

# Использование NAT для сокрытия настоящего IP-адреса ONS15454, чтобы начать сеанс работы с CTC

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Топология](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Конфигурация Cisco ONS 15454](#)

[Конфигурация персонального компьютера](#)

[Настройка маршрутизатора](#)

[Проверка](#)

[Процедура проверки](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## **Введение**

Этот документ предоставляет пример конфигурации для Технологии NAT для установления сеанса между Cisco Transport Controller (CTC) и ONS 15454. Конфигурация использует NAT и список доступа, когда ONS 15454 находится в частной сети, и клиент CTC находится в открытой сети.

Примените NAT и список доступа для целей обеспечения безопасности. NAT скрывает реальный IP - адрес ONS 15454. Список доступа служит межсетевым экраном для управления IP - трафиком в и из ONS 15454.

## **Предварительные условия**

### **Требования**

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются следующие требования:

- Имейте базовые знания о Cisco ONS 15454.
- Знайте, какие маршрутизаторы Cisco поддерживают NAT.

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Релиз 12.1 Программного обеспечения Cisco IOS (11) и позже
- Версия 5. X Cisco ONS 15454 и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Общие сведения

Этот раздел предоставляет существенные общие сведения.

## Топология

Проверка топологии включает:

- Один Cisco ONS 15454, который действует как сервер.
- Один ПК, который служит клиентом СТС.
- Один Маршрутизатор серии Cisco 2600, который оказывает поддержку NAT.

**Примечание:** Cisco ONS 15454 находится во внутренней сети, и ПК находится во внешней сети.

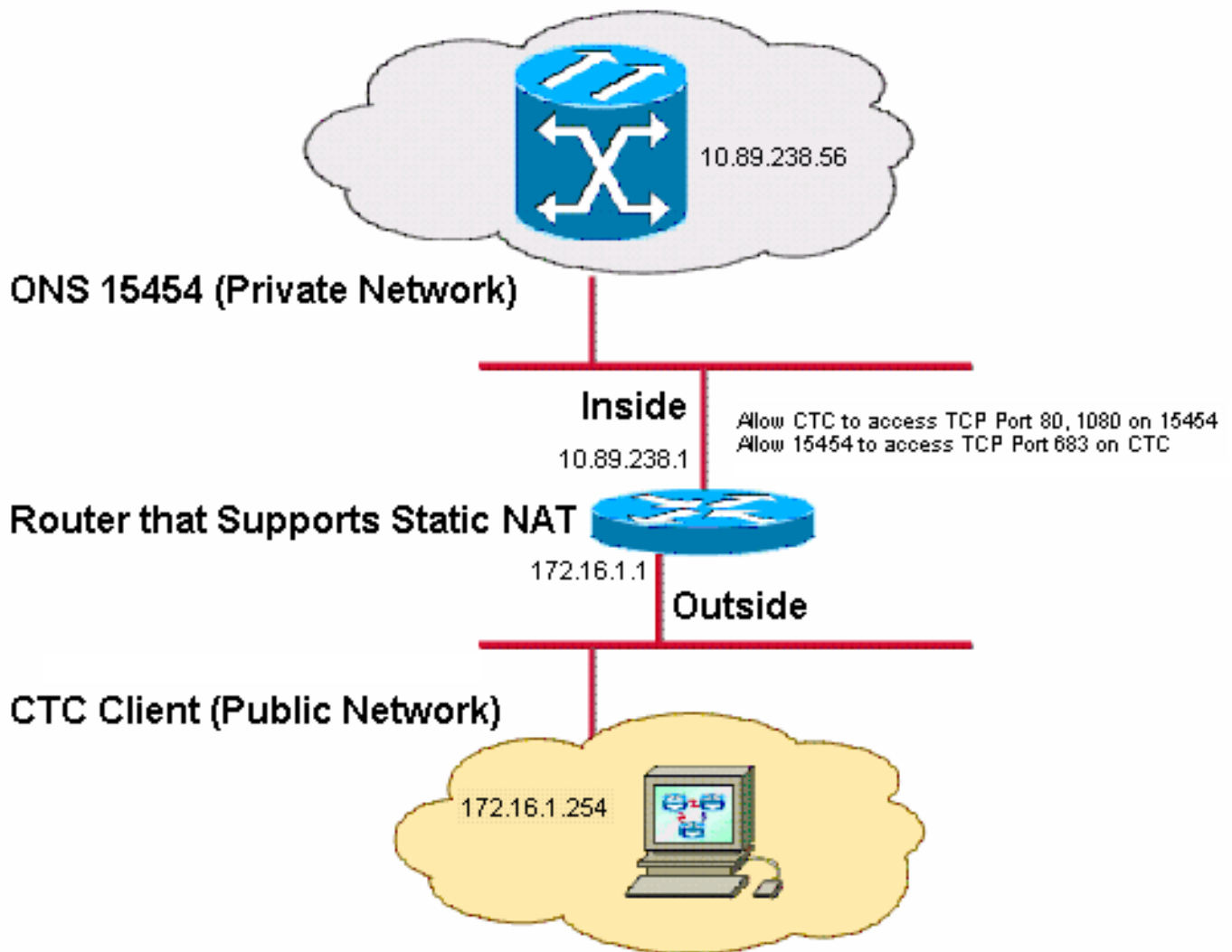
## Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** [Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" \(Поиск команд\) \(только для зарегистрированных клиентов\).](#)

## Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Предположите, что 172.16.0.0 маршрутизуемо в открытой сети.

## Конфигурации

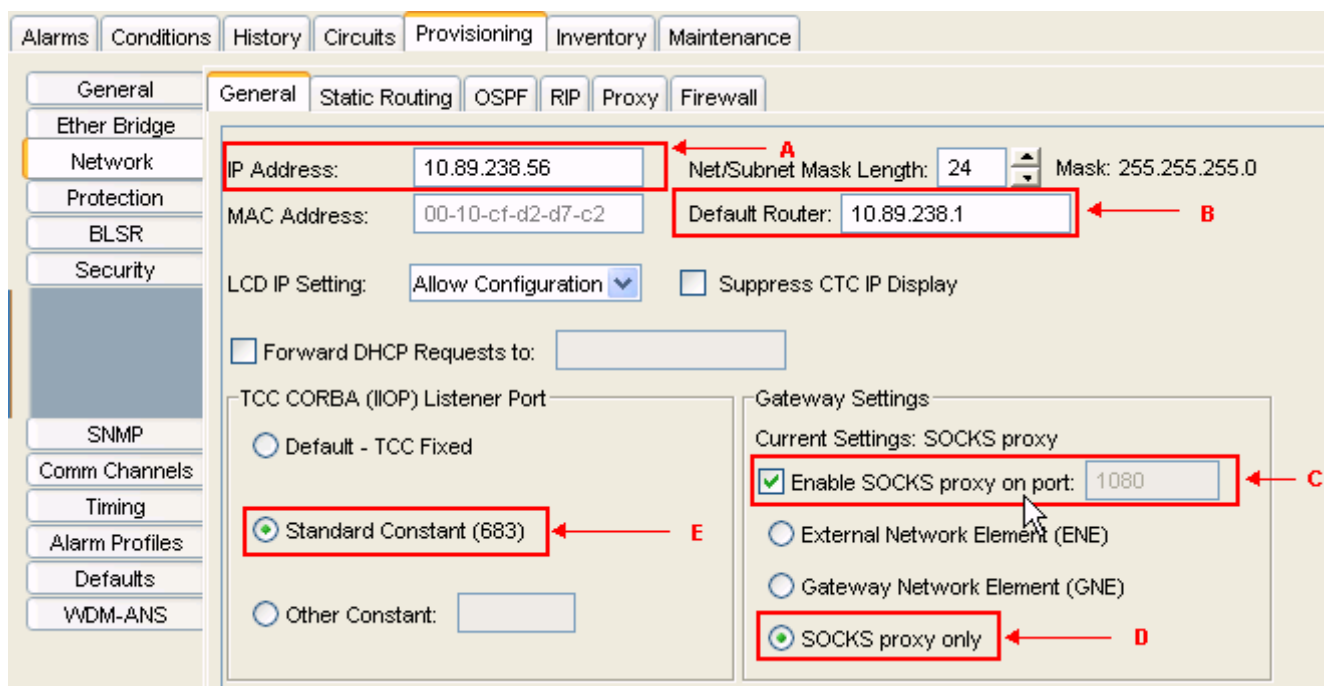
Эти конфигурации используются в данном документе:

- ONS 15454
- ПК
- Маршрутизатор

## Конфигурация Cisco ONS 15454

Выполните следующие действия:

1. В представлении узла нажмите **Provisioning> General> Network**. Проверьте, появляется ли IP-адрес ONS 15454 как 10.89.238.56 в поле IP Address (см. стрелку на [рисунке 2](#)), и что поле Default Router содержит значение 10.89.238.1 (см. стрелку В на [рисунке 2](#)). Рисунок 2 – конфигурация ONS 15454

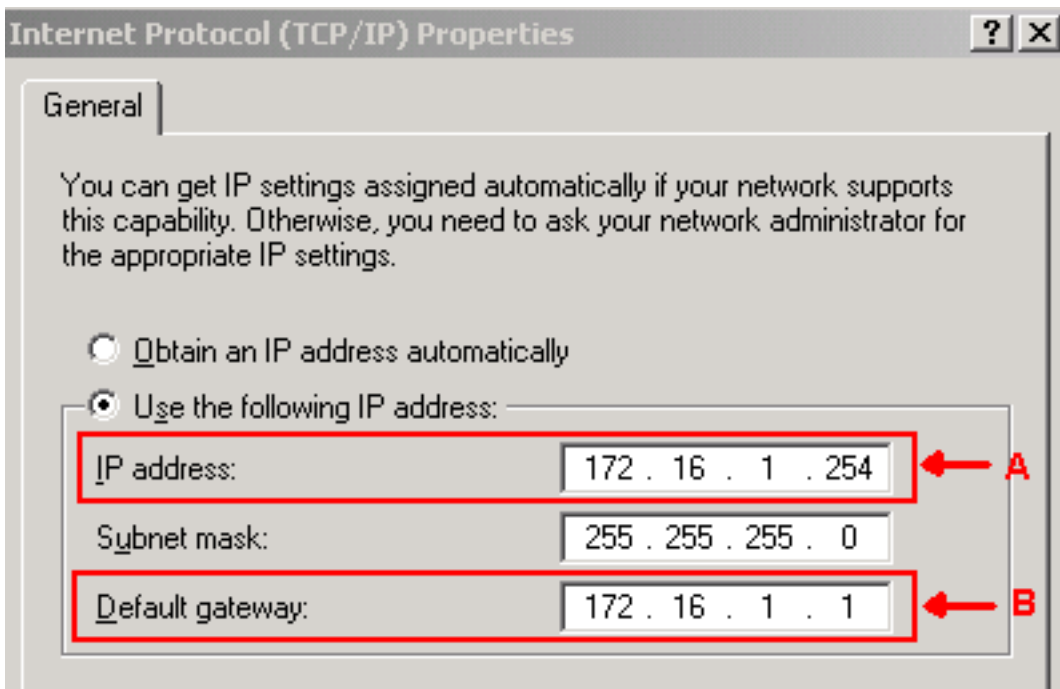


2. Проверьте **Разрешать прокси SOCKS** на флажке порта в разделе Настроек шлюза (см. стрелку C на [рисунке 2](#)), и выберите прокси **SOCKS** только опция (см. стрелку D на [рисунке 2](#)).
3. Выберите требуемую опцию порта прослушивания в CORBA TCC (IOP) раздел Порта прослушивания. У вас есть эти три опции: **По умолчанию - Неподвижный TCC** — Выбирает эту опцию, если ONS 15454 находится на той же стороне межсетевого экрана как компьютер CTC, или если нет никакого межсетевого экрана (по умолчанию). Эта опция устанавливает порт прослушивания ONS 15454 в порт 57790. Если порт 57790 открыт, можно использовать опцию Default - TCC Fixed для доступа через межсетевой экран. **Стандартная константа** — Выбирает эту опцию для использования порта 683, номер порта по умолчанию CORBA, как порт прослушивания ONS 15454. Данный пример использует Стандартную константу (683) (см. стрелку E на [рисунке 2](#)). Если вы не используете порт 683, **другая Константа** — Выбирает эту опцию. Введите порт IOP, который задает ваш администратор межсетевого экрана.

## [Конфигурация персонального компьютера](#)

В Протоколе Интернета (TCP/IP) Диалоговое окно со свойствами проверьте, указывает ли поле IP address 172.16.1.254 как IP-адрес ПК (см. стрелку на [рисунке 3](#)). Также проверьте, является ли 172.16.1.1 шлюзом по умолчанию (см. стрелку B на [рисунке 3](#)).

**Рисунок 3 – конфигурация ПК**



## Настройка маршрутизатора

Выполните следующие действия:

1. Настройте внутренний интерфейс, где находится Cisco ONS 15454.!

```
interface Ethernet1/0
 ip address 10.89.238.1 255.255.255.0
 ip access-group 101 in
 ip nat inside
!
```

2. Настройте список доступа 101.access-list 101 permit tcp any eq www any

```
!
! Allow CTC to access TCP Port 80 on ONS 15454
!
access-list 101 permit tcp any eq 1080 any
!
! Allow CTC to access TCP Port 1080 on ONS 15454
!
access-list 101 permit tcp any any eq 683
!
! Allow ONS 15454 to access TCP Port 683 on the PC
!
```

3. Настройте внешний интерфейс, где находится ПК.interface Ethernet1/1

```
ip address 172.16.1.1 255.255.255.0
ip nat outside
!
```

4. Настройте статический NAT.Конфигурация преобразовывает IP-адрес 10.89.238.56 (внутри локальный) к IP-адресу 172.16.1.200 (вне глобального). Выполните команду **show ip nat translation** на маршрутизаторе для просмотра таблицы преобразования (см. [рисунок 4](#)).!

```
ip nat inside source static 10.89.238.56 172.16.1.200
```

!Рисунок 4 – IP NAT Translation

```
2600-4#show ip nat translation
Pro Inside global  Inside local  Outside local  Outside global
--- 172.16.1.200   10.89.238.56   ---           ---
```

## Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `show`.

- `show access-list` — отображает количество пакетов, которые проходят через список доступа.

## Процедура проверки

Выполните эти шаги для проверки конфигурации:

1. Выполните Microsoft Internet Explorer.
2. Введите `http://172.16.1.200` в Поле адреса окна браузера и нажмите ENTER. 172.16.1.200 внутренний глобальный адрес. В открытой сети пользователи СТС могут обратиться к только 172.16.1.200, который является внутренним глобальным адресом ONS 15454, внутренний локальный адрес которого 10.89.238.56. Окно входа СТС появляется.
3. Введите имя пользователя и пароль для регистрации. Клиент СТС успешно соединяется с ONS 15454.
4. Выполните команду `debug ip nat detailed` для включения IP NAT подробная трассировка. Можно просмотреть переадресации в файле трассировки. Например, переадресация от 10.89.238.56 до 172.16.1.200 (см. стрелку на [рисунке 5](#)), и от 172.16.1.200 до 10.89.238.56 (см. стрелку В на [рисунке 5](#)). Рисунок 5 – Debug IP NAT детализирован

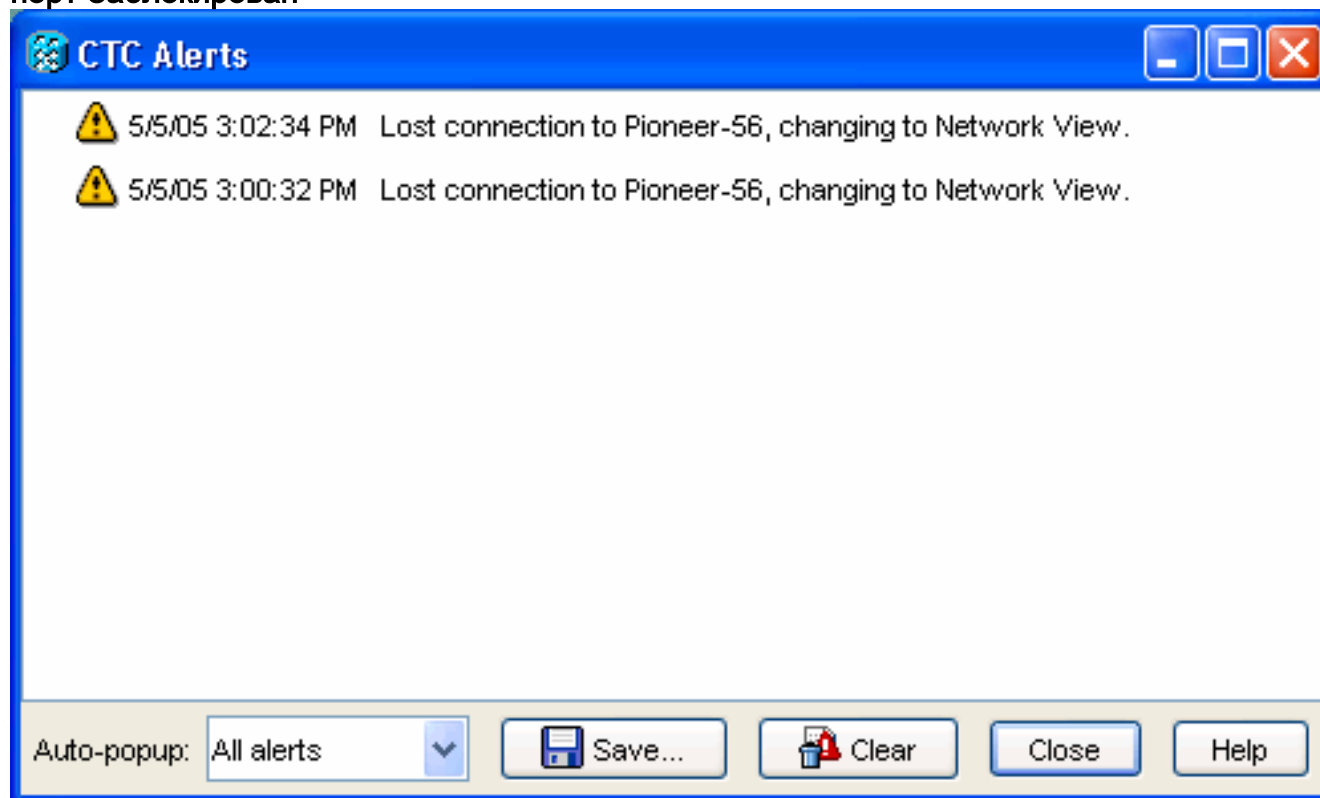
```
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55499]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55499]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55500]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55500]
NAT*: i: tcp (10.89.238.56, 80) -> (172.16.1.254, 2494) [55501]
NAT*: s=10.89.238.56->172.16.1.200, d=172.16.1.254 [55501]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32895]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32895]
NAT*: o: tcp (172.16.1.254, 2494) -> (172.16.1.200, 80) [32897]
NAT*: s=172.16.1.254, d=172.16.1.200->10.89.238.56 [32897]
```

5. Выполните команду `show access-list` на маршрутизаторе для просмотра количества пакетов, которые проходят через список доступа. Рисунок 6 – команда `show access-list`

```
2600-4#show access-list
Extended IP access list 101
  permit tcp any eq www any (56 matches)
  permit tcp any eq 1080 any (330 matches)
  permit tcp any any eq 683 (6 matches)
```

Если список доступа блокирует CORBA TCC (IIOP) Порт прослушивания, сеанс СТС с ONS 15454 регулярно испытывает таймаут, и сигнальное сообщение появляется каждые

две минуты как показано здесь: **Рисунок 7 – Предупреждения CTC: CORBA TCC (IIOP) порт Заблокирован**



Как обходной путь, можно открыть порт прослушивания IIOP CTC. Идентификатор ошибки Cisco [CSCeh96275 \(только зарегистрированные клиенты\)](#) решает эту проблему. В будущем создания conduit для Порта TCP 80 и 1080 на межсетевом экране достаточно для оказания поддержки для сокрытия реального IP - адреса ONS 15454.

## Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

## Дополнительные сведения

- [Cisco Systems – техническая поддержка и документация](#)