Monitoring and Maintaining NAT

Last Updated: December 18, 2011

This module describes how to:

- Monitor Network Address Translation (NAT) using translation information and statistics displays.
- Maintain NAT by clearing NAT translations before the timeout has expired.
- Enable logging of NAT translation by way of syslog to log and track system error messages, exceptions, and other information.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Monitoring and Maintaining NAT

Before performing the tasks in this module, you must be familiar with the concepts described in the "Configuring NAT for IP Address Conservation" module and have NAT configured in your network.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About Monitoring and Maintaining NAT

NAT Display Contents

There are two basic types of IP NAT translation information:

Translation Entries

Translation entry information includes the following:

- The protocol of the port identifying the address.
- The legitimate IP address that represents one or more inside local IP addresses to the outside world.
- The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the NIC or service provider.
- The IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
- The IP address assigned to a host on the outside network by its owner.
- The time since the entry was created (in hours:minutes:seconds).
- The time since the entry was last used (in hours:minutes:seconds).
- Flags indicating the type of translation. Possible flags are:
  - extended--Extended translation
  - static--Static translation
  - destination--Rotary translation
  - outside--Outside translation
  - timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Statistical Information

Statistical information includes the following:

- The total number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
- A list of interfaces marked as outside with the **ip nat outside** command.
- A list of interfaces marked as inside with the **ip nat inside** command.
- The number of times the software does a translations table lookup and finds an entry.
- The number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
- A cumulative count of translations that have expired since the router was booted.
- Information about dynamic mappings.
- Information about an inside source translation.
- The access list number being used for the translation.

- The name of the pool.
- The number of translations using this pool.
- The IP network mask being used in the pool.
- The starting IP address in the pool range.
- The ending IP address in the pool range.
- The type of pool. Possible types are generic or rotary.
- The number of addresses in the pool available for translation.
- The number of addresses being used.
- The number of failed allocations from the pool.

NAT does not support ACL with the log option. The same functionality can be achieved by using one of the following options:

- By having a physical interface or VLAN with the logging option
- By using NetFlow
- By using the syslog feature

Syslog Usage

Syslog Analysis lets you centrally log and track system error messages, exceptions, and other information (such as device configuration changes). You can use the logged error message data to analyze router and network performance. You can customize Syslog Analysis to produce the information and message reports important to your operation.

For more information see the *Resource Manager Essentials and Syslog Analysis: How-To*document*:*

http://www.cisco.com/warp/public/477/RME/rme_syslog.html

How to Monitor and Maintain NAT

Displaying NAT Translation Information

SUMMARY STEPS

1. **enable**
2. **show ip nat translations** [**verbose**]
3. **show ip nat statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip nat translations** [**verbose**] **Example:** `Router# show ip nat translations`	(Optional) Displays active NAT translations.
Step 3	**show ip nat statistics** **Example:** `Router# show ip nat statistics`	(Optional) Displays active NAT translation statistics.

• Examples, page 4

Examples

This section contains the following examples:

Displaying NAT Translations

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1                     192.168.2.12
---                ---
--- 192.168.2.21                     192.168.2.89
---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 192.168.2.20:1220                  192.168.2.95:1220
192.168.2.22:53                           192.168.2.20:53
tcp 192.168.2.20:11012 192.168.2.209:11012 192.168.1.220:23 192.168.2.20:23
tcp 192.168.2.20:1067 192.168.2.20:1067 192.168.2.20:23 192.168.2.20:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
udp 192.168.2.20:1220 192.168.2.23:1220 192.168.2.24:53 192.168.2.25:53
        create 00:00:02, use 00:00:00, flags: extended
```

```
tcp 192.168.2.23:11012 192.168.2.30:11012 192.168.2.20:23 192.168.2.28:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 192.168.2.24:1067 192.168.2.29:1067 192.168.2.20:23 192.168.2.50:23
        create 00:00:02, use 00:00:00, flags: extended
```

Displaying NAT Statistics

The following is sample output from the **show ip nat statistics** command:

```
Router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 192.168.0.0 end 192.168.255.255
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

Clearing NAT Entries Before the Timeout

By default, dynamic address translations will time out from the NAT translation table at some point. Perform this task to clear the entries before the timeout.

SUMMARY STEPS

1. **enable**
2. **clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip*
3. **clear ip nat translation outside** *global-ip local-i* **p**
4. **clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port-global-ip global-port*
5. **clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]}
6. **clear ip nat translation inside** *global-ip local-ip* [**forced**]
7. **clear ip nat translation outside** *local-ip global-ip* [**forced**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Command or Action	Purpose

Step 2 **clear ip nat translation inside** *global-ip local-ip* **outside** *local-ip global-ip*
 	
Example:
`Router# clear ip nat translation inside 192.168.2.209 1220 192.168.2.95 1220`
 	
Example:
`outside 192.168.2.100 53 192.168.2.101 53`
	(Optional) Clears a single dynamic half-entry containing an inside translation, or both inside and outside translation created in a dynamic configuration.
	• A dynamic half-entry will be cleared only if it does not have any child translations.

Step 3 **clear ip nat translation outside** *global-ip local-i* **p** **Example:** `Router# clear ip nat translation outside 192.168.2.100 1220 192.168.2.80`	(Optional) Clears a single dynamic half-entry containing an outside translation created in a dynamic configuration. • A dynamic half-entry will be cleared only if it does not have any child translations.

Step 4 **clear ip nat translation** *protocol* **inside** *global-ip global-port local-ip local-port* **outside** *local-ip local-port-global-ip global-port*
 	
Example:
`Router# clear ip nat translation udp inside 192.168.2.209 1220 192.168.2.195 1220`
 	
Example:
`outside 192.168.2.13 53 192.168.2.132 53`
	(Optional) Clears a UDP translation entry.

Step 5 **clear ip nat translation** {* | [**forced**] | [**inside** *global-ip local-ip*] [**outside** *local-ip global-ip*]} **Example:** `Router# clear ip nat translation *`	(Optional) Clears either all dynamic translations (with the ***** or **forced** keyword), a single dynamic half-entry containing an inside translation, or a single dynamic half-entry containing an outside translation. • When clearing a single dynamic half-entry, it will be cleared only if it does not have any child translations.
Step 6 **clear ip nat translation inside** *global-ip local-ip* [**forced**] **Example:** `Router# clear ip nat translation *`	(Optional) Forces the clearing of a single dynamic half-entry and its child translations containing an inside translation created in a dynamic configuration, with or without its corresponding outside translation. • A dynamic half-entry will always be cleared, regardless of whether it has any child translations.

	Command or Action	Purpose
Step 7	**clear ip nat translation outside** *local-ip global-ip* [**forced**] **Example:** `Router# clear ip nat translation *`	(Optional) Forces the clearing of a single dynamic half-entry and its child translations containing an outside translation created in a dynamic configuration. • A dynamic half-entry will always be cleared, regardless of whether it has any child translations.

Enabling Syslog for Logging NAT Translations

The logging of NAT translations can be enabled and disabled by way of the **syslog** command.

Syslog Analysis lets you centrally log and track system error messages, exceptions, and other information (such as NAT translations). You can use the logged error message data to analyze router and network performance. You can customize Syslog Analysis to produce the information and message reports important to your operation.

Prior to performing this task, you must specify the necessary **syslog** commands such as making sure that logging is enabled, configuring the server's IP address, and establishing the level of messages to be trapped.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat log translations syslog**
4. **no logging console**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip nat log translations syslog** **Example:** `Router(config)# ip nat log translations syslog`	Enables the syslog for logging NAT translations.
Step 4	**no logging console** **Example:** `Router(config)# no logging console`	(Optional) Disables the log display to the console. • Logging to the console is enable by default.

Examples for Monitoring and Maintaining NAT

Clearing UDP NAT Translations Example

The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router# show ip nat translation


Pro Inside global        Inside local       Outside local      Outside global
udp 192.168.2.20:1220                  192.168.2.95:1220
192.168.2.22:53                            192.168.2.20:53
tcp 192.168.2.20:11012 192.168.2.209:11012 171.69.1.220:23 192.168.2.20:23
tcp 192.168.2.20:1067 192.168.2.20:1067 192.168.2.20:23 192.168.2.20:23
Router# clear ip nat translation udp inside 192.168.2.20:1067 192.168.2.20:1067 outside
192.168.2.20:23 192.168.2.20:23
Router# show ip nat translation

Pro Inside global      Inside local       Outside local      Outside global
udp 192.168.2.20:1220                  192.168.2.95:1220
192.168.2.22:53                            192.168.2.20:53
tcp 192.168.2.20:11012 192.168.2.209:11012 171.69.1.220:23 192.168.2.20:23
```

Enabling Syslog Example

The following example shows how to NAT entries into syslog.

```
Router(config)# logging on
Router(config)# logging 1.1.1.1
Router(config)# logging trap informational
Router(Config)# ip nat log translations syslog
```

The format of NAT information logged (for example, for ICMP Ping via NAT Overload configurations) will be as follows:

```
Apr 25 11:51:29 [10.0.19.182.204.28] 1: 00:01:13: NAT:Created icmp
135.135.5.2:7 171 12.106.151.30:7171 54.45.54.45:7171
54.45.54.45:7171
Apr 25 11:52:31 [10.0.19.182.204.28] 8: 00:02:15: NAT:Deleted icmp
135.135.5.2:7 172 12.106.151.30:7172 54.45.54.45:7172
54.45.54.45:7172
```

Where to Go Next

- To configure NAT for use with application level gateways, see the “Using Application Level Gateways with NAT” module.
- To integrate NAT with MPLS VPNs, see the “Integrating NAT with MPLS VPNs” module.
- To configure NAT for high availability, see the “Configuring NAT for High Availability” module.

Additional References

The following sections provide references related to Monitoring and Maintaining NAT.

Related Documents

Related Topic	Document Title
NAT commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	"IP Addressing Commands" chapter in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.3.

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Monitoring and Maintaining NAT

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Monitoring and Maintaining NAT

Feature Name	Releases	Feature Information
NAT--Forced Clear of Dynamic NAT Half-Entries	Cisco IOS 12.2 (33) XND	A second forced keyword was added to the **clear ip nat translation** command to enable the removal of half-entries regardless of whether they have any child translations.