# NAT TCP SIP ALG Support

The NAT TCP SIP ALG Support feature allows embedded messages of the Session Initiation Protocol (SIP) passing through a device that is 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 Session Description Protocol (SDP) messages.

This module describes the NAT TCP SIP ALG Support feature and explains how to configure it.



## Prerequisites for NAT TCP SIP ALG Support

Layer 4 Forwarding (L4F) must be enabled for the feature to function.

## Restrictions for NAT TCP SIP ALG Support

- Network Address Translation (NAT) translates only embedded IPv4 addresses.
- NAT application-layer gateway (ALG) fixup for Session Initiation Protocol (SIP) messages over TCP is not done when Layer 4 Forwarding (L4F) functionality is disabled. In this case, SIP messages are considered as TCP messages and only Layer 3 and Layer 4 fixups are done.
- As per RFC 5128, NAT TCP SIP ALG feature uses Endpoint-Independent mapping to perform address translations. This combination allows incoming SIP traffic from any external endpoint on the public network to a mapped public port. If you do not need Endpoint-Independent mapping, use ACL or Zone-based Policy Firewall to limit the scope of incoming traffic.

# Information About NAT TCP SIP ALG Support

## NAT TCP SIP ALG Support Overview

The NAT TCP SIP ALG Support feature allows embedded messages of the Session Initiation Protocol (SIP) passing through a device that is 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 Session Description Protocol (SDP) messages. The NAT TCP SIP ALG Support feature adds NAT ALG support for fixing up TCP-based SIP messages.

Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. SIP is a protocol developed by IETF for multimedia conferencing over IP. SIP can be configured to operate over TCP-based transports. Cisco SIP implementation enables supported Cisco platforms to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the VoIP internetworking software.

Like other VoIP protocols, SIP is designed to address functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control attributes of an end-to-end call.

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

## SIP Messages

Entities that are present in a Session Initiation Protocol (SIP) deployment communicate with each other by using well-defined SIP messages that take the form of requests and responses. These SIP messages can contain embedded IP address or port information that might belong to a private domain, and such messages must be fixed up when they pass through a Network Address Translation (NAT) device. Fixup denotes the writing of the translated IP address back into the packet. This fixup is normally performed by an application-layer gateway (also called an application-level gateway) (ALG) module that resides on the NAT device.

By default, support for SIP is enabled on the standard TCP port 5060 to exchange SIP messages. You can also configure nonstandard ports for SIP to operate. NAT ALG accepts and attempts fixup operations on all TCP segments that originate from or are destined to the configured SIP port. SIP message processing involves performing the fixup operation on a complete SIP message. A TCP segment may carry multiple SIP messages. It is also possible that a SIP message is segmented and carried in two different TCP segments.

SIP messages are text based. Any adjustment that is made to the message as part of the ALG fixup can result in the message to increase or decrease in size. A change in the message size means that the ALG must make adjustments to the TCP sequence or acknowledgment numbers and keep track of the same. There are cases where the ALG must perform spoof acknowledgments and complete TCP retransmission.

TCP proxy is an essential component that terminates a TCP connection passing through NAT ALG and regenerates the TCP connection. This connection allows NAT ALG to modify the TCP payload without any TCP session handling issues.

The table below identifies the six available SIP request messages.

*Table 1: SIP Request Messages*

| SIP Message | Purpose |
|---|---|
| ACK | Sent by calling party to confirm the receipt of a final response to INVITE. |
| BYE | Sent by calling party or called party to end a call. |
| CANCEL | Sent to end a call that has not yet been connected. |
| INVITE | Request sent from a User Agent Client (UAC) to initiate a session. |
| OPTIONS | Sent to query capabilities of UACs and network servers. |
| REGISTER | Sent by the client to register the address with a SIP proxy. |

The table below identifies the available SIP response methods.

*Table 2: SIP Response Messages*

| SIP Message | Purpose |
|---|---|
| 1xx (Informational) | • 100 = Trying<br>• 180 = Ringing<br>• 181 = Call Is Being Forwarded<br>• 182 = Queued<br>• 183 = Session Progress |
| 2xx (Successful) | • 200 = OK |
| 3xx (Redirection) | • 300 = Multiple Choices<br>• 301 = Moved Permanently<br>• 302 = Moved Temporarily<br>• 303 = See Other<br>• 305 = Use Proxy<br>• 380 = Alternative Service |

| SIP Message | Purpose |
|---|---|
| 4xx (Request Failure) | • 400 = Bad Request<br>• 401 = Unauthorized<br>• 402 = Payment Required<br>• 403 = Forbidden<br>• 404 = Not Found<br>• 405 = Method Not Allowed<br>• 406 = Not Acceptable<br>• 407 = Proxy Authentication Required<br>• 408 = Request Timeout<br>• 409 = Conflict<br>• 410 = Gone<br>• 411 = Length Required<br>• 413 = Request Entity Too Large<br>• 414 = Request URI Too Large<br>• 415 = Unsupported Media Type<br>• 420 = Bad Extension<br>• 480 = Temporarily Not Available<br>• 481 = Call Leg/Transaction Does Not Exist<br>• 482 = Loop Detected<br>• 483 = Too Many Hops<br>• 484 = Address Incomplete<br>• 485 = Ambiguous<br>• 486 - Busy Here |
| 5xx (Server Failure) | • 500 = Internal Server Error<br>• 501 = Not Implemented<br>• 502 = Bad Gateway<br>• 503 = Service Unavailable<br>• 504 = Gateway Timeout<br>• 505 = SIP Version Not Supported |

| SIP Message | Purpose |
|---|---|
| 6xx (Global Failure) | • 600 = Busy Anywhere<br>• 603 = Decline<br>• 604 = Does Not Exist Anywhere<br>• 606 = Not Acceptable |

# SIP Functionality

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format sip:*userID@gateway*.com. The *userID* can be either a username or an E.164 address. The *gateway* can be either a domain (with or without a hostname) or a specific internet IP address.

**Note** An E.164 address is a telephone number with a string of decimal digits, which uniquely indicates the public network termination point. This address contains all information that is necessary to route a call to a termination point.

Users register with a registrar server using their assigned SIP addresses. The registrar server provides SIP addresses to the location server on request. The registrar server processes requests from user-agent clients (UACs) for registration of their current locations.

When a user initiates a call, a SIP request is sent to a SIP server (either a proxy or a redirect server). The request includes the address of the caller (in the From header field) and the address of the intended called party (in the To header field).

A SIP end user might move between end systems. The location of the end user can be dynamically registered with the SIP server. The location server can use one or more protocols (including Finger, RWhois, and Lightweight Directory Access Protocol [LDAP]) to locate the end user. Because the end user can be logged in at more than one station and the location server can sometimes have inaccurate information, the location server might return more than one address for the end user. If the request is coming through a SIP proxy server, the proxy server tries each of the returned addresses until it locates the end user. If the request is coming through a SIP redirect server, the redirect server forwards all the addresses to the caller available in the Contact header field of the invitation response.

# SIP Functionality with a Proxy Server

A proxy server receives Session Initiation Protocol (SIP) requests from a client and forwards them on the client's behalf. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

SIP is a peer-to-peer protocol. The peers in a session are called user agents (UAs).

When communicating through a proxy server, the caller UA sends an INVITE request to the proxy server and then the proxy server determines the path and forwards the request to the called party. The called UA responds to the proxy server, which then forwards the response to the caller. When both parties respond with an acknowledgment (SIP ACK message), the proxy server forwards the acknowledgments to their intended party

and a session, or conference, is established between them. The Real-time Transfer Protocol (RTP) is then used for communication across the connection now established between the caller and called UA.

# How to Configure NAT TCP SIP ALG Support

## Specifying a Port for NAT TCP SIP ALG Support

Network Address Translation (NAT) support for Session Initiation Protocol (SIP) is enabled by default. SIP uses the default TCP port 5060 to exchange messages. If required, you can configure a different port to handle SIP messages.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service sip tcp port** *port-number*
4. **end**
5. **debug ip nat sip**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip nat service sip tcp port** *port-number*<br>**Example:**<br>`Device(config)# ip nat service sip tcp port 8000` | Specifies a port number other than the default port. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **debug ip nat sip**<br>**Example:**<br>`Device# debug ip nat sip` | Displays SIP messages that NAT recognizes and the embedded IP addresses contained in those messages. |

# Configuration Examples for NAT TCP SIP ALG Support

## Example: Specifying a Port for NAT TCP SIP ALG Support

The following example shows how to configure the nonstandard port 8000:

```
Device(config)# ip nat service sip tcp port 8000
```

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

```
Device# debug ip nat sip

May 23 14:11:17.243 IST: NAT-L4F:setting ALG_NEEDED flag in subblock for SIP message
May 23 14:11:17.243 IST: NAT-ALG: lookup=0 l7_bytes_recd=509 appl_type=7
May 23 14:11:17.243 IST: NAT-ALG: Complete SIP Message header of size: 376

May 23 14:11:17.243 IST: NAT-ALG: Message body length: 133
May 23 14:11:17.243 IST: NAT-ALG: Total SIP message length: 509
May 23 14:11:17.243 IST: NAT-ALG: after state machine:
May 23 14:11:17.243 IST: NAT-ALG: l7_bytes_recd=509
May 23 14:11:17.243 IST: NAT-ALG: remaining_hdr_sz=0
May 23 14:11:17.243 IST: NAT-ALG: remaining_payl_sz=0
May 23 14:11:17.243 IST: NAT-ALG: tcp_alg_state=0
May 23 14:11:17.243 IST: NAT-ALG: complete_msg_len=509
May 23 14:11:17.243 IST: NAT-SIP-TCP: Number of SIP messages received: 1
May 23 14:11:17.243 IST: NAT: SIP: [0] processing INVITE message
May 23 14:11:17.243 IST: NAT: SIP: [0] register:0 door_created:0
May 23 14:11:17.243 IST: NAT: SIP: [0] translated embedded address 192.168.122.3->10.1.1.1
May 23 14:11:17.243 IST: NAT: SIP: [0] register:0 door_created:0
May 23 14:11:17.243 IST: NAT: SIP: [0] translated embedded address 192.168.122.3->10.1.1.1
May 23 14:11:17.243 IST: NAT: SIP: [0] register:0 door_created:0
May 23 14:11:17.243 IST: NAT: SIP: [0] register:0 door_created:0
May 23 14:11:17.243 IST: NAT: SIP: Contact header found
May 23 14:11:17.243 IST: NAT: SIP: Trying to find expires parameter
May 23 14:11:17.243 IST: NAT: SIP: [0] translated embedded address 192.168.122.3->10.1.1.1
May 23 14:11:17.243 IST: NAT: SIP: [0] register:0 door_created:0
May 23 14:11:17.243 IST: NAT: SIP: [0] message body found
May 23 14:11:17.243 IST: NAT: SIP: Media Lines present:1
May 23 14:11:17.243 IST: NAT: SIP: Translated global m=(192.168.122.3, 6000) -> (10.1.1.1,
 6000)
May 23 14:11:17.243 IST: NAT: SIP: old_sdp_len:133 new_sdp_len :130
May 23 14:11:17.243 IST:  l4f_send returns 497 bytes
May 23 14:11:17.243 IST:  Complete buffer written to proxy
```

# Additional Reference for NAT TCP SIP ALG Support

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| NAT commands | Cisco IOS IP Addressing Services Command Reference |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 2543 | *SIP: Session Initiation Protocol* |

### 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 NAT TCP SIP ALG Support

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 3: Feature Information for NAT TCP SIP ALG Support***

| Feature Name | Releases | Feature Information |
|---|---|---|
| NAT TCP SIP ALG Support | 15.3(1)T | The NAT TCP SIP ALG Support feature allows embedded messages of the Session Initiation Protocol (SIP) passing through a device that is 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 Session Description Protocol (SDP) messages. |