

Configuración de clientes con cables de puente de grupo de trabajo (WGB) con NAT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Configurar](#)

[Controlador de LAN inalámbrica](#)

[Bridge del Grupo de Trabajo](#)

[Router](#)

[Controlador de LAN inalámbrica](#)

[Bridge del Grupo de Trabajo](#)

[Router](#)

Introducción

Este documento describe la configuración de los clientes conectados por cable detrás de Network Access Translation para acceder a la red a través de Workgroup Bridge.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conceptos y configuración del controlador de LAN inalámbrica (WLC) 9800
- Conceptos y configuración de Workgroup Bridge (WGB)
- Conceptos y configuración de Network Access Control (NAT)
- Conceptos y configuración de switching

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 9800-CL WLC Cisco IOS® XE 26.1.1
- WGB WP-WIFI6-B integrado en el router 1821 versión 26.1.1
- Router robusto Catalyst IR1821, Cisco IOS 17.15.4
- Switch 9300, Cisco IOS 17.15.4

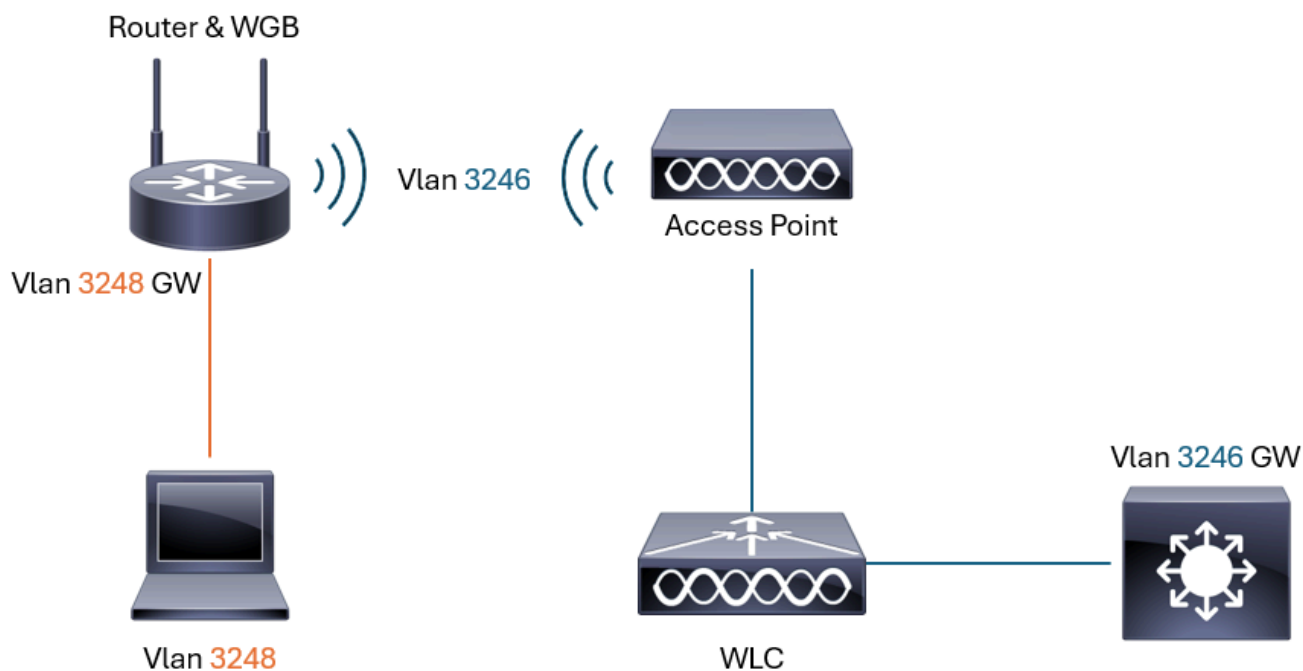
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Hay implementaciones de WGB que requieren que los clientes cableados detrás del WGB estén en un vLAN diferente que el WGB y al mismo tiempo que el vLAN no existe en el WGB, WLC o en los dispositivos de red detrás del WLC.

En este escenario, el uso de NAT proporciona la configuración y la flexibilidad necesarias para hacer que los clientes cableados se comuniquen con la red (aplicaciones, Internet, servidores, etc.) detrás del WLC.

Diagrama de la red



Topología

Configurar

Controlador de LAN inalámbrica

Esta sección explica la configuración básica de WLAN, el perfil de política WLAN y la etiqueta de política para difundir el identificador de conjunto de servicios (SSID) al que se conecta el WGB.



Precaución: Cualquier cambio de configuración en estos parámetros en producción puede provocar la desconexión de un cliente inalámbrico.

Paso 1. Configure el SSID.

Paso 1.1. Vaya a Configuration > Tags & Profiles > WLANs. Haga clic en Add (Agregar). Introduzca el nombre del perfil y del SSID. Haga clic en Apply (Aplicar).

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

Configuración De Wlan

CLI:

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

Paso 1.2. Configure los parámetros de seguridad SSID. Elija PSK, ingrese la contraseña PSK y haga clic en Apply.

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

Seguridad Wlan

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

```

Paso 1.3. Configure AironetIE en el SSID. Navegue hasta la pestaña Advanced, habilite CCX

Aironet IE y haga clic en Apply.

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☐

Max Client Connections

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☐

Per WLAN

n

Cancel

Update & Apply to Device

Aironet IE

CLI:

<#root>

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

Paso 2. Configure el perfil de política WLAN.

Paso 2.1. Vaya a Configuration > Tags & Profiles > WLANs. Haga clic en Add (Agregar). Introduzca un nombre. Configure como Enable the Status y Passive Client. A continuación, haga clic en Aplicar.

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 buttons for '+ Add', 'Delete', and 'Clone'. The dialog title is 'Add Policy Profile'. A warning message states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'General' tab is selected, showing fields for Name* (PolicyWGB), Description (Enter Description), Status (ENABLED), and Passive Client (ENABLED). Below these are IP MAC Binding (ENABLED) and Encrypted Traffic Analytics (DISABLED). The 'WLAN Switching Policy' section includes Central Switching (ENABLED), Central Authentication (ENABLED), Central DHCP (ENABLED), and Flex NAT/PAT (DISABLED). The 'CTS Policy' section includes Inline Tagging (unchecked), SGACL Enforcement (unchecked), and Default SGT (2-65519). At the bottom are 'Cancel' and 'Apply to Device' buttons.

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

CTS Policy

Inline Tagging ☐

SGACL Enforcement ☐

Default SGT 2-65519

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Cancel Apply to Device

Política WLAN

CLI:

<#root>

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

Paso 2.2. Vaya a Políticas de acceso. Haga clic en VLAN/VLAN Group y elija el 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

Configuración De Vlan

CLI:

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

Paso 3. Configure la etiqueta de política y aplíquela a los puntos de acceso (AP) a los que se conecta el WGB.

Paso 3.1. Vaya a Configuración > Etiquetas y perfiles > Etiquetas. Haga clic en Directiva y, a continuación, en Agregar. Introduzca un nombre y haga clic en Agregar. Elija el SSID y el perfil de política. Haga clic en Apply (Aplicar).

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 50 items per page 1 - 1 of 1 Items

Map WLAN and Policy

Cancel Apply to Device

Etiqueta

CLI:

```
<#root>
```

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



Nota: Recuerde aplicar la etiqueta de directiva a todos los puntos de acceso que difundan el SSID.

Bridge del Grupo de Trabajo

Esta sección explica la configuración en el WGB. La configuración permite al WGB conectarse a la red y obtener conectividad a través de 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

Esta sección explica cómo configurar NAT para permitir la conectividad entre los clientes cableados en vLAN3248 al vLAN3246.

vLAN3248 reside solamente en el router y no tiene ninguna conectividad al lado de la red que está detrás del WLC.

El router hace NAT para transportar el tráfico de los clientes cableados en vLAN3248 al lado de la red detrás del WLC en vLAN3246 a través del WGB.



Nota: Para los clientes cableados conectados al router detrás del WGB, para tener conectividad fuera de su vLAN, la única configuración soportada es NAT. No se admite el enrutamiento Inter-vLAN.

Paso 1. Configure vLAN 3246 y vLAN 3248 en un nivel de capa dos.

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

Paso 2. Configure el puerto del WGB desde el router.

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

Paso 3. Configuración de la interfaz virtual conmutada (SVI) de WGB vLAN y la vLAN del cliente por cable.

Paso 3.1. Configuración de WGB SVI. La dirección IP 10.10.246.1 es la gateway para vLAN 3246 configurada en el switch de Capa 3 detrás del WLC. Esta SVI del router está utilizando la siguiente dirección IP utilizable.

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

Paso 3.2. Configuración de vLAN de interfaz de clientes con cable. Los clientes con cables del router utilizan vLAN 3248. Esta SVI es la gateway de los clientes con cable, ya que estos clientes sólo existen en este router. Configure una dirección MAC única para esta SVI.

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



Precaución: Configure una dirección MAC única por SVI. De forma predeterminada, el router utiliza la misma dirección MAC para todas las SVI y esto puede crear conflictos en esta implementación.

Paso 4. Configure una lista de acceso (ACL) y permita la red de los clientes conectados por cable.

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

Paso 5. Configure un route-map que coincida con la ACL y la interfaz WGB.

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

Paso 6. Configuración de NAT.

Paso 6.1. Configuración de NAT en las SVI. El SVI 3248 es el NAT interno y el 3246 es el NAT externo.

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

Paso 6.2. Configuración de NAT en el router. Utilice el route-map como origen. Esta configuración permite que los clientes cableados en vLAN3248 tengan conectividad con la red en vLAN3246 detrás del WLC.

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

Paso 6.3 Este paso es opcional, si hay una necesidad de acceder a los dispositivos detrás del WGB en vLAN3248 desde los dispositivos detrás del WLC en vLAN3246 se puede configurar vía NAT.

Como ejemplo, la configuración mostrada muestra cómo configurar el acceso para un dispositivo detrás del router y WGB con la dirección IP 10.10.248.10 a través del protocolo de escritorio remoto (RDP) desde los dispositivos detrás del WLC en vLAN3246.

Se puede utilizar cualquier puerto que dependa de lo que se necesite acceder (SSH, Telenet, RDP, HTTP, etc.) en el dispositivo detrás del router en vLAN 3248.

Para acceder al dispositivo 10.10.248.10 a través de RDP desde un dispositivo en vLAN3246, la conexión RDP se realiza al SVI del 3246 vLAN en el router (10.10.246.2), verifique la sección [Verificar](#) de este documento.

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

Paso 7. Configure el puerto de cliente con cable en vLAN 3248 en el router.

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



Nota: Esta configuración utiliza clientes por cable en vLAN 3248 con direcciones IP estáticas. Si se necesita DHCP, se puede configurar en el router.

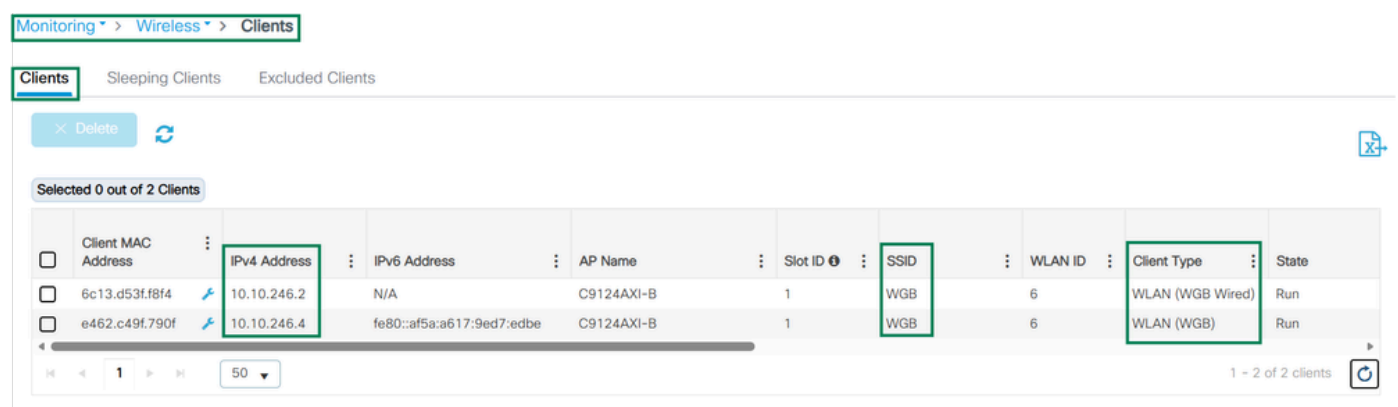
Verificación

Verifique la conexión del WGB y la SVI del vLAN 3246 que aparece como cliente con cable. También, confirme la conectividad de los clientes cableados en vLAN 3248 a la red, envíe un ping al gateway de vLAN 3246 que existe detrás del WLC.

Controlador de LAN inalámbrica

Verifique desde el WLC que el WGB y el SVI del vLAN 3246 configurado en el router se muestran en la lista de clientes inalámbricos.

GUI:



Cliente WGB y WGB

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

Bridge del Grupo de Trabajo

Confirme que el WGB se muestra conectado al 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

```

Confirme la SVI de los programas vLAN 3246 en la tabla de puente WGB.

<#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

Desde el router, confirme que es accesible desde vLAN3248 a la red detrás del WLC en vLAN3246 y que es exitoso.

<#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

Confirme que las traducciones NAT se muestran correctamente.

<#root>

Router#

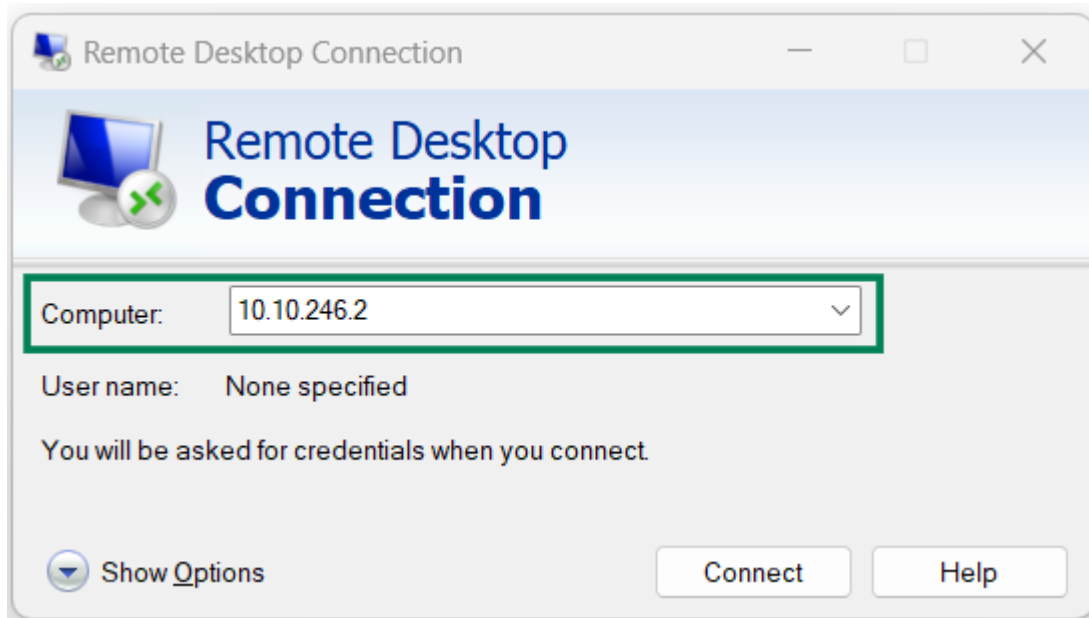
show ip nat translations

```
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
```

Si se utiliza el paso de configuración opcional de NAT, confirme que la conectividad RDP de vLAN3246 a un dispositivo en vLAN3248 es correcta.

RDP se utiliza en el ejemplo de este documento, sin embargo, se puede utilizar cualquier otro protocolo.

Utilice el SVI del vLAN3246 configurado en el router que es 10.10.246.2 para RDP el dispositivo 10.10.248.10 detrás del router en vLAN3248.



Dispositivo remoto RDP

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).