



Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

First Published: June 22, 2006

Last Updated: November 17, 2006

The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature extends support for Network Address Translation (NAT) traversal to the mobile router when the mobile router is in private addressing space behind a NAT-enabled device and needs to register directly to the public home agent using a private collocated care-of address (CCoA).

NAT traversal is based on the RFC 3519 specification and defines how Mobile IP should operate to traverse networks that deploy NAT within their network. NAT traversal allows Mobile IP to interoperate with networks that have NAT enabled by providing an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added that establish User Datagram Protocol (UDP) tunneling.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router”](#) section on page 13.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/fn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router, page 2](#)
- [Restrictions for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router, page 2](#)
- [Information About Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router, page 2](#)
- [How to Configure the Mobile Router for RFC 3519 NAT Traversal Support, page 4](#)



Corporate Headquarters:

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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router, page 7](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)
- [Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router, page 13](#)
- [Glossary, page 14](#)

Prerequisites for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

The mobile router should have the ability to obtain a CCoA on the visited network.

Restrictions for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

- If the network does not allow communication between a UDP port chosen by a mobile node and UDP port 434 on the home agent, the Mobile IP registration and the data tunneling will not work.
- Only UDP/IP encapsulation is supported.

Information About Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Before you configure the Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Access Router feature, you should understand the following concepts:

- [NAT Traversal Support Overview, page 2](#)
- [Mobile IP Support for NAT Traversal on the Mobile Router Feature Design, page 3](#)

This document uses the terms “mobile node” and “mobile router.” Most of the conceptual information in this document applies to both a mobile node and a mobile router. The term “mobile router” also applies to the Cisco 3200 Mobile Access Router. Refer to the “[Glossary](#)” section for definitions of these terms.

NAT Traversal Support Overview

Network Address Translation (NAT) is a mechanism that conserves address space by reducing the need for globally unique IP addresses. NAT is designed to allow networks with private addressing schemes to exchange traffic with public networks. However, NAT can conflict with the delivery of Mobile-IP-encapsulated traffic for a mobile node (or mobile router) that resides behind a NAT-enabled router.

In Mobile IP, usually IP-in-IP tunneling or generic routing encapsulation (GRE) tunneling allows traffic to be sent between the home agent or mobile nodes either directly or through a foreign agent. These tunneling mechanisms do not generally contain enough information to permit unique translation from the public address to the particular care-of address (CoA) of a mobile node or foreign agent that resides behind the NAT-enabled router. Specifically, there are no TCP/UDP port numbers to permit unique translation of the private CoA into the public address. Thus, the traffic from the mobile node cannot be routed even after a successful registration and will always be dropped at the NAT gateway.

NAT traversal solves this problem by using UDP tunneling as an encapsulation mechanism for tunneling Mobile IP data traffic, for both forward and reverse tunneling, between the home agent and foreign agent or between the home agent and mobile node. UDP tunneling is established by the use of new message extensions in the initial Mobile IP registration request and reply exchange that request UDP tunneling. Registration requests and replies do not use UDP tunneling.

UDP-tunneled packets that have been sent by a mobile node use the same ports as the registration request message. The source port may vary between new registration requests but remains the same for all tunneled data and reregistrations. The destination port is always 434. UDP-tunneled packets that are sent by a home agent use the same ports, but in reverse.

When the registration request packet traverses a NAT-enabled router, the home agent detects the traversal by comparing the source IP address of the packet with the CoA inside the request. If the two addresses differ, the home agent detects that a NAT gateway exists in the middle. If the home agent is configured to accept NAT traversal, it accepts the registration request and enables the use of UDP tunneling, and the data traffic passes through the NAT gateway. Thereafter, any traffic from the home agent to the mobile node is sent through the UDP tunnel. If there is a foreign agent, the foreign agent must also be configured for NAT traversal in order for UDP tunneling to work. See the [“Mobile IP Support for NAT Traversal on the Mobile Router Feature Design”](#) section for information about the scenario in which the mobile router chooses to register with the home agent using a private CCoA.

By setting the force bit in the UDP tunneling request, the mobile node or mobile router can request that Mobile IP UDP tunneling be established regardless of the NAT detection outcome by the home agent. This capability can be useful in networks that have firewalls and other filtering devices that allow TCP and UDP traffic but do not support NAT translation. The final outcome of whether the mobile node or mobile router will receive UDP tunneling is determined by whether the home agent is configured to accept such requests.

NAT devices are designed to drop the translation state after a period of traffic inactivity over the tunnel. NAT traversal support has implemented a keepalive mechanism that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel. The keepalive messages are sent to ensure that NAT keeps the state information associated with the session and that the tunnel stays open.

The keepalive timer interval is configurable on the home agent, the mobile router, and the foreign agent but is controlled by the home agent keepalive interval value sent in the registration reply. When the home agent sends a keepalive value in the registration reply, the mobile node, mobile router, or foreign agent must use that value as its keepalive timer interval.

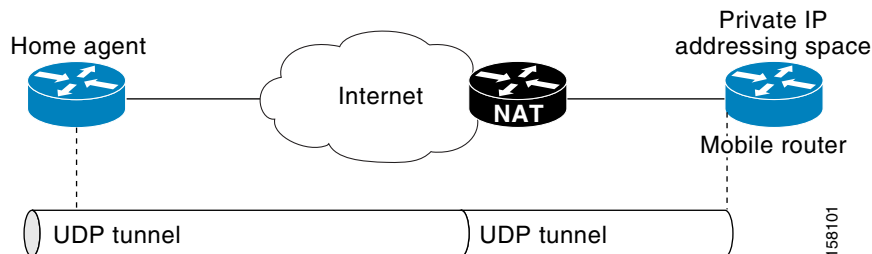
The keepalive timer interval configured on the foreign agent or mobile router is used only if the home agent returns a keepalive interval of zero in the registration reply.

Mobile IP Support for NAT Traversal on the Mobile Router Feature Design

The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature was designed for the scenario where the mobile router is behind a NAT-enabled router and needs to register directly to the home agent using a private CCoA address.

If configured for NAT traversal, the mobile router will request UDP tunneling in its registration request. If the home agent is configured for NAT traversal, the home agent will send a registration reply stating that it will accept UDP tunneling. Upon receiving this reply, the mobile router will create a UDP tunnel with the agreed-upon encapsulation type. The mobile router will also enable the periodic keepalive message between the mobile router and the home agent. If there is a keepalive failure or if there is no keepalive response from the home agent for three or more successive registration requests, the mobile router will terminate the UDP tunnel and will restart the registration process. Figure 1 shows the UDP tunnel that was set up between the home agent and the mobile router.

Figure 1 *Topology Showing the UDP Tunnel Between the Home Agent and the Mobile Router*



How to Configure the Mobile Router for RFC 3519 NAT Traversal Support

This section contains the following tasks:

- [Configuring the Mobile Router for NAT Traversal Support, page 4](#) (required)
- [Configuring the Home Agent for NAT Traversal Support, page 5](#) (required)
- [Verifying Mobile Router NAT Traversal Support, page 6](#) (optional)

Configuring the Mobile Router for NAT Traversal Support

This task shows you how to configure the mobile router for NAT traversal support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip mobile router-service collocated registration nat traversal** [*keepalive seconds*] [*force*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface FastEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 4	ip mobile router-service collocated registration nat traversal [keepalive <i>seconds</i>] [force] Example: Router(config-if)# ip mobile router-service collocated registration nat traversal keepalive 45 force	Enables NAT traversal support for the mobile router. The keywords and arguments are as follows: <ul style="list-style-type: none"> keepalive <i>seconds</i>—(Optional) Configures the keepalive interval, in seconds, that the mobile router will use when the home agent does not offer a specific value and just returns zero. The range is from 0 to 65535. The default is 110. <p>Note Setting the <i>keepalive-time</i> argument to zero disables the keepalive timer. The mobile router does not use the keepalive interval unless the home agent sends back a zero in the registration reply.</p> <ul style="list-style-type: none"> force—(Optional) Allows the mobile router to force the home agent to allocate a NAT UDP tunnel without performing detection presence of NAT along the HA-MR path. <p>Note If you configure the mobile router to force the home agent to allocate a UDP tunnel but do not configure the home agent to force UDP tunneling, the home agent will reject the forced UDP tunneling request. The decision of whether to force UDP tunneling is controlled by the home agent.</p>
Step 5	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Configuring the Home Agent for NAT Traversal Support

This task shows you how to configure the home agent for NAT traversal support.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile home-agent nat traversal** [*keepalive seconds*] [**forced** {**accept** | **reject**}]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip mobile home-agent nat traversal [<i>keepalive seconds</i>] [forced { accept reject }] Example: Router(config)# ip mobile home-agent nat traversal keepalive 45 forced accept	Enables NAT traversal support for the home agent. The keywords and argument are as follows: <ul style="list-style-type: none"> • keepalive seconds—(Optional) Time, in seconds, between keepalive messages that are sent between UDP endpoints to refresh NAT translation timers. The range is 0 to 65535. The default is 110. • forced—(Optional) Enables the home agent to accept or reject forced UDP tunneling from the mobile node regardless of the NAT-detection outcome. <ul style="list-style-type: none"> – accept—Accepts UDP tunneling. – reject—Rejects UDP tunneling. This is the default behavior.
Step 4	exit Example: Router(config)# exit	Exits global configuration mode.

Verifying Mobile Router NAT Traversal Support

Perform this task to verify mobile router NAT traversal support.

SUMMARY STEPS

1. **enable**
2. **show ip mobile binding** [**home-agent** *ip-address* | **nai string** [*session-id string*] | **summary**]
3. **show ip mobile globals**

4. `show ip mobile tunnel [interface]`
5. `show ip mobile router interface`
6. `show ip mobile router registration`
7. `show ip mobile router`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip mobile binding [home-agent ip-address nai string [session-id string] summary] Example: Router# show ip mobile binding	Displays the mobility binding on the home agent.
Step 3	show ip mobile globals Example: Router# show ip mobile globals	Displays global information for mobile agents.
Step 4	show ip mobile tunnel [interface] Example: Router# show ip mobile tunnel	Displays active tunnels.
Step 5	show ip mobile router interface Example: Router# show ip mobile router interface	Displays information about the interfaces configured for roaming.
Step 6	show ip mobile router registration Example: Router# show ip mobile router registration	Displays pending and/or accepted registrations of the mobile router.
Step 7	show ip mobile router Example: Router# show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.

Configuration Examples for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

This section provides the following configuration example:

- [Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router: Example, page 8](#)

Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router: Example

The following example shows how to configure NAT traversal between the home agent and the mobile router.

Home Agent Configuration

```
interface Loopback1
 ip address 198.168.2.1 255.255.255.255
!
router mobile
!
! The following command sets the UDP keepalive interval to 60 seconds and enables the HA
! to accept forced UDP tunneling registration requests.
!
ip mobile home-agent nat traversal keepalive 60 forced accept
ip mobile home-agent
ip mobile virtual-network 10.99.100.0 255.255.255.0
ip mobile host 10.99.100.1 10.99.100.100 virtual-network 10.99.100.0 255.255.255.0
ip mobile mobile-networks 10.99.100.2
 description MAR-3200
 register
!
ip mobile secure host 10.99.100.1 10.99.100.100 spi 100 key hex
12345678123456781234567812345678 algorithm md5 mode prefix-suffix
```

Mobile Router Configuration

```
interface Loopback1
! Description MR's home address.
ip address 10.99.100.2 255.255.255.255
!
interface FastEthernet0/0
 description Wi-Fi Link
 ip address 10.5.3.32 255.255.255.0
! The following command sets the UDP keepalive interval to 60 seconds and enables the
! mobile router to request UDP tunneling.
ip mobile router-service collocated registration nat traversal keepalive 60 force
ip mobile router-service roam priority 120
!
ip mobile router
 address 10.99.100.2 255.255.255.0
 collocated single-tunnel
 home-agent 10.1.1.1 priority 110
 mobile-network Vlan210
 reverse-tunnel
```


Additional References

The following sections provide references related to the Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature.

Related Documents

Related Topic	Document Title
Mobile IP information and configuration tasks	Cisco IOS IP Mobility Configuration Guide , Release 12.4
Mobile IP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS IP Mobility Command Reference , Release 12.4T
Information about NAT Traversal Support for Mobile IP	Mobile IP Support for RFC 3519 NAT Traversal , Cisco IOS Release 12.4 feature module
Cisco 3200 Series Mobile Access Router documentation	Cisco 3200 Series Mobile Access Router Software Configuration Guide

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. 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 commands only.

- [ip mobile router-service colocated registration nat traversal](#)

ip mobile router-service collocated registration nat traversal

To enable Network Address Translation (NAT) traversal support for the mobile router, use the **ip mobile router-service collocated registration nat traversal** command in interface configuration mode. To disable NAT traversal support for the mobile router, use the **no** form of this command.

ip mobile router-service collocated registration nat traversal [*keepalive seconds*] [*force*]

no ip mobile router-service collocated registration nat traversal [*keepalive seconds*] [*force*]

Syntax Description

keepalive seconds	(Optional) Configures the keepalive interval, in seconds, that the mobile router will use when the home agent does not offer a specific value and just returns zero. The range is from 0 to 65535. The default is 110. Note When the value zero is chosen, the keepalive timer is disabled.
force	(Optional) Allows the mobile router to force the home agent to allocate a NAT UDP tunnel without performing detection presence of NAT along the HA-MR path.

Command Default

The mobile router does not support NAT traversal.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

UDP tunneling is negotiated only when the mobile router registers to the home agent in collocated care-of address (CCoA) mode.

If you configure the mobile router to force the home agent to allocate a UDP tunnel but do not configure the home agent to force UDP tunneling, the home agent will reject the forced UDP tunneling request. The decision of whether to force UDP tunneling is controlled by the home agent.

Examples

The following example shows a mobile router configured with a keepalive timer set to 56 seconds and forced to request UDP tunneling.

```
ip mobile router-service collocated registration nat traversal keepalive 56 force
```

Related Commands

Command	Description
ip mobile home-agent nat traversal	Enables NAT traversal support for Mobile IP home agents.
ip mobile foreign-agent nat traversal	Enables NAT traversal support for Mobile IP foreign agents.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information for mobile agents.
show ip mobile tunnel	Displays information about active tunnels.
show ip mobile visitor	Displays the table that contains the visitor list of the foreign agent.

Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/fn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router

Feature Name	Releases	Feature Information
Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router	12.4(6)XE 12.4(11)T	The Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router feature extends support for NAT traversal to the mobile router when the mobile router is in private addressing space behind a NAT-enabled device and needs to register directly to the public home agent using a private CCoA. In Cisco IOS Release 12.4(11)T, the feature name changed from Mobile IP Support for RFC 3519 NAT Traversal on the Cisco 3200 Mobile Router to Mobile IP Support for RFC 3519 NAT Traversal on the Mobile Router.

Glossary

agent advertisement—An advertisement message constructed by an attachment of a special extension to an ICMP Router Discovery Protocol (IRDP).

care-of address—The termination point of the tunnel to a mobile node or mobile router. This can be a collocated care-of address, by which the mobile node or mobile router acquires a local address and detunnels its own packets, or a foreign agent care-of address, by which a foreign agent detunnels packets and forwards them to the mobile node or mobile router.

CDPD—cellular digital packet data. Open standard for two-way wireless data communication over high-frequency cellular telephone channels. Allows data transmissions between a remote cellular link and a NAP. Operates at 19.2 kbps.

foreign agent—A router on the visited network of a foreign network that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers packets to the mobile node or mobile router that were tunneled by the home agent of the mobile node. For packets sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

GPRS—general packet radio service. A service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for Global System for Mobile Communications (GSM) networks.

home agent—A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while they are away from home. It keeps current location information for registered mobile nodes called a *mobility binding*.

home network—The network, possibly virtual, whose network prefix equals the network prefix of the home address of a mobile node.

mobile network—A network that moves with the mobile router. A mobile network is a collection of hosts and routes that are fixed with respect to each other but are mobile, as a unit, with respect to the rest of the Internet.

mobile node—A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming that link-layer connectivity to a point of attachment is available.

mobile router—A mobile node that is a router. It provides for the mobility of one or more entire networks moving together, perhaps on an airplane, a ship, a train, an automobile, a bicycle, or a kayak. The nodes connected to a network served by the mobile router may themselves be fixed nodes or mobile nodes or routers.

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. Registration may happen directly from the mobile node to the home agent or through a foreign agent.

tunnel—The path followed by a packet while it is encapsulated from the home agent to the mobile node. The model is that, while it is encapsulated, a packet is routed to a knowledgeable de-encapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.

