NAT Optimized SIP Media Path with SDP

The NAT Optimized SIP Media Path with SDP feature allows the creation of a shorter path for Session Initiation Protocol (SIP) media channels by distributing endpoint IP addressing information with Session Descriptor Protocol (SDP) of SIP messages. This feature allows endpoints to communicate directly by using standard routing and eliminates the need for them to traverse through upstream NAT routers.

The Message Digest 5 (MD5) algorithm is supported.

History for the NAT Optimized SIP Media Path with SDP Feature

Release	Modification
12.4(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

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

Information About the NAT Optimized SIP Media Path with SDP Feature

Before enabling the NAT Optimized SIP Media Path with SDP feature, be sure you understand the following concepts:

Benefits of NAT Optimized SIP Media Path with SDP

- The media path can be shortened, decreasing voice delay.
- More control of voice policy is possible because the media path is closer to the customer domain and not deep within the service provider cloud.

NAT Optimized SIP Media Path with SDP Feature Design

The NAT Optimized SIP Media Path with SDP feature provides the ability to optimize the media path taken by a SIP VoIP session when NAT is used. NAT forces the VoIP traffic to take at least one extra hop in the network, which usually results in several additional hops being added to the path between two IP hosts.

Cisco IOS NAT will add the relevant translation information per SIP session within the SIP protocol messages. The SIP Application Layer Gateway support within Cisco IOS NAT will extract this translation information from the SIP packets and create NAT table entries.

The “piggybacking” of NAT translation information within the SIP call flows, the design of how users interact with the application when they talk to it, will allow the media path of a SIP VoIP session between two calling parties to take the optimized routing path between each other.

How to Configure NAT Optimized SIP Media Path with SDP

This section contains the following procedures:

Configuring a NAT Optimized SIP Media Path with SDP Messages Including MD5 Authentication

Perform this task to configure SDP messages with a NAT optimized SIP Media path including MD5 authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat piggyback-support sip-alg sdp-only router** *router-id* [**md5-authentication** *md5-authentication-key*]

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.
Step 3	**ip nat piggyback-support sip-alg sdp-only router** *router-id* **md5-authentication** *md5-authentication-key* **Example:** `Router(config)# ip nat piggyback-support sip-alg sdp-only router 100 md5-authentication md5-key`	Enables SDP messages with a NAT optimized SIP Media path including MD5 authentication.

Configuring a NAT Optimized SIP Media Path with SDP Messages Without MD5 Authentication

Perform this task to configure SDP messages with a NAT optimized SIP Media path without MD5 authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat piggyback-support sip-alg sdp-only router** *router-id*

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.
Step 3	**ip nat piggyback-support sip-alg sdp-only router** *router-id* **Example:** `Router(config)# ip nat piggyback-support sip-alg sdp-only router 100`	Enables SDP messages with a NAT optimized SIP Media path without MD5 authentication.

Configuration Examples for NAT Optimized SIP Media Path with SDP

This section provides the following configuration examples:

- Configuring a NAT Optimized SIP Media Path with SDP Including MD5 Authentication: Example, page 4
- Configuring a NAT Optimized SIP Media Path with SDP Without MD5 Authentication: Example, page 4

Configuring a NAT Optimized SIP Media Path with SDP Including MD5 Authentication: Example

The following example shows how to configure a NAT optimized SIP media path with SDP including MD5 authentication:

```
ip nat piggyback-support sip-alg sdp-only router 100 md5-authentication md5-key
```

Configuring a NAT Optimized SIP Media Path with SDP Without MD5 Authentication: Example

The following example shows how to configure a NAT optimized SIP media path with SDP without MD5 authentication:

```
ip nat piggyback-support sip-alg sdp-only router 100
```

Additional References

The following sections provide references related to the NAT Optimized SIP Media Path with SDP feature.

Related Documents

Related Topic	Document Title
IP NAT commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*, Release 12.4T
IP NAT configuration tasks	"NAT" section of the *Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4

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 Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **clear ip nat translation**
- **debug ip nat**
- **ip nat piggyback-support**

clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in privileged EXEC mode.

clear ip nat translation {***** | [**inside** *global-ip global-port local-ip local-port*] | [**outside** *local-ip global-ip*] [**piggyback-internal** | **esp** | **tcp** | **udp**]}

Syntax Description

*****	Clears all dynamic translations.
inside	(Optional) Clears the inside translations containing the specified *global-ip* and *local-ip* addresses.
global-ip	(Optional) Global IP address.
global-port	(Optional) Global port.
local-ip	(Optional) Local IP address.
local-port	(Optional) Local port.
outside	(Optional) Clears the outside translations containing the specified *global* and *local* addresses.
piggyback-internal	(Optional) Clears translations created by the piggyback.
esp	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
tcp	(Optional) Clears the TCP entries from the translation table.
udp	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The **esp** keyword was added.
12.4(2)T	The **piggyback-internal** keyword was added.

Usage Guidelines

Use this command to clear entries from the translation table before they time out.

Examples

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

```
Router# show ip nat translations

Pro Inside global        Inside local       Outside local      Outside global
udp 172.31.233.209:1220  192.168.1.95:1220  172.31.2.132:53    172.31.2.132:53
tcp 172.31.233.209:11012 192.168.1.89:11012 172.31.1.220:23    172.31.1.220:23
tcp 172.31.233.209:1067  192.168.1.95:1067  172.31.1.161:23    172.31.1.161:23
Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
```

```
10.69.2.132 53 10.69.2.132 53

Router# show ip nat translations

Pro     Inside global       Inside local       Outside local      Outside global
tcp     10.69.233.209:11012 10.168.1.89:11012  10.69.1.220:23     10.69.1.220:23
tcp     10.69.233.209:1067  10.168.1.95:1067   10.69.1.161:23     10.69.1.161:23
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

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** | **ipsec** | **piggyback-support** | **port** | **pptp** | **route** | **sip** | **skinny** | **vrf** | **wlan-nat**]

no debug ip nat [*access-list* | **detailed** | **h323** | **ipsec** | **port** | **pptp** | **route** | **sip** | **skinny** | **vrf** | **wlan-nat**]

Syntax Description

access-list	(Optional) Standard IP access list number. If the datagram is not permitted by the specified access list, suppresses the related debugging output.
detailed	(Optional) Displays debugging information in a detailed format.
h323	(Optional) Displays H.225, H.245, and H.323 protocol information.
ipsec	(Optional) Displays IP Security (IPSec) packet information.
piggyback-support	(Optional) Displays piggyback information.
port	(Optional) Displays port information.
pptp	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.
route	(Optional) Displays route information.
sip	(Optional) Displays Session Initiation Protocol (SIP) information.
skinny	(Optional) Displays debug information in a concise format.
vrf	(Optional) Displays Virtual Private Network (VPN) routing and forwarding (VRF) traffic-related information.
wlan-nat	(Optional) Displays Wireless LAN information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	The **h323** keyword was added.
12.2(8)T	The **sip** keyword was added.
12.2(13)T	The **ipsec** and **vrf** keywords were added.
12.3(2)XE	The **wlan-nat** keyword was added.
12.3(7)T	The **wlan-nat** keyword was implemented in Cisco IOS Release 12.3(7)T.
12.3(11)T	The output in the **h323** keyword was expanded to include H.245 tunneling.
12.4(2)T	The **piggyback-support** keyword was added.

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 each packet that the router translates. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also displays information about certain errors or exception 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. To display messages related to the processing of VRF messages, use the **debug ip nat vrf** 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 Domain Name System (DNS) request and reply debugging output. The remaining lines show 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]
```

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 host on the outside. The debugging output displays the H.323 message 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 channel
number 1
NAT:H323:[0] received pak, payload_len=46
NAT:H323:[0] processed up to new_payload_len 4
NAT:H323:[0] expecting data len=42--payload_len left 42
NAT:H323:[0] try to process tpkt with len 42, payload_len left 42
NAT:H225:processing a Facility message
NAT:H225:pdu_len :31 msg_IE:28
NAT:H323:choice-value:9
NAT:H225:[0] found h245Tunneling
NAT:H225:[0] found h245Control
NAT:H225:[0] h245control PDU length:20
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 2
NAT:H245:[0] found OLC forward mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=51001
NAT:H245:[0] TransportAddress addr changed 192.168.122.50->135.25.30.129
NAT:H245:[0] message changed, encoding back
NAT:H245:exit process tpkt with new_len 20
NAT:H225:message changed, encoding back
NAT:H323:[0] processed up to new_payload_len 46
NAT:H323:[0] new pak payload len is 46
```

Table 2 describes the significant fields shown in the display.

Table 2 debug ip nat h323 Field Descriptions

Field	Description
NAT	Indicates that the packet is being translated by the NAT feature.
H.225, H.245, and H.323	Protocol of the packet.
[0]	Indicates that the packet is moving from a host outside the network to one host inside the network.
[1]	Indicates that the packet is moving from a host inside the network to one host outside the network.

The following is sample output from the **debug ip nat ipsec** command:

```
Router# debug ip nat ipsec

5d21h:NAT:new IKE going In->Out, source addr 192.168.122.35, destination addr
192.168.22.20, initiator cookie
0x9C42065D
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.35 SPI=0xAAE32A0A,
IG=192.168.22.40, OL=192.168.22.20,
OG=192.168.22.20
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0xA64B5BB6,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.35

5d21h:NAT:new IKE going In->Out, source addr 192.168.122.20, destination addr
192.168.22.20, initiator cookie
0xC91738FF
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.20 SPI=0x3E2E1B92,
IG=192.168.22.40, OL=192.168.22.20,
OG=192.168.22.20
5d21h:NAT:IPSec:Inside host (IL=192.168.122.20) trying to open an ESP connection to
Outside host (OG=192.168.22.20),
wait for Out->In reply
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0x1B201366,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.20
```

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 debugging output 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->10.2.2.2
NAT:SIP:[0] translated embedded address
192.168.122.3->10.2.2.2
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
10.2.2.2->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address
10.2.2.2->192.168.122.3
```

```
NAT:SIP:[1] translated embedded address
10.2.2.2->192.168.122.3
NAT:SIP:[1] processing INVITE message
NAT:SIP:[1] translated embedded address
10.2.2.2->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20
```

Table 3 describes the significant fields shown in the display.

Table 3 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.
[0]	Indicates that the packet is moving from a host outside the network to one host inside the network.
[1]	Indicates that the packet is moving from a host inside the network to one host outside the network.

The following is sample output from the **debug ip nat vrf** command:

```
Router# debug ip nat vrf

6d00h:NAT:address not stolen for 192.168.121.113, proto 1 port 7224
6d00h:NAT:creating portlist proto 1 globaladdr 10.2.2.10
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.2.2.10:wanted 7224 got 7224
6d00h:NAT:i:icmp (192.168.121.113, 7224) -> (168.58.88.2, 7224) [2460]
6d00h:NAT:s=192.168.121.113->10.2.2.10, d=168.58.88.2 [2460] vrf=> shop

6d00h:NAT*:o:icmp (168.58.88.2, 7224) -> (10.2.2.10, 7224) [2460]      vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=10.2.2.10->192.168.121.113 [2460] vrf=> shop

6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.2.2.10:wanted 7225 got 7225
6d00h:NAT:i:icmp (192.168.121.113, 7225) -> (168.58.88.2, 7225) [2461]
6d00h:NAT:s=192.168.121.113->10.2.2.10, d=168.58.88.2 [2461] vrf=> shop
6d00h:NAT*:o:icmp (168.58.88.2, 7225) -> (10.2.2.10, 7225) [2461]      vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=10.2.2.10->192.168.121.113 [2461] vrf=> shop
6d00h:NAT:Allocated Port for 192.168.121.113 -> 10.2.2.10:wanted 7226 got 7226
6d00h:NAT:i:icmp (192.168.121.113, 7226) -> (168.58.88.2, 7226) [2462]
6d00h:NAT:s=192.168.121.113->10.2.2.10, d=168.58.88.2 [2462] vrf=> shop
```

Table 4 describes the significant fields shown in the display.

Table 4 debug ip nat vrf Field Descriptions

Field	Description
NAT	Indicates that the packet is being translated by the NAT feature.
s=192.168.121.113->2.2.2.10	Source address of the packet and how it is being translated.
d=168.58.88.2	Destination address of the packet.
[2460]	IP identification number of the packet.
vrf=>	Indicates that NAT is applied to a particular VPN.

ip nat piggyback-support

To enable a NAT optimized SIP media path, use the **ip nat piggyback-support** command in global configuration mode. To disable a NAT optimized SIP media path, use the **no** form of this command.

ip nat piggyback-support sip-alg {**sdp-only** | **all-messages**} **router** *router-id* **md5-authentication** *md5-authentication-key*

no ip nat piggyback-support sip-alg {**sdp-only** | **all-messages**} **router** *router-id* **md5-authentication** *md5-authentication-key*

Syntax Description

sip-alg	SIP protocol algorithm.
sdp-only	Establishes piggybacking in SDP only.
all-messages	Establishes piggybacking in all messages except SDP.
router *router-id*	Piggyback router ID number.
md5-authentication md5-authentication-*key*	MD5 authentication key.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example shows how to configure a NAT optimized SIP media path with SDP:

```
ip nat piggyback-support sip-alg sdp-only router 100 authentication md5-key
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.