



# NAT Support for SIP

---

## Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes the NAT Support for SIP feature in Cisco IOS Release 12.2(8)T and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 3](#)
- [Command Reference, page 3](#)
- [Glossary, page 10](#)

## Feature Overview

Session Initiation Protocol (SIP) is a protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group. The Cisco SIP functionality equips Cisco routers to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the Voice over IP (VoIP) internetworking software.

Session Description Protocol (SDP) is a protocol that describes multimedia sessions. SDP may be used in SIP message bodies to describe multimedia sessions used for creating and controlling multimedia sessions with two or more participants.

The NAT Support for SIP feature allows SIP embedded messages passing through a router configured with Network Address Translation (NAT) to be translated and encoded back to the packet. An application layer gateway (ALG) is used with NAT to translate the SIP or SDP messages.

For configuration information on SIP, consult the *Cisco IOS SIP Configuration Guide* located in the [Voice Configuration Library](#).

## Benefits

The NAT Support for SIP feature adds the ability to deploy Cisco IOS NAT between VoIP solutions based on SIP.

## Restrictions

NAT will translate only embedded IP version 4 addresses.

## Related Documents

- *Cisco IOS IP Configuration Guide, Release 12.2*
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2*

## Supported Platforms

- Cisco 2600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco 7700 series
- Cisco MC3810
- Cisco SOHO 70 series
- Cisco uBR925
- Cisco uBR7200 series

### **Determining Platform Support Through Cisco Feature Navigator**

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

### Standards

No new or modified standards are supported by this feature.

### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

### RFCs

No new or modified RFCs are supported by this feature.

## Configuration Tasks

None.

NAT support for SIP is enabled by default. If this feature has been disabled, you can reenable NAT support for SIP by using the **ip nat service sip** global configuration command.

## Verifying NAT Translation of SIP Messages

None

## Configuration Examples

None

## Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **debug ip nat**
- **ip nat service**

# debug ip nat

To display information about IP packets translated by the IP Network Address Translation (NAT) feature, use the **debug ip nat** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip nat** [*access-list* | **detailed** | **h323** | **sip** | **pptp**]

**no debug ip nat** [*access-list* | **detailed** | **h323** | **sip** | **pptp**]

## Syntax Description

<i>access-list</i>	(Optional) The standard IP access list number. If the datagram is not permitted by the specified access list, the related debugging output is suppressed.
<b>detailed</b>	(Optional) Displays debug information in a detailed format.
<b>h323</b>	(Optional) Displays H.225 and H.245 protocol information.
<b>sip</b>	(Optional) Displays Session Initiation Protocol (SIP) information.
<b>pptp</b>	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.

## Defaults

Disabled

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	This command was modified to include the <b>h323</b> keyword.
12.2(8)T	This command was modified to include the <b>sip</b> keyword.

## Usage Guidelines

The NAT feature reduces the need for unique, registered IP addresses. It can also save private network administrators from needing to renumber hosts and routers that do not conform to global IP addressing.

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also outputs information about certain errors or exceptional conditions, such as the failure to allocate a global address. To display messages related to the processing of H.225 signaling and H.245 messages, use the **debug ip nat h323** command. To display messages related to the processing of SIP messages, use the **debug ip nat sip** command.



### Caution

Because the **debug ip nat** command generates a substantial amount of output, use it only when traffic on the IP network is low, so other activity on the system is not adversely affected.

## Examples

The following is sample output from the **debug ip nat** command. In this example, the first two lines show the debugging output produced by a Domain Name System (DNS) request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. All Telnet packets, except for the first packet, were translated in the fast path, as indicated by the asterisk (\*).

```
Router# debug ip nat

NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

Table 1 describes the significant fields shown in the display.

**Table 1** debug ip nat Field Descriptions

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature. An asterisk (*) indicates that the translation is occurring in the fast path. The first packet in a conversation always goes through the slow path (that is, it is process switched). The remaining packets go through the fast path if a cache entry exists.
s=192.168.1.95—172.31.233.209	Source address of the packet and how it is being translated.
d=172.31.2.132	Destination address of the packet.
[6825]	IP identification number of the packet. Might be useful in the debugging process to correlate with other packet traces from protocol analyzers.

The following is sample output from the **debug ip nat detailed** command. In this example, the first two lines show the debugging output produced by a DNS request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. In this example, the inside host 192.168.1.95 was assigned the global address 172.31.233.193.

```
Router# debug ip nat detailed

NAT: i: udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT: o: udp (172.31.2.132, 53) -> (172.31.233.193, 1493) [63671]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22400]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22401]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22402]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22060]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22071]
```

Table 2 describes the significant fields shown in the display.

**Table 2** *debug ip nat detailed Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature. An asterisk (*) indicates that the translation is occurring in the fast path.
i:	Indicates that the packet is moving from a host inside the network to one outside the network.
o:	Indicates that the packet is moving from a host outside the network to one inside the network.
udp	Protocol of the packet.
(192.168.1.95, 1493)— (172.31.2.132, 53)	Indicates that the packet is sent from IP address 192.168.1.95, port number 1493 to IP address 172.31.2.132, port number 53.
[22399]	IP identification number of the packet.

The following is sample output from the **debug ip nat h323** command. In this example, an H.323 call is established between two hosts, one host on the inside and the other one on the outside. The debug output displays the H.323 messages names that NAT recognizes and the embedded IP addresses contained in those messages.

Router# **debug ip nat h323**

```
NAT:H225:[0] processing a Setup message
NAT:H225:[0] found Setup sourceCallSignalling
NAT:H225:[0] fix TransportAddress addr=192.168.122.50 port=11140
NAT:H225:[0] found Setup fastStart
NAT:H225:[0] Setup fastStart PDU length:18
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC forward mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[0] Setup fastStart PDU length:29
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC reverse mediaChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16516
NAT:H245:[0] found OLC reverse mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[1] processing an Alerting message
NAT:H225:[1] found Alerting fastStart
NAT:H225:[1] Alerting fastStart PDU length:25
NAT:H245:[1] processing OpenLogicalChannel message, forward channe
```

Table 3 describes the significant fields shown in the display.

**Table 3** *debug ip nat h323 Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
H.225 and H.245:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

The following is sample output from the **debug ip nat sip** command. In this example, one IP phone registers with a Cisco SIP proxy and then calls another IP phone. The debug displays the SIP messages that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat sip

NAT:SIP:[0] processing REGISTER message
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] message body found
NAT:SIP:[0] found address/port in SDP body:192.168.122.20
20332
NAT:SIP:[1] processing SIP/2.0 100 Trying reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing INVITE message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20
```

Table 4 describes the significant fields shown in the display.

**Table 4** *debug ip nat sip Field Descriptions*

Field	Description
NAT:	Indicates that the packet is being translated by the NAT feature.
SIP:	Protocol of the packet.
[1]	Indicates that the packet is moving from a host inside the network to one outside the network.
[0]	Indicates that the packet is moving from a host outside the network to one inside the network.

## ip nat service

To specify a port other than the default port, use the **ip nat service** command in global configuration mode. To disable the port, use the **no** form of this command.

```
ip nat service {list {access-list-number | access-list-name} ftp tcp port port-number | sip [tcp | udp] port port-number | skinny tcp port port-number}
```

```
no ip nat service {list {access-list-number | access-list-name} ftp tcp port port-number | sip [tcp | udp] port port-number | skinny tcp port port-number}
```

Syntax Description		
<b>list</b> <i>access-list-number</i>		Standard access list number in the range from 1 to 199.
<b>list</b> <i>access-list-name</i>		Name of a standard IP access list.
<b>ftp</b>		FTP protocol.
<b>tcp</b>		(Optional) TCP protocol.
<b>port</b> <i>port-number</i>		Port other than the default port in the range from 1 to 65533.
<b>sip</b>		Session Initiation Protocol.
<b>udp</b>		(Optional) UDP protocol.
<b>skinny</b>		Skinny protocol.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	The <b>skinny</b> keyword was added.
	12.2(8)T	The <b>sip</b> keyword was added.

**Usage Guidelines** A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service ftp** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service skinny** command.

NAT listens on the default port of the SIP Proxy/UA server to translate the SIP messages. If the SIP Proxy/UA uses a port other than the default port, that port needs to be configured using the **ip nat service sip** command.

---

**Examples**

The following example configures the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the nonstandard 20002 port of the CallManager:

```
ip nat service skinny tcp port 20002
```

The following example configures the nonstandard 8000 port of the of the Cisco SIP proxy server:

```
ip nat service sip tcp port 8000
```