



# Configuring Hosted NAT Traversal for Session Border Controller

---

**Last Updated: December 18, 2011**

The Cisco IOS Hosted NAT Traversal for Session Border Controller Phase-1 feature enables a Cisco IOS Network Address Translation (NAT) Session Initiation Protocol (SIP) Application Level Gateway (ALG) router to act as a Session Border Controller (SBC) on a Cisco Multiservice IP-to-IP gateway, ensuring a seamless delivery of VoIP services.

The Cisco IOS Hosted NAT Traversal for Session Border Controller Phase-2 feature provides registration throttling, media flow-through, and Stateful NAT (SNAT) support.

- [Finding Feature Information, page 1](#)
- [Prerequisites for Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller, page 2](#)
- [Restrictions for Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller, page 2](#)
- [Information About Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller, page 2](#)
- [How to Configure Cisco IOS Hosted NAT for Session Border Controller, page 4](#)
- [Configuration Examples for Configuring Cisco IOS Hosted NAT for Session Border Controller, page 9](#)
- [Additional References, page 10](#)
- [Feature Information for Configuring Hosted NAT Traversal for Session Border Controller, page 11](#)

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.



---

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

## Prerequisites for Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller

- Before you configure the Cisco IOS Hosted NAT Traversal for Session Border Controller feature, you should understand the concepts documented in “Cisco IOS Hosted NAT Traversal for Session Border Controller Overview” section.
- All access lists required for use with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the “Creating an IP Access List and Applying It to an Interface” module in the *Securing the Data Plane Configuration Guide*.
- Before performing the tasks in this module, you should verify that SIP has not been disabled. SIP is enabled by default.

## Restrictions for Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller

- Phase 1 supports flow-around mode for inside to inside media calls and flow-through for inside to outside media calls.
- If the intermediate routers between the inside phones and the NAT SBC are configured for Port Address Translation (PAT), the user agents (phones and proxy) must support symmetric signaling and symmetric and early media. The override port must be configured on the NAT SBC router. In the absence of support for symmetric signaling and symmetric and early media, the intermediate routers must be configured for non-PAT and the override address should be configured in the NAT SBC.

## Information About Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller

- [Voice and Multimedia over IP Networks, page 2](#)
- [Cisco IOS Hosted NAT Traversal for Session Border Controller Overview, page 3](#)

## Voice and Multimedia over IP Networks

SIP is a protocol developed by the 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 the H.323 protocol within the VoIP internetworking software.

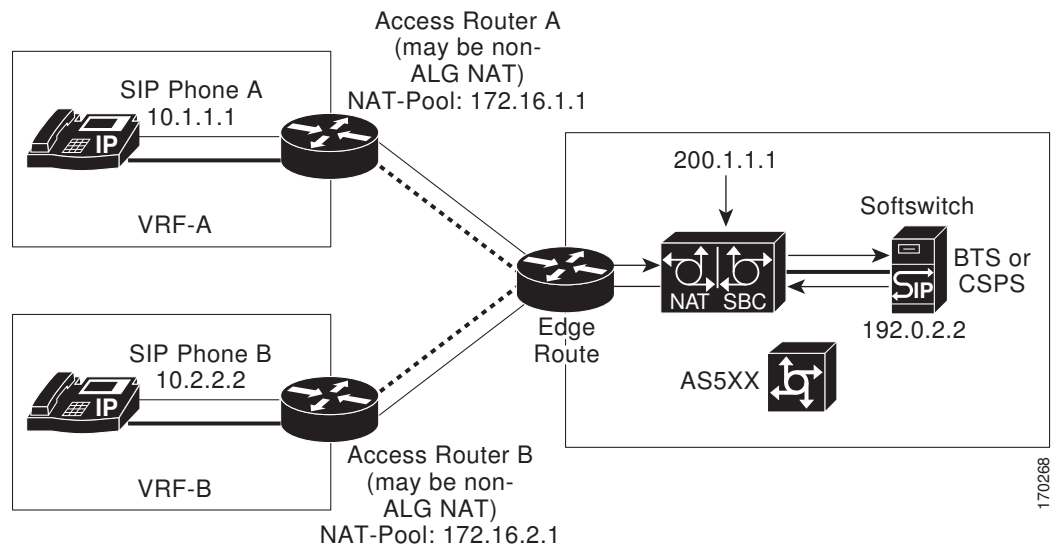
Session Description Protocol (SDP) describes multimedia sessions. SDP may be used in SIP message bodies to describe the multimedia sessions that are used for creating and controlling the multimedia sessions with two or more participants.

## Cisco IOS Hosted NAT Traversal for Session Border Controller Overview

Private IP addresses and ports inserted in the packet payload by client devices, such as IP phones and video conferencing stations, are not routable in public networks using NAT. In addition, intermediate routers between the inside phones and the NAT SBC can have the non-ALG functionality. The hosted NAT traversal handles the signaling and the media streams involved in the setting up, conducting, and tearing down of calls that traverse these intermediate routers.

The figure below illustrates how the NAT SBC handles embedded SIP/SDP information for the address and port allocation by differentiating the overlapped embedded information.

**Figure 1 NAT as a SIP Session Border Controller**



The inside phones have the proxy configured as the NAT SBC's preconfigured address and port. NAT SBC has the Softswitch's address and port preconfigured as the proxy. The NAT SBC intercepts the packets destined from the inside phones to itself and translates the inside hosts and other information in the SIP/SDP payload and the IP/UDP destination address or port to the Softswitch's address and port, and vice versa.

SIP/SDP information is either a NAT or a PAT in order for the Real-Time Transport Protocol (RTP) flow to be directly between the phones in the NAT SBC inside domain.

The address-only fields are not translated by the NAT SIP ALG. The address-only fields are handled by the NAT SBC, except for the proxy-authorization and authorization translation, because these will break the authentication.

If the intermediate routers between the inside phones and the NAT SBC are configured to do a PAT, the user agents (phones and proxy) must support symmetric signaling and symmetric and early media. You must configure the override port on the NAT SBC router. In the absence of support for symmetric signaling and symmetric and early media, the intermediate routers must be configured without PAT and the override address should be configured in the NAT SBC.

The registration throttling support enables you to define the parameters in the Expires: header and the expires= parameter. It allows you to elect to not forward certain registration messages to the Softswitch.

# How to Configure Cisco IOS Hosted NAT for Session Border Controller

- [Configuring Cisco IOS Hosted NAT for Session Border Controller, page 4](#)

## Configuring Cisco IOS Hosted NAT for Session Border Controller

Perform this task to configure NAT for SBC.

**Note**

---

When you use the NAT SBC feature and you want the call IDs to be translated, you must configure two address pools in such a way that the pool for SBC is accessed before the pool for the call IDs. Use the **ip nat pool** command to configure the address pools. Access lists are chosen in ascending order, so you should assign the list associated with the SBC pool a lower number than the list associated with the call ID pool.

---

**Note**

---

The proxy of the inside phones must be set to 200.1.1.1. The VPN routing and forwarding (VRF) instance configuration as shown is optional.

---

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface *type number*
4. ip nat inside
5. exit
6. interface *type number*
7. ip nat outside
8. exit
9. ip nat pool *name start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}
10. ip nat pool *name start-ip end-ip* {netmask *netmask* | prefix-length *prefix-length*}
11. ip nat inside source list *access-list-number* pool *name* [*vrf vrf-name*] [*overload*]
12. ip nat outside source list *access-list-number* pool *name*
13. ip nat sip-sbc
14. proxy *inside-address inside-port outside-address outside-port* protocol **udp**
15. vrf-list
16. vrf-name *vrf - name*
17. exit
18. ip nat sip-sbc
19. call-id-pool *call -id-pool*
20. session -timeout *seconds*
21. mode allow -flow-around
22. override address
23. end

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
<b>Step 3</b>	<p><code>interface type number</code></p> <p><b>Example:</b></p> <pre>Router(config)# interface ethernet 1/1</pre>	Specifies an interface and returns to interface configuration mode.
<b>Step 4</b>	<p><code>ip nat inside</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ip nat inside</pre>	Connects the interface to the inside network (the network subject to NAT translation).
<b>Step 5</b>	<p><code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and enters global configuration mode.
<b>Step 6</b>	<p><code>interface type number</code></p> <p><b>Example:</b></p> <pre>Router(config)# interface ethernet 1/3</pre>	Specifies an interface and enters interface configuration mode.
<b>Step 7</b>	<p><code>ip nat outside</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# ip nat outside</pre>	Connects the interface to the outside network.
<b>Step 8</b>	<p><code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.
<b>Step 9</b>	<p><code>ip nat pool name start-ip end-ip {netmask netmask   prefix-length prefix-length}</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat pool inside-pool-A 172.16.0.1 172.16.0.10 prefix-length 16</pre>	<p>Defines a pool of global addresses to be allocated for the inside network.</p> <p><b>Note</b> You must configure two address pools when you are using the NAT SBC feature and you want to translate the call IDs. In this step you are configuring the first address pool.</p>

Command or Action	Purpose
<p><b>Step 10</b> <code>ip nat pool name start-ip end-ip {netmask netmask   prefix-length prefix-length}</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat pool outside-pool 203.0.113.1 203.0.113.10 prefix-length 24</pre>	<p>Defines a pool of global addresses to be allocated for the outside network.</p> <p><b>Note</b> You must configure two address pools when you are using the NAT SBC feature and you want to translate the call IDs. In this step, you are configuring the second address pool.</p>
<p><b>Step 11</b> <code>ip nat inside source list access-list-number pool name [vrf vrf-name] [overload]</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat inside source list 1 pool inside-pool-A vrf vrfA overload</pre>	<p>Enables NAT of the inside source address and configures the access list for translation.</p>
<p><b>Step 12</b> <code>ip nat outside source list access-list-number pool name</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat outside source list 3 pool outside-pool</pre>	<p>Enables NAT of the outside source address and configures the access list for translation.</p>
<p><b>Step 13</b> <code>ip nat sip-sbc</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat sip-sbc</pre>	<p>Enters IP NAT SBC configuration mode.</p>
<p><b>Step 14</b> <code>proxy inside-address inside-port outside-address outside-port protocol udp</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# proxy 200.1.1.1 5060 192.0.2.2 5060 protocol udp</pre>	<p>Configures the address or port that the inside phones will be referring to, and the outside proxy's address and port to which the NAT SBC translates the destination IP address and port.</p>
<p><b>Step 15</b> <code>vrf-list</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# vrf-list</pre>	<p>(Optional) Enters IP NAT SBC VRF configuration mode.</p>

Command or Action	Purpose
<p><b>Step 16</b> <code>vrf-name vrf - name</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc-vrf)# vrf-name vrf1</pre>	(Optional) Defines SBC VRF list names.
<p><b>Step 17</b> <code>exit</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc-vrf)# exit</pre>	Exits IP NAT SBC VRF configuration mode and enters global configuration mode.
<p><b>Step 18</b> <code>ip nat sip-sbc</code></p> <p><b>Example:</b></p> <pre>Router(config)# ip nat sip-sbc</pre>	Enters IP NAT SBC configuration mode.
<p><b>Step 19</b> <code>call-id-pool call -id-pool</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# call-id-pool pool-name</pre>	<p>Specifies a dummy pool name for the in to out SIP signaling packet's call ID that it will be translated to, and that a 1:1 association will be maintained rather than using the regular NAT pool.</p> <ul style="list-style-type: none"> <li>• This pool can be used in an overload scenario: <ul style="list-style-type: none"> <li>◦ NAT mapping with an appropriate access control list (ACL) and a NAT pool matching the pool name must be configured.</li> <li>◦ This pool is not used for any other NAT processing except for call ID processing.</li> </ul> </li> </ul>
<p><b>Step 20</b> <code>session -timeout seconds</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# session-timeout 300</pre>	<p>Configures the timeout duration for NAT entries pertaining to SIP signaling flows.</p> <ul style="list-style-type: none"> <li>• The default is 5 minutes.</li> </ul>
<p><b>Step 21</b> <code>mode allow -flow-around</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# mode allow-flow-around</pre>	<p>Enables flow-around for RTP.</p> <ul style="list-style-type: none"> <li>• This flow applies to traffic between phones in the inside domain.</li> </ul>



Command or Action	Purpose
<p><b>Step 22</b> <code>override address</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# override address</pre>	<p>Allows the NAT SBC to override the out to in traffic's destination IP during signaling or RTP traffic, or to override the address and port.</p>
<p><b>Step 23</b> <code>end</code></p> <p><b>Example:</b></p> <pre>Router(config-ipnat-sbc)# end</pre>	<p>Exits IP NAT SBC configuration mode and enters privileged EXEC mode.</p>

## Configuration Examples for Configuring Cisco IOS Hosted NAT for Session Border Controller

- [Example Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller, page 9](#)

### Example Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller

The following example shows how to configure the Cisco IOS Hosted NAT Traversal as Session Border Controller feature:

```
interface ethernet1/1
 ip nat inside
!
interface ethernet1/2
 ip nat inside
!
interface ethernet1/3
 ip nat outside
!
ip nat pool inside-pool-A 172.16.0.1 172.16.0.10 prefix-length 16
ip nat pool inside-pool-B 192.168.0.1 192.168.0.10 prefix-length 24
ip nat pool outside-pool 203.0.113.1 203.0.113.10 prefix-length 24
ip nat inside source list 1 pool inside-pool-A vrf vrfA overload
ip nat inside source list 2 pool inside-pool-B vrf vrfB overload
ip nat outside source list 3 pool outside-pool
!
! Access-list for VRF-A inside phones
access-list 1 permit 172.16.0.0 255.255.0.0
!
! Access-list for VRF-B inside phones
access-list 2 permit 192.0.2.0 255.255.255.0
!
access-list 3 permit 203.0.113.0 255.255.255.0
ip nat sip-sbc
 proxy 200.1.1.1 5060 192.0.2.2 5060 protocol udp
 vrf-list
  vrf-name vrfA
  vrf-name vrfB
```

```

exit
call-id-pool pool-name
session-timeout 300
mode allow-flow-around
override address

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
NAT commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Addressing Services Command Reference</i>
Configuring an IP access list	“Creating an IP Access List and Applying It to an Interface” module in the <i>Securing the Data Plane Configuration Guide</i>

### Standards

Standards	Title
None	--

### MIBs

MIBs	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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for Configuring Hosted NAT Traversal for Session Border Controller

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1** Feature Information for Configuring Hosted NAT Traversal for Session Border Controller

Feature Name	Releases	Feature Information
Cisco IOS Hosted NAT Traversal for Session Border Controller Phase-1	12.4(9)T	The Cisco IOS Hosted NAT Traversal for Session Border Controller feature provides transparency with the use of a proxy device on the NAT outside domain.
Hosted NAT Support for Session Border Controller Phase-2	12.4(15)T	The Hosted NAT Support for Session Border Controller Phase-2 feature provides registration throttling, media flow-through, and SNAT support.
NAT as SIP Session Border Controller Media Flow	12.4(9)T	The NAT as SIP Session Border Controller Media Flow feature provides support for media flow-around for RTP or RTCP exchanges between phones on the inside domain of the SBC.
NAT as SIP Session Border Controller Support for Address-Only Fields	12.4(9)T	The NAT as SIP Session Border Controller Support for Address-Only Fields feature provides support for the translation of SIP address-only fields.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.