

# Verwenden Sie NAT, um die tatsächliche IP-Adresse des CTC auszublenden, um eine Sitzung mit der ONS 15454 einzurichten.

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Topologie](#)

[Konfiguration](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[Konfiguration von Cisco ONS 15454](#)

[PC-Konfiguration](#)

[Routerkonfiguration](#)

[Überprüfung](#)

[Überprüfungsverfahren](#)

[Fehlerbehebung](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Network Address Translation (NAT), um eine Sitzung zwischen dem Cisco Transport Controller (CTC) und ONS 15454 einzurichten. Bei der Konfiguration wird die tatsächliche IP-Adresse des CTC über NAT ausgeblendet, wenn der CTC in der Firewall ansässig ist.

**Hinweis:** Damit dieses Verfahren funktioniert, müssen Sie sicherstellen, dass die Ports nicht blockiert oder gefiltert werden.

## Voraussetzungen

### Anforderungen

Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass Sie über die folgenden Themen verfügen:

- Cisco ONS 15454
- Cisco Router mit NAT-Unterstützung

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ONS 15454 Version 5.0 und höher
- Cisco IOS® Softwareversion 12.1(11) und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps von Cisco zu Konventionen).

## Hintergrundinformationen

### Topologie

Die Topologie besteht aus den folgenden Elementen:

- Ein Cisco ONS 15454
- Ein PC
- Zwei Cisco Router der Serie 2600

Die Cisco ONS 15454 ist im externen Netzwerk installiert und fungiert als Server. Der PC befindet sich im internen Netzwerk und dient als CTC-Client.

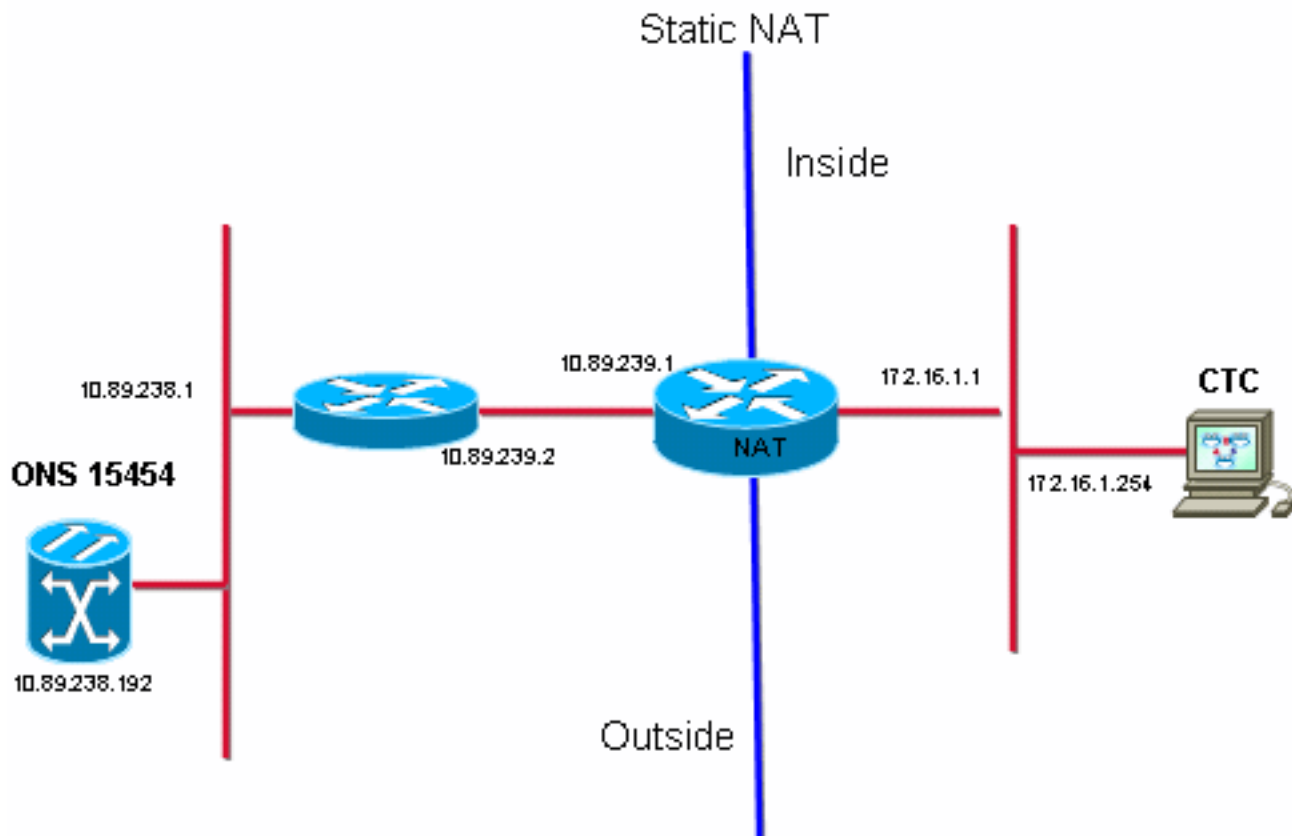
## Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

**Hinweis:** Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfigurationen

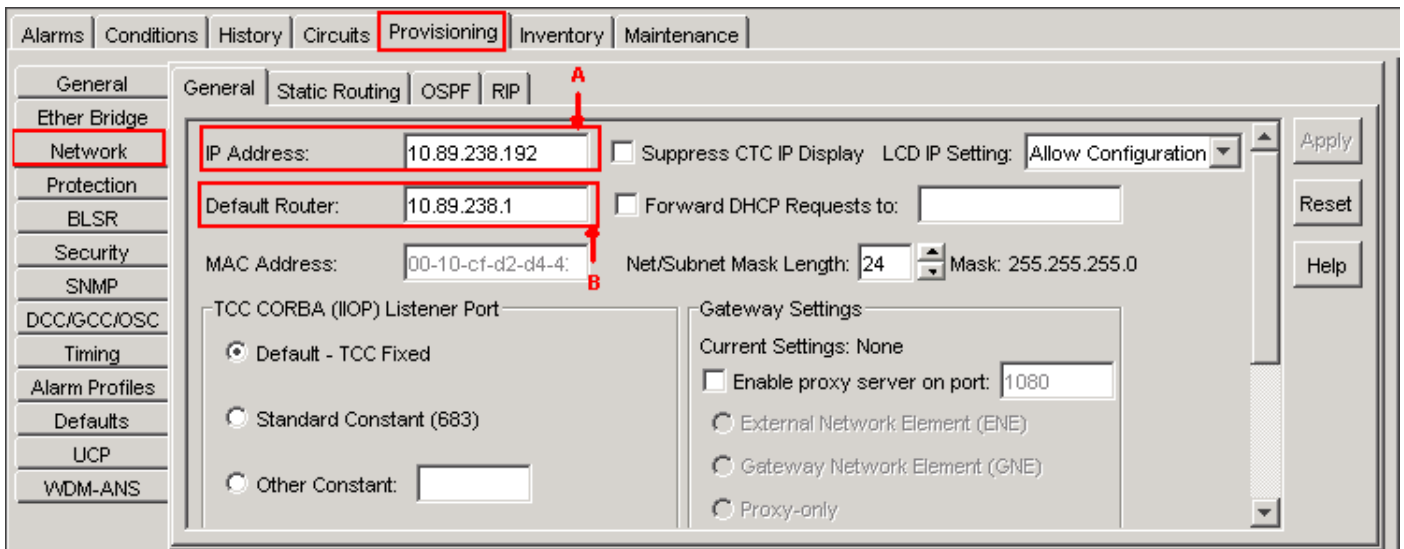
In diesem Dokument werden folgende Konfigurationen verwendet:

- Cisco ONS 15454
- PC
- Cisco Router der Serie 2600

### Konfiguration von Cisco ONS 15454

10.89.238.192 ist die IP-Adresse des ONS 15454 (siehe Pfeil A in [Abbildung 2](#)), und 10.89.238.1 stellt den Standardrouter dar (siehe Pfeil B in [Abbildung 2](#)).

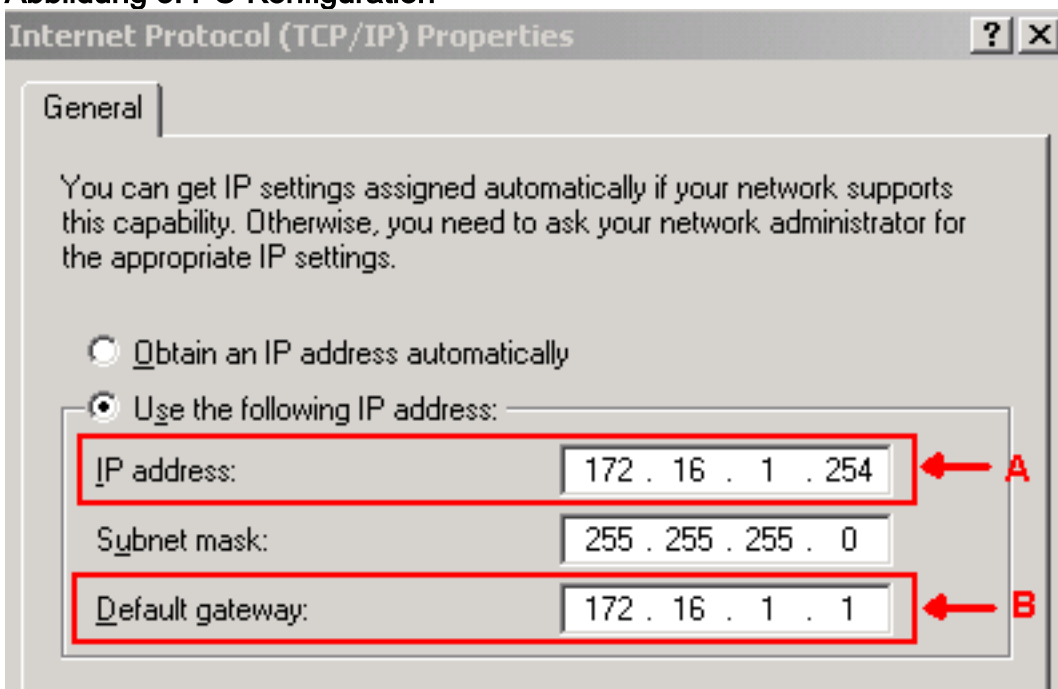
**Abbildung 2: Konfiguration von ONS 15454**



## PC-Konfiguration

172.16.1.254 ist die IP-Adresse des PCs (siehe Pfeil A in [Abbildung 3](#)), und 172.16.1.1 stellt das Standardgateway dar (siehe Pfeil B in [Abbildung 3](#)). NAT übersetzt die IP-Adresse aus Sicherheitsgründen in 10.89.239.100. Der Cisco Router der Serie 2600 bietet die erforderliche Unterstützung für NAT und Routing.

Abbildung 3: PC-Konfiguration



## Routerkonfiguration

Gehen Sie wie folgt vor, um die NAT-Unterstützung auf den Routern zu konfigurieren:

1. Konfigurieren Sie die externe Schnittstelle.

```
!
interface Ethernet1/1
 ip address 10.89.239.1 255.255.255.0
 ip nat outside
!
```

2. Konfigurieren Sie die interne Schnittstelle, auf der sich der PC befindet.

```
interface Ethernet1/2
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
!
```

### 3. Konfigurieren Sie statische NAT.

```
!
 ip nat inside source static 172.16.1.254 10.89.239.100
!
```

Die Konfiguration wandelt die IP-Adresse 172.16.1.254 (innerhalb lokal) (siehe Pfeil B in [Abbildung 4](#)) in 10.89.239.100 (innerhalb global) um (siehe Pfeil A in [Abbildung 4](#)).

### 4. Geben Sie den Befehl `show ip nat translation` auf dem Router ein. **Abbildung 4: IP NAT-Übersetzungen**

```
2600-3#show ip nat translations
Pro Inside global A Inside local B Outside local Outside global
--- 10.89.239.100 ← 172.16.1.254 ← ---
2600-3#
```

## Überprüfung

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

### Überprüfungsverfahren

Führen Sie diese Schritte aus:

1. Führen Sie Microsoft Internet Explorer aus.
2. Geben Sie `http://10.89.238.192` in die Adressleiste des Browserfensters ein, und drücken Sie die EINGABETASTE. Das Fenster CTC-Anmeldung wird angezeigt.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um sich anzumelden. Der CTC-Client muss erfolgreich eine Sitzung mit der ONS 15454 aufbauen.

## Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

### Befehle zur Fehlerbehebung

Einige Befehle des Typs `show` werden vom Tool [Output Interpreter unterstützt \(nur für registrierte Kunden\)](#), mit dem sich [Analysen der Ausgabe von Befehlen des Typs show abrufen lassen](#).

**Hinweis:** Bevor Sie `Debugbefehle` ausgeben, lesen Sie [Wichtige Informationen über Debug-Befehle](#).

- `debug ip nat detail`: Schaltet die detaillierte IP NAT-Verfolgung ein.

Die Ausgabe des Befehls `debug ip nat` gibt die Adressübersetzungen an. NAT übersetzt beispielsweise 172.16.1.254 bis 10.89.239.100, wenn der CTC Daten an ONS 15454 sendet (siehe Pfeil A in [Abbildung 5](#)). Ebenso übersetzt NAT 10.89.239.100 bis 172.16.1.254, wenn der CTC Daten von ONS 15454 empfängt (siehe Pfeil B in [Abbildung 5](#)).

## Abbildung 5: Detailliertes Debuggen der IP NAT

```
2600-4#debug ip nat detailed
IP NAT detailed debugging is on
2600-4#
03:03:15: NAT*: i: tcp (172.16.1.254, 2968) -> (10.89.238.192, 57790) [32790]
03:03:15: NAT*: s=172.16.1.254->10.89.239.100, d=10.89.238.192 [32790]
03:03:15: NAT*: o: tcp (10.89.238.192, 57790) -> (10.89.238.200, 2968) [3135]
03:03:15: NAT*: s=10.89.238.192, d=10.89.239.100->172.16.1.254 [3135]
03:03:15: NAT*: o: tcp (10.89.238.192, 57790) -> 10.89.238.200, 2968) [3136]
03:03:15: NAT*: s=10.89.238.192, d=10.89.239.100->172.16.1.254 [3136]
03:03:15: NAT*: i: tcp (172.16.1.254, 2968) -> (10.89.238.192, 57790) [32791]
03:03:15: NAT*: s=172.16.1.254->10.89.239.100, d=10.89.238.192 [32791]
```

The diagram shows a sequence of NAT debug messages. Two red boxes highlight source IP changes: one for the outgoing packet (s=172.16.1.254->10.89.239.100) and one for the incoming packet (d=10.89.239.100->172.16.1.254). Red arrows labeled 'A' and 'B' point to these changes.

## Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)