's. Klik op Add (Toevoegen). Voer de naam van het profiel en de SSID in. Klik op Apply (Toepassen).

GUI:

Configuration > Tags & Profiles > WLANs

+ Add × Delete Clone Enable WLAN Disable WLAN

Add WLAN

General Security Advanced

Profile Name* WGB

SSID* WGB

WLAN ID* 6

Status **ENABLED** ☒

Broadcast SSID **ENABLED** ☒

Wi-Fi 6E Compatibility 1/2 requirements met

Wi-Fi 7 Compatibility 0/3 requirements met 0/3 bands enabled

Radio Policy ⓘ

Show slot configuration

6 GHz
Status ☐ DISABLED

5 GHz
Status **ENABLED** ☒

2.4 GHz
Status ☐ DISABLED

802.11b/g Policy 802.11b/g ▼

Cancel Apply to Device

WLAN-configuratie

CLI:

```
config t
wlan WGB 6 WGB
radio policy dot11 5ghz
no shutdown
```

Stap 1.2. De SSID-beveiligingsparameters configureren. Kies PSK, voer het PSK-wachtwoord in en klik op Toepassen.

GUI:

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

☒ WPA + WPA2
☐ WPA2 + WPA3
☐ WPA3
☐ Static WEP
☐ None

MAC Filtering ☐

Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐
WPA2 Policy ☒

GTK Randomize ☐
OSEN Policy ☐

WPA2 Encryption

AES(CCMP128) ☒
CCMP256 ☐

GCMP128 ☐
GCMP256 ☐

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Disabled

Over the DS ☐

Reassociation Timeout *

20

Auth Key Mgmt (AKM)

802.1X

⚠

☐
FT + 802.1X ☐

802.1X-SHA256 ☐
CCKM

⚠

☐

PSK

⚠

☒
FT + PSK ☐

PSK-SHA256 ☐
Easy-PSK ☐

PSK Format

ASCII

PSK Type

Unencrypted

Pre-Shared Key*

↶ Cancel

📁

Update & Apply to Device

WLAN-beveiliging

CLI:

```

config t
wlan WGB 6 WGB
shutdown
no security ft adaptive
security wpa psk set-key ascii 0 12345678
no security wpa akm dot1x
security wpa akm psk
no shutdown

```

Stap 1.3. AironetIE configureren in de SSID. Navigeer naar het tabblad Geavanceerd, schakel

CCX Aironet IE in en klik op Toepassen.

GUI:

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

GeneralSecurityAdvancedAdd To Policy Tags

Coverage Hole Detection☒

CCX Aironet IE☒

Advertise AP Name☐

P2P Blocking Action

Disabled

Multicast Buffer

DISABLED

Media Stream Multicast-direct☐

11ac MU-MIMO☒

Wi-Fi to Cellular Steering☐

Wi-Fi Alliance Agile Multiband

DISABLED

Fastlane+ (ASR) ☒

Deny LAA (RCM) clients☐

6 GHz Client Steering☐

Latency Measurements Announcements☐

Universal Admin☐

OKC☒

Load Balance☐

Band Select☐

IP Source Guard☐

WMM Policy

Allowed

mDNS Mode

Bridging

Off Channel Scanning Defer

Defer Priority

☐0☐1☐2

☐3☐4☒5

☒6☐7

Scan Defer Time

100

Assisted Roaming (11k)

Prediction Optimization☐

Max Client Connections

Per WLAN

n

Cancel

Update & Apply to Device

Aironet IE

CLI:

<#root>

```
config t
wlan WGB 6 WGB
shutdown
ccx aironet-iesupport
no shutdown
```

Stap 2. Het WLAN-beleidsprofiel configureren.

Stap 2.1. Navigeer naar Configuration > Tags & Profiles > WLAN's. Klik op Add (Toevoegen). Voer een naam in. Configureren als Status en passieve client inschakelen. Klik vervolgens op Toepassen.

GUI:

The screenshot shows the 'Add Policy Profile' dialog box in a network management interface. The breadcrumb trail at the top is 'Configuration > Tags & Profiles > Policy'. Below the breadcrumb are three buttons: '+ Add' (highlighted with a green box), 'Delete', and 'Clone'. The dialog title is 'Add Policy Profile' with a close button (X) in the top right corner. A yellow warning banner states: '⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' Below the banner are five tabs: 'General' (highlighted with a green box), 'Access Policies', 'QOS and AVC', 'Mobility', and 'Advanced'. The 'General' tab contains several configuration fields: 'Name*' (text box with 'PolicyWGB'), 'Description' (text box with 'Enter Description'), 'Status' (toggle switch set to 'ENABLED'), 'Passive Client' (toggle switch set to 'ENABLED'), 'IP MAC Binding' (toggle switch set to 'ENABLED'), and 'Encrypted Traffic Analytics' (toggle switch set to 'DISABLED'). To the right of these fields is a 'WLAN Switching Policy' section with four toggle switches: 'Central Switching' (ENABLED), 'Central Authentication' (ENABLED), 'Central DHCP' (ENABLED), and 'Flex NAT/PAT' (DISABLED). Below these is a 'CTS Policy' section with three fields: 'Inline Tagging' (checkbox, unchecked), 'SGACL Enforcement' (checkbox, unchecked), and 'Default SGT' (text box with '2-65519'). At the bottom of the dialog are two buttons: 'Cancel' and 'Apply to Device'.

Configuration > Tags & Profiles > Policy

+ Add Delete Clone

Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General Access Policies QOS and AVC Mobility Advanced

Name* PolicyWGB

Description Enter Description

Status ENABLED

Passive Client ENABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT 2-65519

Cancel Apply to Device

WLAN-beleid

CLI:

<#root>

```
config t
wireless profile policy PolicyWGB
passive-client
no shutdown
```

Stap 2.2. Navigeer naar Toegangsbeleid. Klik op VLAN/VLAN-groep en kies de WGB vLAN.

GUI:

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

RADIUS Profiling☐

HTTP TLV Caching☐

DHCP TLV Caching☐

WLAN Local Profiling

Global State of Device ClassificationDisabled ⓘ

Local Subscriber Policy NameSearch or Select

VLAN

VLAN/VLAN GroupVLAN3246 x ⓘ

Multicast VLANEnter Multicast VLAN

Note : Selecting a VLAN Group is a valid config only for Central Switching SSIDs. Do not use with SSIDs enabled for Flex Local Switching

WLAN ACL

IPv4 ACLSearch or Select

IPv6 ACLSearch or Select

URL Filters ⓘ

Pre AuthSearch or Select

Post AuthSearch or Select

Cancel

Update & Apply to Device

VLAN-configuratie

CLI:

```
conf t
wireless profile policy PolicyWGB
shutdown
vlan VLAN3246
no shutdown
```

Stap 3. Configureer de beleidstag en pas deze toe op de toegangspunten (AP) waarmee de WGB verbinding maakt.

Stap 3.1. Navigeer naar Configuration > Tags & Profiles > Tags. Klik op Beleid en vervolgens op Toevoegen. Voer een naam in en klik op Toevoegen. Kies de SSID en het beleidsprofiel. Klik op Apply (Toepassen).

GUI:

Configuration > Tags & Profiles > Tags

Policy Site RF AP

+ Add × Delete Clone

Add Policy Tag

Name* WGBTag

Description Enter Description

WLAN-POLICY Maps : 1

+ Add × Delete

☐	WLAN Profile	Policy Profile
☐	WGB	PolicyWGB

1 - 1 of 1 Items

Map WLAN and Policy

Cancel Apply to Device

labelen

CLI:

<#root>

```
config t
wireless tag policy WGBTag
wlan WGB policy PolicyWGB
```



Opmerking: vergeet niet om de Policy Tag toe te passen op alle toegangspunten die de SSID uitzenden.

Werkgroepbrug

In dit gedeelte wordt de configuratie op de WGB uitgelegd. Met de configuratie kan de WGB verbinding maken met het netwerk en verbinding maken via vLAN3246.

CLI:

```
configure ap hostname WGB1
configure ap address ipv4 static 10.10.246.4 255.255.255.0 10.10.246.1
configure ap management add username admin password P0ssw0rd123! secret P0ssw0rd123!
configure ssid-profile WGB ssid WGB authentication psk 12345678 key-management wpa2
configure dot11Radio 1 mode wgb ssid-profile WGB
configure dot11Radio 1 enable
```

Router

In dit gedeelte wordt uitgelegd hoe NAT kan worden geconfigureerd om connectiviteit tussen de bekabelde clients in vLAN3248 en vLAN3246 mogelijk te maken.

vLAN3248 bevindt zich alleen in de router en heeft helemaal geen connectiviteit met de zijkant van het netwerk dat achter de WLC zit.

De router doet NAT om het verkeer van de bekabelde clients in vLAN3248 naar de zijkant van het netwerk achter de WLC in vLAN3246 te transporteren via de WGB.



Opmerking: voor de bekabelde clients die zijn aangesloten op de router achter de WGB, is de enige ondersteunde configuratie NAT om connectiviteit uit hun vLAN te halen. Inter-vLAN-routering wordt niet ondersteund.

Stap 1. Configureer de vLAN 3246 en vLAN 3248 op laag twee.

```
conf t
vlan 3246
exit
vlan 3248
end
```

Stap 2. Configureer de poort van de WGB vanaf de router.

```
conf t
interface Wlan-GigabitEthernet 0/1/4
switchport trunk native vlan 3246
switchport trunk allowed vlan 3246
switchport mode trunk
```

Stap 3. Configureer de Switched Virtual Interface (SVI) van het WGB vLAN en de bekabelde client vLAN.

Stap 3.1. WGB SVI-configuratie. Het IP-adres 10.10.246.1 is de gateway voor vLAN 3246 die is geconfigureerd in de Layer 3-switch achter de WLC. Deze SVI in de router gebruikt het volgende bruikbare IP-adres.

```
config t
interface Vlan3246
ip address 10.10.246.2 255.255.255.0
```

Stap 3.2. De configuratie van de vLAN-interface van bekabelde clients. Bekabelde clients in de router gebruiken vLAN 3248. Deze SVI is de toegangspoort van de bekabelde clients, omdat deze clients alleen in deze router bestaan. Configureer een uniek MAC-adres voor deze SVI.

```
config t
interface Vlan3248
mac-address 6c13.d53f.aabb
ip address 10.10.248.1 255.255.255.0
```



Waarschuwing: Configureer een uniek MAC-adres per SVI. De router gebruikt standaard hetzelfde MAC-adres voor alle SVI's en dit kan conflicten veroorzaken bij deze implementatie.

Stap 4. Configureer een Access List (ACL) en sta het netwerk van de bekabelde clients toe.

```
config t
ip access-list extended NATACL
10 permit ip 10.10.248.0 0.0.0.255 any
```

Stap 5. Configureer een routekaart die overeenkomt met de ACL en de WGB-interface.

```
conf t
route-map WGBACL permit 10
match ip address NATACL
match interface Vlan3246
```

Stap 6. NAT configureren.

Stap 6.1. NAT configureren in de SVI's. De SVI 3248 is de NAT binnen en 3246 de NAT buiten.

```
config t
interface Vlan3248
ip nat inside
exit
interface Vlan3246
ip nat outside
```

Stap 6.2. Configureer NAT in de router. Gebruik de routekaart als bron. Met deze configuratie kunnen de bekabelde clients op vLAN3248 verbinding maken met het netwerk in vLAN3246 achter de WLC.

```
config t
ip nat inside source route-map WGBACL interface Vlan3246 overload
```

Stap 6.3 Deze stap is optioneel, als er een behoefte is om toegang te krijgen tot de apparaten achter de WGB in vLAN3248 vanaf apparaten achter de WLC in vLAN3246, kan deze worden geconfigureerd via NAT.

De getoonde configuratie laat bijvoorbeeld zien hoe u de toegang voor een apparaat achter de router en WGB met IP-adres 10.10.248.10 via Remote Desktop Protocol (RDP) configureert vanaf apparaten achter de WLC in vLAN3246.

Elke poort kan worden gebruikt die afhankelijk is van wat moet worden benaderd (SSH, Telenet, RDP, HTTP, enzovoort) in het apparaat achter de router in vLAN 3248.

Als u het 10.10.248.10-apparaat via RDP wilt benaderen vanaf een apparaat in vLAN3246, wordt de RDP-verbinding gemaakt met de SVI van het 3246 vLAN in de router (10.10.246.2). Raadpleeg het gedeelte [Verifiëren](#) van dit document.

```
config t
ip nat inside source static tcp 10.10.248.10 3389 interface Vlan3246 3389
```

Stap 7. Configureer de bekabelde clientpoort in vLAN 3248 op de router.

```
config t
interface GigabitEthernet0/1/0
switchport mode access
switchport access vlan 3248
```



Opmerking: deze configuratie maakt gebruik van bekabelde clients in vLAN 3248 met statische IP-adressen. Als DHCP nodig is, kan deze in de router worden geconfigureerd.

Verifiëren

Controleer de verbinding van de WGB en de SVI van de vLAN 3246 die als een bekabelde client wordt vermeld. Bevestig ook de connectiviteit van de bekabelde clients op vLAN 3248 met het netwerk en stuur een ping naar de gateway van vLAN 3246 die achter de WLC bestaat.

Draadloze LAN-controller

Controleer vanuit de WLC of de WGB en de SVI van de vLAN 3246 die in de router zijn geconfigureerd, worden weergegeven in de lijst met draadloze clients.

GUI:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

×

 Delete

Selected 0 out of 2 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State
☐	6c13.d53f.f8f4	10.10.246.2	N/A	C9124AXI-B	1	WGB	6	WLAN (WGB Wired)	Run
☐	e462.c49f.790f	10.10.246.4	fe80::af5a:a617:9ed7:edbe	C9124AXI-B	1	WGB	6	WLAN (WGB)	Run

1 50 1 - 2 of 2 clients

WGB- en WGB-client

CLI:

<#root>

9800L#

show wireless client summary

Number of Clients: 2

MAC Address	AP Name	Type	ID	State	Protocol	Method	Role
6c13.d53f.f8f4	C9124AXI-B	WLAN	6	Run	11ac	None	Local
e462.c49f.790f	C9124AXI-B	WLAN	6	Run	11ac	None	Local

9800L#

show wireless client summary detail

Number of Clients: 2

MAC Address	SSID	AP Name	State	IP Address	VLAN	BSSID	Auth Method	Protocol	Channel
6c13.d53f.f8f4	WGB	C9124AXI-B	Run	10.10.246.2	3246	5c64.f171.6eae	[PSK]	11ac	36
e462.c49f.790f	WGB	C9124AXI-B	Run	10.10.246.4	3246	5c64.f171.6eae	[PSK]	11ac	36

9800L#

show wireless wgb summary

Number of WGBs: 1

MAC Address	AP Name	WLAN	State	Clients
e462.c49f.790f	C9124AXI-B	6	Run	1

Werkgroepbrug

Bevestig dat de WGB-shows zijn verbonden met de SSID.

<#root>

WGB#

show wgb dot11 associations

```

Uplink Radio ID : 1
Uplink Radio MAC : E4:62:C4:9F:79:0F
SSID Name : WGB
Connected Duration : 0 hours, 7 minutes, 9 seconds
Parent AP Name : C9124AXI-B
Parent AP MAC : 5C:64:F1:71:6E:AE
Uplink State : CONNECTED
Auth Type : PSK
Key management Type : WPA2
Dot11 type : 11ac
Channel : 36
Bandwidth : 20 MHz
Current Datarate : 104 Mbps
Max Datarate : 286 Mbps
RSSI : 41
IP : 10.10.246.4/24
Default Gateway : 10.10.246.1
IPV6 : ::/128
Assoc timeout : 5000 Msec
Auth timeout : 5000 Msec
Dhcp timeout : 60 Sec
Country-code : US

```

Bevestig de SVI van de vLAN 3246-shows in de WGB-brugtabel.

<#root>

WGB#

show wgb bridge

```

***Client ip table entries***
mac vap port vlan_id seen_ip confirm_ago fast_brg
6C:13:D5:3F:F8:F4 0 wired0 0 10.10.246.2 28.112000 true
5C:64:F1:71:6E:AF 0 wbridge1 0 0.0.0.0 1064.320000 true

```

Router

Van de router bevestigen dat het bereikbaar is van vLAN3248 naar het netwerk achter de WLC in vLAN3246 en het is succesvol.

<#root>

Router#

```
ping 10.10.246.1 source vlan 3248
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.246.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.248.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms

Bevestig dat NAT-vertalingen correct worden weergegeven.

<#root>

Router#

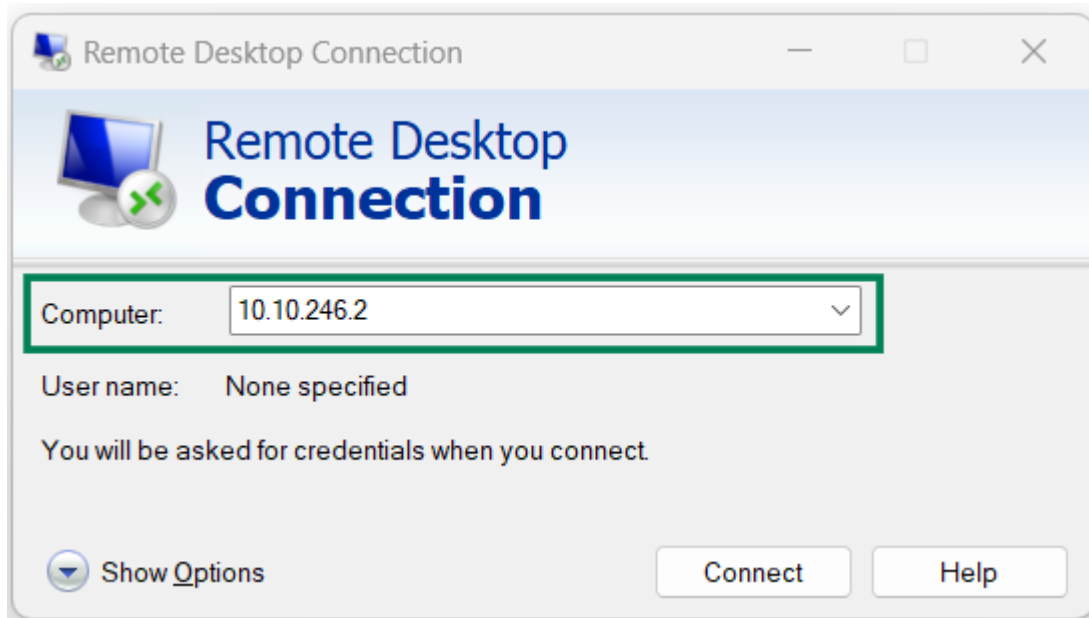
```
show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global
icmp 10.10.246.2:12 10.10.248.1:12 10.10.246.1:12 10.10.246.1:12
Total number of translations: 1
```

Als de optionele configuratiestap van NAT wordt gebruikt, controleert u of de RDP-connectiviteit van vLAN3246 naar een apparaat in vLAN3248 succesvol is.

RDP wordt gebruikt in het voorbeeld van dit document, maar elk ander protocol kan worden gebruikt.

Gebruik de SVI van de vLAN3246 die is geconfigureerd in de router die 10.10.246.2 is om het RDP-apparaat 10.10.248.10 achter de router in vLAN3248 te gebruiken.



RDP-apparaat op afstand

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.