

NAT로 WGB(Workgroup Bridge) 유선 클라이언트 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[무선 LAN 컨트롤러](#)

[워크그룹 브리지](#)

[라우터](#)

[무선 LAN 컨트롤러](#)

[워크그룹 브리지](#)

[라우터](#)

소개

이 문서에서는 Workgroup Bridge를 통해 네트워크에 액세스하기 위해 Network Access Translation을 지원하는 유선 클라이언트의 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- 9800 WLC(Wireless Lan Controller) 개념 및 컨피그레이션
- WGB(Workgroup Bridge) 개념 및 구성
- NAT(Network Access Control) 개념 및 컨피그레이션
- 스위칭 개념 및 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-CL WLC Cisco IOS® XE 26.1.1
- 1821 라우터 버전 26.1.1에 통합된 WGB WP-WIFI6-B
- Catalyst IR1821 Rugged Router, Cisco IOS 17.15.4
- 9300 스위치, Cisco IOS 17.15.4

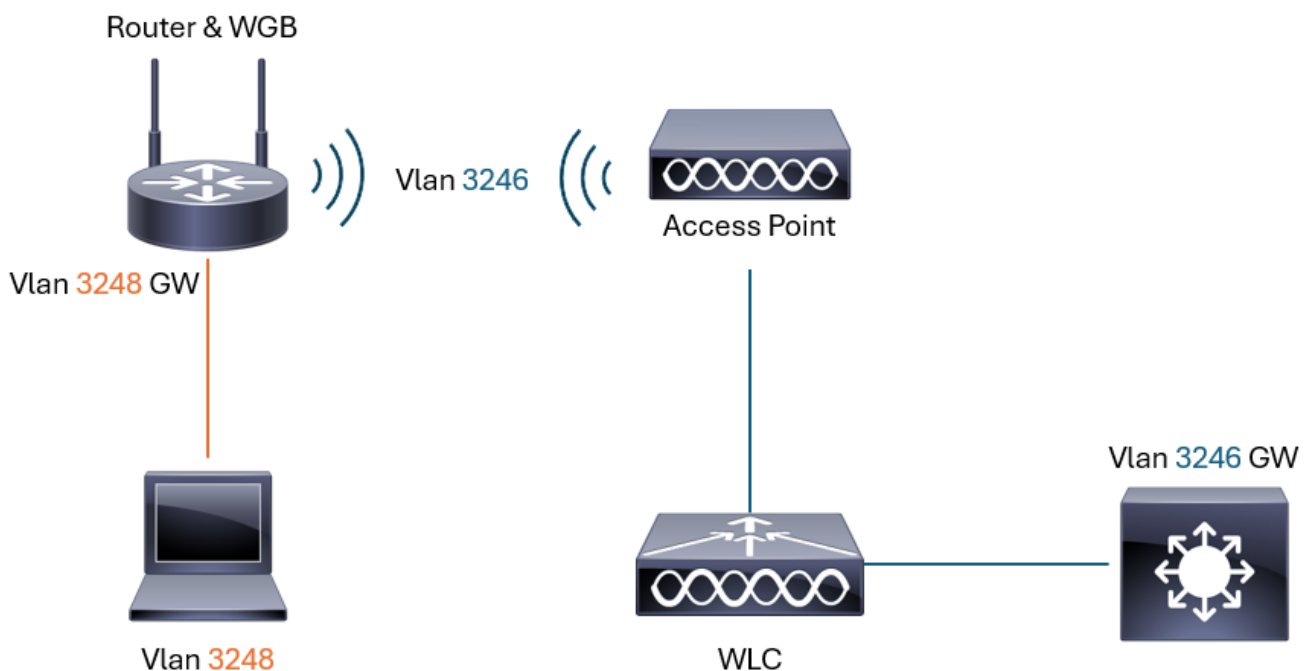
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

WGB 뒤에 있는 유선 클라이언트가 WGB와 다른 vLAN에 있어야 하는 동시에 vLAN이 WGB, WLC 또는 WLC 뒤에 있는 네트워크 장치에 존재하지 않아야 하는 WGB 구현이 있습니다.

이 시나리오에서 NAT를 사용하면 유선 클라이언트가 WLC 뒤의 네트워크(애플리케이션, 인터넷, 서버 등)와 통신할 수 있는 데 필요한 컨피그레이션 및 유연성을 제공합니다.

네트워크 다이어그램



구성

무선 LAN 컨트롤러

이 섹션에서는 WGB가 연결되는 SSID(Service Set Identifier)를 브로드캐스트하기 위한 WLAN, WLAN-Policy Profile 및 Policy Tag의 기본 컨피그레이션에 대해 설명합니다.



주의: 프로덕션에서 이러한 매개변수의 컨피그레이션을 변경하면 무선 클라이언트 연결이 끊어질 수 있습니다.

1단계. SSID를 구성합니다.

1.1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > WLANs(WLAN)로 이동합니다. Add(추가)를 클릭합니다. 프로파일 및 SSID 이름을 입력합니다. 적용을 클릭합니다.

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 컨피그레이션

CLI:

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

1.2단계. SSID 보안 매개변수를 구성합니다. PSK를 선택하고 PSK 비밀번호를 입력한 다음 Apply(적용)를 클릭합니다.

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 보안

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

```

1.3단계. SSID에서 AironetIE를 구성합니다. Advanced(고급) 탭으로 이동하여 CCX Aironet IE를 활

성화하고 Apply(적용)를 클릭합니다.

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
```

2단계. WLAN-Policy 프로필을 구성합니다.

2.1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동합니다. Add(추가)를 클릭합니다. 이름을 입력합니다. Enable the Status and Passive Client로 구성합니다. 그런 다음 Apply를 클릭합니다.

GUI:

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

WLAN 정책

CLI:

<#root>

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

2.2단계. Access Policies(액세스 정책)로 이동합니다. VLAN/VLAN Group(VLAN/VLAN 그룹)을 클릭하고 WGB vLAN을 선택합니다.

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 Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

VLAN3246 × ⓘ

Multicast VLAN

Enter 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 ACL

Search or Select ▼ ⓘ

IPv6 ACL

Search or Select ▼ ⓘ

URL Filters ⓘ

Pre Auth

Search or Select ▼ ⓘ

Post Auth

Search or Select ▼ ⓘ

↶ Cancel

📄 Update & Apply to Device

Vlan 컨피그레이션

CLI:

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

3단계. 정책 태그를 구성하고 WGB가 연결되는 액세스 포인트(AP)에 적용합니다.

3.1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그)로 이동합니다. Policy(정책)를 클릭한 다음 Add(추가)를 클릭합니다. Name(이름)을 입력한 다음 Add(추가)를 클릭합니다. SSID 및 정책 프로파일을 선택합니다. 적용을 클릭합니다.

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

태그

CLI:

<#root>

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



참고: SSID를 브로드캐스트하는 모든 액세스 포인트에 정책 태그에 적용해야 합니다.

워크그룹 브리지

이 섹션에서는 WGB의 컨피그레이션에 대해 설명합니다. 이 컨피그레이션을 통해 WGB를 네트워크에 연결하고 vLAN3246을 통해 연결할 수 있습니다.

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
```

라우터

이 섹션에서는 vLAN3248의 유선 클라이언트와 vLAN3246 간의 연결을 허용하도록 NAT를 구성하는 방법에 대해 설명합니다.

vLAN3248은 라우터에만 상주하며 WLC 뒤에 있는 네트워크 측면에 전혀 연결되지 않습니다.

라우터는 vLAN3248의 유선 클라이언트 트래픽을 WGB를 통해 vLAN3246의 WLC 뒤의 네트워크 측면으로 전송하도록 NAT를 수행합니다.



참고: WGB 뒤에 있는 라우터에 연결된 유선 클라이언트의 경우 vLAN에서 연결을 유지하기 위해 지원되는 컨피그레이션은 NAT뿐입니다. vLAN 간 라우팅은 지원되지 않습니다.

1단계. 레이어 2 레벨에서 vLAN 3246 및 vLAN 3248을 구성합니다.

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

2단계. 라우터에서 WGB의 포트를 구성합니다.

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

3단계. WGB vLAN 및 유선 클라이언트 vLAN의 SVI(Switched Virtual Interface)를 구성합니다.

3.1단계. WGB SVI 컨피그레이션 IP 주소 10.10.246.1은 WLC 뒤의 레이어 3 스위치에 구성된 vLAN 3246용 게이트웨이입니다. 라우터의 이 SVI는 사용 가능한 다음 IP 주소를 사용합니다.

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

3.2단계. 유선 클라이언트는 vLAN 구성을 인터페이스합니다. 라우터의 유선 클라이언트는 vLAN 3248을 사용합니다. 이 클라이언트는 이 라우터에만 있으므로 이 SVI는 유선 클라이언트의 게이트웨이입니다. 이 SVI에 대해 고유한 MAC 주소를 구성합니다.

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



주의: SVI별로 고유한 MAC 주소를 구성합니다. 기본적으로 라우터는 모든 SVI에 대해 동일한 MAC 주소를 사용하므로 이 구현에서 충돌이 발생할 수 있습니다.

4단계. ACL(Access List)을 구성하고 유선 클라이언트의 네트워크를 허용합니다.

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

5단계. ACL 및 WGB 인터페이스와 일치하는 경로 맵을 구성합니다.

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

6단계. NAT 구성

6.1단계. SVI에서 NAT를 구성합니다. SVI 3248은 내부 NAT이고 3246은 외부 NAT입니다.

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

6.2단계. 라우터에 NAT를 구성합니다. route-map을 소스로 사용합니다. 이 컨피그레이션을 사용하면 vLAN3248의 유선 클라이언트가 WLC 뒤에 있는 vLAN3246의 네트워크와 연결할 수 있습니다.

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

6.3단계 이 단계는 선택 사항이며, vLAN3246의 WLC 뒤에 있는 디바이스에서 vLAN3248의 WGB 뒤에 있는 디바이스에 액세스해야 하는 경우 NAT를 통해 구성할 수 있습니다.

예를 들어, 표시된 컨피그레이션에서는 vLAN3246의 WLC 뒤에 있는 디바이스에서 RDP(Remote Desktop Protocol)를 통해 IP 주소 10.10.248.10을 사용하여 라우터 뒤에 있는 디바이스 및 WGB에 대한 액세스를 구성하는 방법을 보여줍니다.

vLAN 3248의 라우터 뒤에 있는 디바이스에서 액세스해야 하는 항목(SSH, Telenet, RDP, HTTP 등)에 따라 달라지는 모든 포트를 사용할 수 있습니다.

vLAN3246의 디바이스에서 RDP를 통해 10.10.248.10 디바이스에 액세스하려면 라우터 (10.10.246.2)에 있는 3246 vLAN의 SVI에 RDP 연결이 설정되어 있어야 합니다. 이 문서의 [Verify\(확인\)](#) 섹션을 확인하십시오.

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

7단계. 라우터의 vLAN 3248에 유선 클라이언트 포트를 구성합니다.

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



참고: 이 컨피그레이션에서는 고정 IP 주소가 있는 vLAN 3248의 유선 클라이언트를 사용합니다. DHCP가 필요한 경우 라우터에서 구성할 수 있습니다.

다음을 확인합니다.

유선 클라이언트로 나열된 vLAN 3246의 WGB와 SVI의 연결을 확인합니다. 또한 vLAN 3248의 유선 클라이언트가 네트워크에 연결되어 있는지 확인하고 WLC 뒤에 있는 vLAN 3246 게이트웨이로 ping을 보냅니다.

무선 LAN 컨트롤러

WLC에서 라우터에 구성된 vLAN 3246의 WGB 및 SVI가 무선 클라이언트 목록에 표시되는지 확인합니다.

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 및 WGB 클라이언트

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

워크그룹 브리지

WGB가 SSID에 연결된 것으로 표시되는지 확인합니다.

```
<#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
```

WGB 브리지 테이블에 표시된 vLAN 3246의 SVI를 확인합니다.

```
<#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
```

라우터

라우터에서 vLAN3248에서 vLAN3246의 WLC 뒤에 있는 네트워크로 연결할 수 있으며 성공적인지 확인합니다.

<#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

NAT 변환이 올바르게 표시되는지 확인합니다.

<#root>

Router#

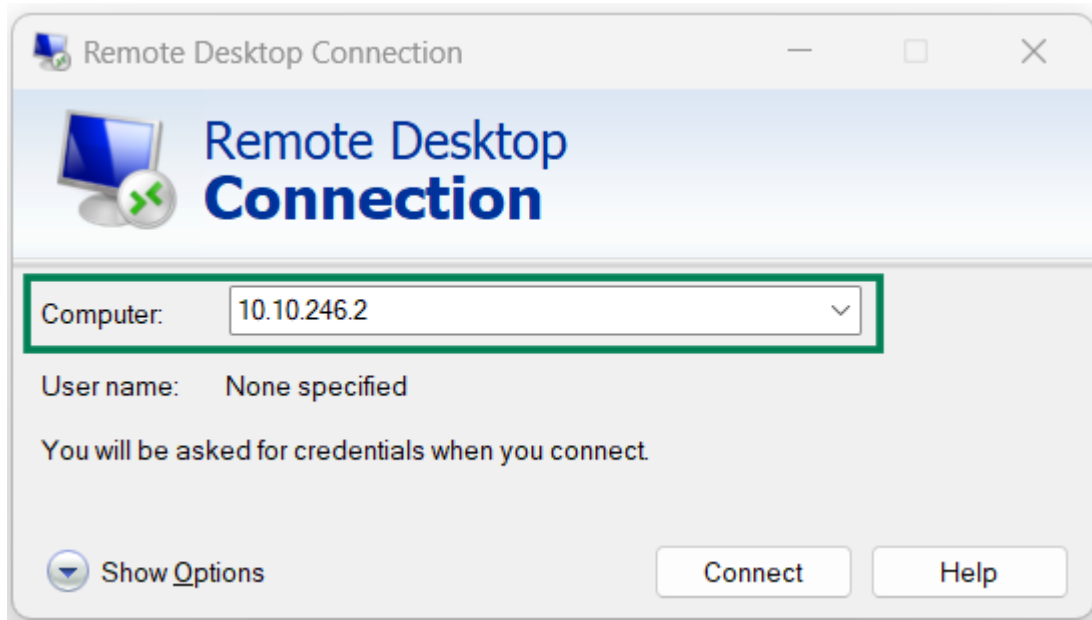
show ip nat translations

```
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
```

NAT의 선택적 컨피그레이션 단계를 사용하는 경우 vLAN3246에서 vLAN3248의 디바이스로 RDP 연결이 성공하는지 확인합니다.

RDP는 이 문서의 예에서 사용되지만 다른 프로토콜을 사용할 수 있습니다.

10.10.246.2인 라우터에 구성된 vLAN3246의 SVI를 사용하여 vLAN3248의 라우터 뒤에 있는 10.10.248.10에서 RDP를 수행합니다.



RDP 원격 디바이스

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.