Cisco ONS 15454 and NAT

Document ID: 65343

Contents

Introduction

This document describes the different types of Network Address Translation (NAT), and maps each type of NAT to the relevant ONS 15454 software version which supports that type.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ONS 15454
- CTC
- NAT

Components Used

The information in this document is based on these software and hardware versions:

- All versions of Cisco ONS 15454

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

In many cases in the field, different NAT scenarios are in play and do not work properly. You can identify most of these scenarios through the symptoms. Most of the problems stem from the inability of the Network Element (NE) to initiate a connection back to the Cisco Transport Controller (CTC) workstation.

Often, when CTC does not support a particular configuration of NAT, CTC consistently drops and reconnects to nodes at specific intervals. In newer versions, CTC can recover from disconnects without dropping from view. In such versions, you can notice this issue during interaction with the node through CTC.

The same symptoms also occur due to incorrect configurations of the external firewall where Access Lists dictate security. The Access Lists do not allow the NE to initiate certain connections to or from defined IP addresses and/or ports, back towards the CTC Workstation. Frequent disconnects can also occur when the external firewall time−out settings are too short.

For sample firewall Access Lists that you can use with the ONS 15454, refer to the External Firewalls section of Cisco ONS 15454 Reference Manual, Release 5.0.

NAT

NAT allows a single device, for example, a router, to act as an agent between the Internet and a local network. This section explains the various types of NAT.

For more information, refer to RFC 2663 − IP Network Address Translator Terminology and Considerations ⬀ .

Traditional NAT

Traditional NAT allows hosts within a private network to transparently access hosts in the external network. Traditional NAT initiates outbound sessions from the private network.

This section briefly describes the two variations of Traditional NAT:

- **Basic NAT**: Basic NAT sets aside a block of external addresses. Basic NAT uses these addresses to translate addresses of hosts in a private domain when the hosts initiate sessions with the external domain.
- **Network Address Port Translation (NAPT)**: NAPT extends the notion of translation one step further. NAPT also translates transport identifiers, for example, TCP and UDP port numbers, and ICMP query identifiers. Such translation multiplexes the transport identifiers of a number of private hosts into the transport identifiers of a single external address.

    Note: NAPT is also called Port Address Translation (PAT).

Bi−Directional NAT

A device on the outside network initiates a transaction with a device on the inside. In order to permit this initiation, the basic version of NAT was enhanced to include advanced capabilities. This enhancement is most commonly known as Bi−directional NAT, but is also referred to as Two−Way NAT and Inbound NAT. With a Bi−directional NAT, you can initiate sessions from hosts in the public network and the private network. Private network addresses are bound to globally unique addresses, statically or dynamically as you establish connections in either direction.

Performance of NAT on inbound transactions is more difficult than outbound NAT. The reason is that the inside network generally knows the IP address of outside devices, because these devices are public. However, the outside network does not know the private addresses of the inside network. Even if the outside network is aware of the IP addresses of private networks, you can never specify these IP addresses as the target of an IP datagram that you initiate from outside, because they are not routable.

You can use one of these two methods to resolve the hidden address problem:

- Static mapping
- TCP/IP Domain Name System (DNS)

Note: In this document, Bi−directional NAT implies Basic NAT, but Basic NAT does not imply Bidirectional NAT.

Twice NAT

Twice NAT is a variation of NAT. Twice NAT modifies both the source and destination addresses when a datagram crosses address realms. This concept is in contrast to Traditional NAT and Bi−Directional NAT, which translate only one of the addresses (either source or destination).

ONS 15454 and NAT Compatibility

This table shows the ONS 15454 and NAT compatibility:

Type of NAT	CTC Sees	Gateway Network Element (GNE) Sees	Supported CTC Version
Basic NAT	GNE IP	Translated IP	Release 3.3
NAPT	GNE IP	Translated IP	Release 4.0
Bi−Directional NAT	Translated IP	CTC IP	Release 5.0
Twice NAT	Translated IP	Translated IP	Release 5.0

Troubleshoot

In case of a communication problem between the NE and CTC, the output of the **fhDebug** command contains this error message:

```
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
```
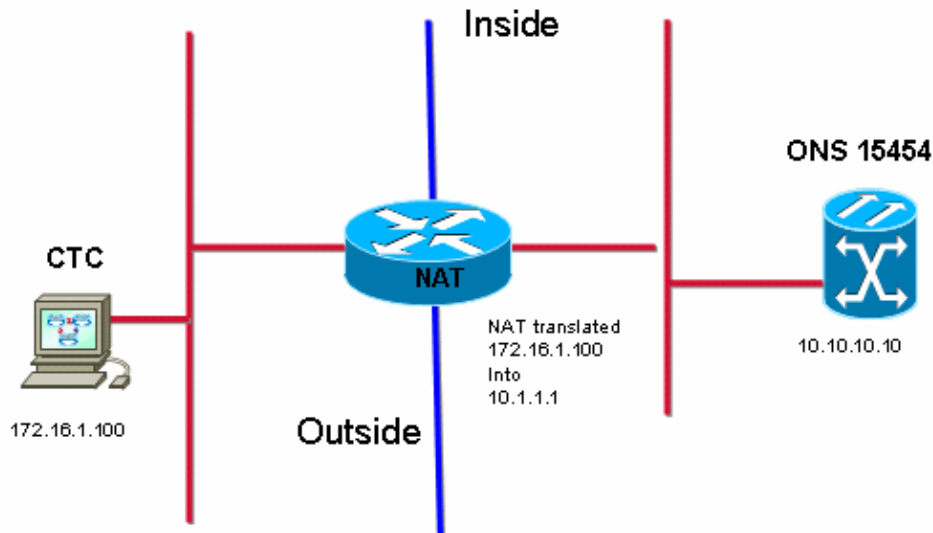
Several reasons can cause this error. However, if the error occurs at regular predictable intervals (usually ~2 or ~4 minutes), the reason can be the presence of either a type of NAT that CTC does not support, or a firewall without the necessary port permissions.

Observe that 172.16.1.100 is the IP address of the CTC workstation and 10.1.1.1 is the NAT address (see

Figure 1).

Figure 1   Topology

Here is the partial output of the **inetstatShow** command:

```
-> 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 addre
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 addre
```

This output shows no evidence of this address. The output shows the public address that the ISP uses, which is evidence of a Traditional NAT scenario.

In order to identify Bi–directional NAT and Twice NAT, you need a sniffer trace from the same network segment as the CTC workstation. Ideally, a sniffer that runs on the CTC workstation is most suitable.

Related Information

- **Cisco ONS 15454 Reference Manual, Release 5.0**
- **Technical Support & Documentation – Cisco Systems**

Updated: Jan 09, 2006   Document ID: 65343