

Cisco ONS 15454 und NAT

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[NAT](#)

[Traditionelle NAT](#)

[Bidirektionale NAT](#)

[Zweifache NAT](#)

[ONS 15454 und NAT-Kompatibilität](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument werden die verschiedenen Typen der Network Address Translation (NAT) beschrieben und jeder NAT-Typ der entsprechenden Softwareversion der ONS 15454 zugeordnet, die diesen Typ unterstützt.

[Voraussetzungen](#)

[Anforderungen](#)

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco ONS 15454
- CTC
- NAT

[Verwendete Komponenten](#)

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

- Alle Versionen von Cisco ONS 15454

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

In vielen Fällen im Feld sind verschiedene NAT-Szenarien im Spiel und funktionieren nicht ordnungsgemäß. Sie können die meisten dieser Szenarien durch die Symptome identifizieren. Die meisten Probleme resultieren aus der Unfähigkeit des Netzwerkelements (NE), eine Verbindung zurück zur CTC-Workstation (Cisco Transport Controller) herzustellen.

Wenn der CTC häufig keine bestimmte NAT-Konfiguration unterstützt, verwirft und stellt in bestimmten Abständen eine Verbindung zu Knoten her. In neueren Versionen kann der CTC von Unterbrechungen wiederherstellen, ohne die Anzeige zu verlieren. In solchen Versionen können Sie dieses Problem bei der Interaktion mit dem Knoten über CTC bemerken.

Dieselben Symptome treten auch aufgrund falscher Konfigurationen der externen Firewall auf, bei denen die Sicherheit von Zugriffslisten diktiert wird. Die Zugriffslisten erlauben dem NE nicht, bestimmte Verbindungen zu oder von definierten IP-Adressen und/oder Ports zurück zur CTC-Workstation herzustellen. Häufige Verbindungsunterbrechungen können auch auftreten, wenn die Zeitüberschreitungseinstellungen für die externe Firewall zu kurz sind.

Beispiele für Firewall-Zugriffslisten, die Sie mit der ONS 15454 verwenden können, finden Sie im Abschnitt [Externe Firewalls](#) im [Cisco ONS 15454 Referenzhandbuch, Version 5.0](#).

NAT

Mit NAT kann ein einzelnes Gerät, z. B. ein Router, als Agent zwischen dem Internet und einem lokalen Netzwerk fungieren. In diesem Abschnitt werden die verschiedenen NAT-Typen erläutert.

Weitere Informationen finden Sie unter [Terminologie und Überlegungen des RFC 2663 - IP Network Address Translator](#).

Traditionelle NAT

Mit der herkömmlichen NAT können Hosts in einem privaten Netzwerk transparent auf Hosts im externen Netzwerk zugreifen. Herkömmliche NAT initiiert ausgehende Sitzungen aus dem privaten Netzwerk.

In diesem Abschnitt werden kurz die beiden Varianten der herkömmlichen NAT beschrieben:

- **Grundlegende NAT:** Bei Basic NAT wird ein Block externer Adressen reserviert. Die grundlegende NAT verwendet diese Adressen, um Adressen von Hosts in einer privaten Domäne zu übersetzen, wenn die Hosts Sitzungen mit der externen Domäne initiieren.
- **Network Address Port Translation (NAPT):** NAPT erweitert den Begriff der Übersetzung um

einen Schritt weiter. NAPT übersetzt auch Transportkennungen, z. B. TCP- und UDP-Portnummern sowie ICMP-Abfragekennungen. Bei einem solchen Übersetzungs-Multiplexer werden die Transportkennungen einer Reihe privater Hosts in die Transportkennungen einer einzelnen externen Adresse eingegeben. **Hinweis:** NAPT wird auch als Port Address Translation (PAT) bezeichnet.

Bidirektionale NAT

Ein Gerät im externen Netzwerk initiiert eine Transaktion mit einem Gerät im Inneren. Um diese Initiierung zu ermöglichen, wurde die grundlegende Version von NAT um erweiterte Funktionen erweitert. Diese Erweiterung wird am häufigsten als bidirektionale NAT bezeichnet, wird aber auch als Two-Way NAT und Inbound NAT bezeichnet. Mit einer bidirektionalen NAT können Sie Sitzungen von Hosts im öffentlichen Netzwerk und im privaten Netzwerk initiieren. Private Netzwerkadressen werden beim Herstellen von Verbindungen in beide Richtungen statisch oder dynamisch an global eindeutige Adressen gebunden.

Die NAT für eingehende Transaktionen ist schwieriger als die ausgehende NAT. Der Grund hierfür ist, dass das interne Netzwerk im Allgemeinen die IP-Adresse externer Geräte kennt, da diese Geräte öffentlich sind. Das externe Netzwerk kennt jedoch nicht die privaten Adressen des internen Netzwerks. Auch wenn das externe Netzwerk die IP-Adressen von privaten Netzwerken kennt, können Sie diese IP-Adressen niemals als Ziel eines IP-Datagramms angeben, das Sie von außerhalb initiieren, da sie nicht routbar sind.

Sie können eine der beiden folgenden Methoden verwenden, um das Problem mit der ausgeblendeten Adresse zu beheben:

- Statische Zuordnung
- DNS (TCP/IP Domain Name System)

Hinweis: In diesem Dokument impliziert bidirektionale NAT eine grundlegende NAT, die grundlegende NAT impliziert jedoch keine bidirektionale NAT.

Zweifache NAT

Zweifache NAT ist eine Variante von NAT. Zweimal NAT ändert sowohl die Quell- als auch die Zieladresse, wenn ein Datagramm Adressbereiche durchquert. Dieses Konzept unterscheidet sich von herkömmlichen NAT- und bidirektionalen NAT-Adressen, die nur eine der Adressen übersetzen (Quelle oder Ziel).

ONS 15454 und NAT-Kompatibilität

Diese Tabelle zeigt die ONS 15454- und NAT-Kompatibilität:

NAT-Typ	CTC-Sees	GNE-Sees (Gateway Network Element)	Unterstützte CTC-Version
Grundlegende NAT	GNE IP	Übersetztes IP	Version 3.3
NAPT	GNE IP	Übersetztes IP	Version 4.0

Bidirektionale NAT	Übersetztes IP	CTC-IP	Version 5.0
Zweifache NAT	Übersetztes IP	Übersetztes IP	Version 5.0

Fehlerbehebung

Bei einem Kommunikationsproblem zwischen NE und CTC enthält die Ausgabe des Befehls **fhDebug** folgende Fehlermeldung:

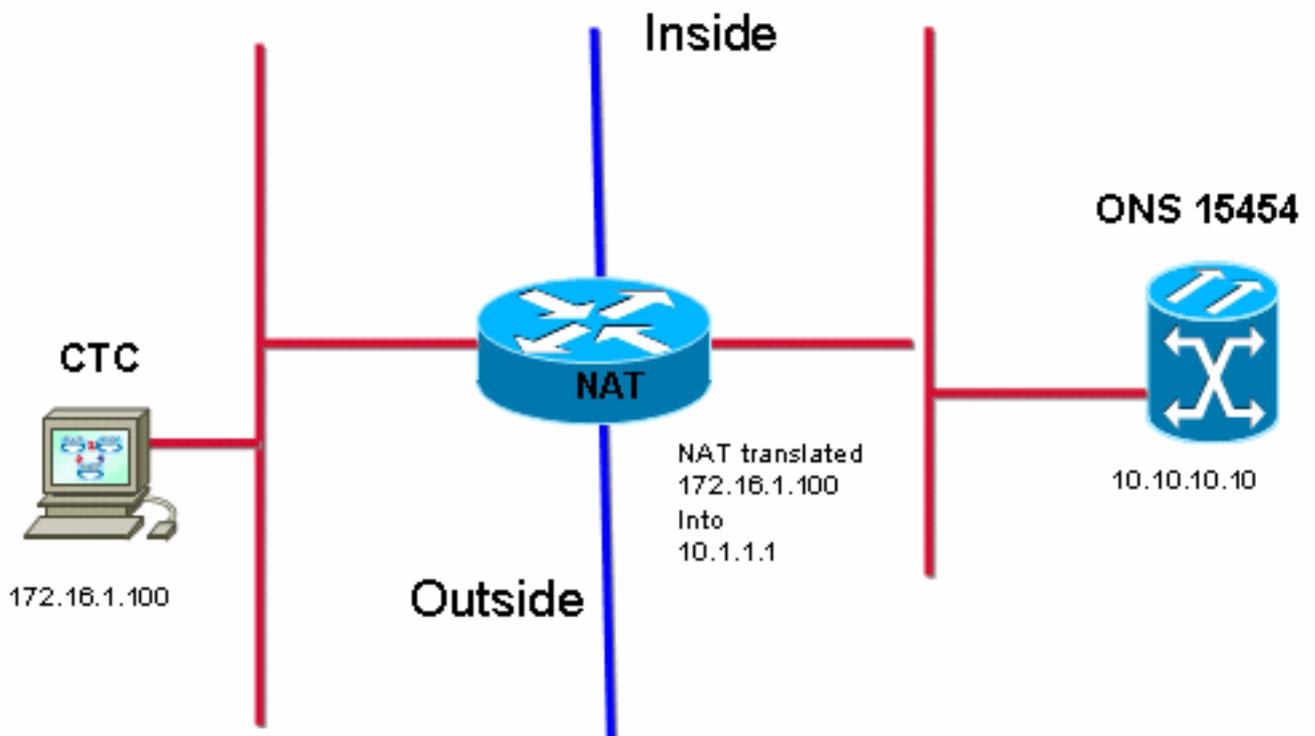
```
OCT 27 18:35:37.09 UTC ERROR      ObjectChange.cc:432   tEventMgr
CORBA::NO_IMPLEMENT/0x3d0004 updating [192.168.1.100:EventReceiver]. Marking c
```

```
OCT 27 18:36:17.09 UTC DEBUG      AlarmImpl.cc:353     tEventMgr
Removing corba client [192.168.1.100:EventReceiver] from auton msg list
```

Dieser Fehler kann aus mehreren Gründen verursacht werden. Wenn der Fehler jedoch in regelmäßigen, vorhersehbaren Intervallen (in der Regel ~2 oder ~4 Minuten) auftritt, kann dies entweder auf eine Art von NAT zurückzuführen sein, die vom CTC nicht unterstützt wird, oder auf eine Firewall ohne die erforderlichen Port-Berechtigungen.

Beachten Sie, dass 172.16.1.100 die IP-Adresse der CTC-Workstation und 10.1.1.1 die NAT-Adresse ist (siehe [Abbildung 1](#)).

Abbildung 1: Topologie



Hier ist die Teilausgabe des Befehls **inetstatShow**:

```
-> inetstatShow
Active Internet connections (including servers)
```

PCB	Typ	Rx-Q	Tx-Q	Local Address	Foreign Address	(state)
2145984	TCP	0	0	10.10.10.10:1052	10.1.1.1:1029	SYN_SENT
21457f8	TCP	0	0	10.10.10.10:80	10.1.1.1:1246	TIME_WAIT
2145900	TCP	0	0	10.10.10.10:57790	10.1.1.1:1245	ESTABLISHED --- ISP assigned address
21453d8	TCP	0	0	10.10.10.10:80	10.1.1.1:1244	TIME_WAIT
2144f34	TCP	0	0	10.10.10.10:80	10.1.1.1:1238	TIME_WAIT
2144eb0	TCP	0	0	10.10.10.10:1080	10.1.1.1:1224	ESTABLISHED --- ISP assigned address

Diese Ausgabe enthält keine Beweise für diese Adresse. Die Ausgabe zeigt die öffentliche Adresse, die der ISP verwendet. Dies ist ein Beweis für ein traditionelles NAT-Szenario.

Um bidirektionale NAT und doppelte NAT zu identifizieren, benötigen Sie eine Sniffer-Trace aus demselben Netzwerksegment wie die CTC-Workstation. Im Idealfall ist ein Sniffer, der auf der CTC-Workstation ausgeführt wird, am besten geeignet.

Zugehörige Informationen

- [Cisco ONS 15454 Referenzhandbuch, Version 5.0](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)