Mobile IP Support for RFC 3519 NAT Traversal

The Mobile IP: Support for RFC 3519 NAT Traversal feature introduces an alternative method for tunneling Mobile IP data traffic. New extensions in the Mobile IP registration request and reply messages have been added for establishing User Datagram Protocol (UDP) tunneling.

The benefit of this feature is that mobile devices in collocated mode that use a private IP address (RFC 1918) or foreign agents (FAs) that use a private IP address for the care-of address (CoA) are now able to establish a tunnel and traverse a NAT-enabled router with mobile node (MN) data traffic from the home agent (HA).

Feature History for Mobile IP: Support for RFC 3519 NAT Traversal

Release	Modification
12.3(8)T	This feature was introduced.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

Restrictions for Mobile IP Support for RFC 3519 NAT Traversal

- If the network does not allow communication between a UDP port chosen by an MN and the HA UDP port 434, the Mobile IP registration and the data tunneling will not work.
- Only the IP-to-UDP encapsulation method is supported.

Information About Mobile IP Support for RFC 3519 NAT Traversal

Design of the Mobile IP Support for RFC 3519 NAT Traversal Feature

Because of the depletion of globally routable addresses, service providers and enterprises are using addresses from private- and public-address realms and are using NAT-based solutions for achieving transparent routing between these address realms. Private IP addresses (RFC 1918) allow each enterprise to use the same addresses except that the addresses cannot be seen in the Internet outside of the enterprise or service provider network.

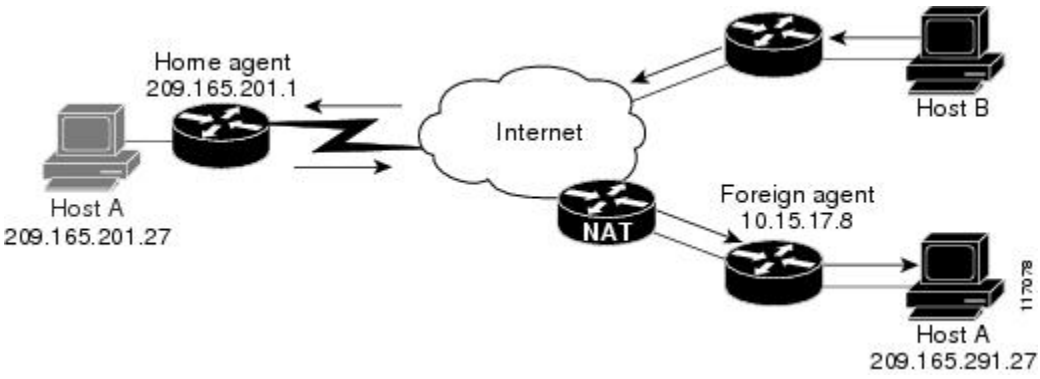
Network Address Translation (NAT) allows for the translation of a private IP address to a public IP address. NAT uses the port number in the second header to organize the translations and determine which translation (if any) to use when it sees a returning packet.

The Mobile IP: Support for RFC 3519 NAT Traversal feature uses new message extensions in registration packets to establish UDP tunneling. When the MN registration packet traverses a NAT-enabled router, the HA detects the traversal by comparing the source IP address with the CoA and establishes UDP tunneling if the MN indicates that it is capable of UDP tunneling. The MN indicates the UDP tunneling capability by including the UDP tunneling extension in the registration request.

The NAT-enabled router allows the UDP registration packet to proceed through. UDP tunneling allows data packets from the HA to use the NAT translation set up by the registration packet. This occurs because the UDP tunnel header uses the same UDP source and destination port as the original registration packet, thus allowing it to use the NAT translation created for and by the registration packet traversing the NAT-enabled router. This allows the MN to receive data packets from the HA when it normally would not with the default IPinIP tunneling.

The figure below shows Mobile IP components and their relationships.

Figure 1: Mobile IP Components and Relationships



Note UDP tunneling is the only method that supports NAT traversal in Mobile IP.

Network Address Translation Devices

Network Address Translation (NAT) devices rely on IP addresses and port numbers from IP, TCP, and UDP layers for demultiplexing data to peers behind a NAT network. When a message is initiated from a private-address host to a public-address host, NAT modifies the source IP address in the packet to a globally routable source address and the source port number to a unique source port number that it can use for identifying the peer that initiates the message. NAT then preserves the private address, port-to-public address, and port mapping in its translation table and uses the NAT-translation entry to route the return traffic.

The Mobile IP: Support for RFC 3519 NAT Traversal feature provides UDP tunneling for data packets so that NAT devices can translate the IP addresses and forward the data packets from the HA to the MN.

UDP Tunneling

There are two directions for UDP tunneling: forward and reverse. Forward tunneling is done by an HA that forwards packets towards the MN, and reverse tunneling starts at the MN care-of address and terminates at the HA.

UDP tunneled packets that have been sent by an MN use the same ports as the registration request message. In particular, 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 an HA use the same ports, but in reverse.

Note UDP tunneling is for Mobile IP data traffic only. Registration requests and replies do not use UDP tunneling.

By setting the force bit in the UDP tunneling request, the MN can request Mobile IP UDP tunneling be established regardless of the NAT detection outcome by the HA. The final outcome of whether or not the MN will receive UDP tunneling is determined by whether or not the HA is configured to accept such requests.

Keepalive Management

The purpose of the keepalive messages is to refresh the active timer on the NAT translation in the NAT-enabled router. This maintains the NAT translation for use by the HA even when the MN is silent. This allows data packets from the HA to use the NAT translation created by the registration packet to traverse the NAT-enabled router and reach the MN even when the MN may not be sending any packets to the HA to keep the NAT translation active.

The keepalive timer interval is configurable on both the HA and the FA but is controlled by the HA keepalive interval value sent in the registration reply. When the HA sends a keepalive value in the registration reply, the MN or FA must use that value as its keepalive timer interval.

The keepalive interval configured on the FA is only used if the HA returns a keepalive interval of zero in the registration reply.

Note You cannot configure the HA to send a keepalive interval value of zero the FA or MN.

New Message Extensions

An extension is added to the end of a registration packet and indicates that it is a type, length, value (TLV) message. RFC 3519 discusses the UDP tunnel request and reply extension and a Mobile IP tunnel data message that serves to differentiate traffic tunneled to port 434.

The Mobile IP--Support for RFC 3519 NAT Traversal feature adds the following new UDP tunnel message extensions:

- Request--This message extension indicates that the sender is capable of handling UDP tunneling. Some encapsulation formats are optional.
- Reply--This message extension indicates whether or not the HA will use UDP tunneling. The HA also sends the keepalive interval in the reply message.
- Mobile IP tunnel data--This message extension is used to differentiate UDP data traffic tunneled to port 434 from other Mobile IP messages that use a UDP header such as registration requests.

UDP Tunnel Flag

The Mobile IP--Support for RFC 3519 NAT Traversal feature adds a new UDP tunnel flag in the agent advertisement that indicates the capability of the FA to support NAT traversal. The flag is a bit set in the advertisement.

How to Configure Mobile IP Support for RFC 3519 NAT Traversal

Configuring the Home Agent for NAT Traversal Support

SUMMARY STEPS

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

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 mobile home-agent nat traversal [keepalive keepalive-time] [forced {accept | reject}]** **Example:** `Router(config)# ip mobile home-agent nat traversal keepalive 45 forced accept`	Enables UDP tunneling for an HA. The keywords and argument are as follows: • **keepalive** *keepalive-time* --(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. You cannot configure the HA to send a zero as the keepalive timer to the FA or MN. • **forced** --(Optional) Enables the HA to accept or reject forced UDP tunneling from the MN regardless of the NAT-detection outcome. • **accept**--Accepts UDP tunneling. • **reject**--Rejects UDP tunneling. This is the default. **Note** If the **forced** keyword is not specified, the command defaults to reject UDP tunneling.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the Foreign Agent for NAT Traversal Support

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**]
4. **exit**

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 mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**] **Example:** `Router(config)# ip mobile foreign-agent nat traversal keepalive 45 force`	Enables UDP tunneling for the FA. The keywords and argument are as follows: • **keepalive** *keepalive-time* --(Optional) Allows the FA to use a configured time (in seconds) for keepalive messages when the HA keepalive time is not configured. The range is 0 to 65535. The default is 110. **Note** The Cisco HA will never send a time of zero. If you have Cisco hardware only, you do not need to configure the **keepalive** keyword.

	Command or Action	Purpose
		• **force** --(Optional) Sets the "force" bit in the message extension. The default is not to force UDP tunneling.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying NAT Traversal Support

SUMMARY STEPS

1. **show ip mobile globals**
2. **show ip mobile binding**
3. **show ip mobile visitor**
4. **show ip mobile tunnel**
5. **debug ip mobile**

DETAILED STEPS

Step 1 **show ip mobile globals**

Use this command to verify the FA and HA configurations, for example:

Example:

```
Router# show ip mobile globals
IP Mobility global information:
Home agent
 Registration lifetime: 10:00:00 (36000 secs)
 Broadcast disabled
 Replay protection time: 7 secs
 Reverse tunnel enabled
 ICMP Unreachable enabled
 Strip realm disabled
 NAT Traversal disabled
 HA Accounting disabled
 NAT UDP Tunneling support enabled
 UDP Tunnel Keepalive 60
 Forced UDP Tunneling enabled
 Virtual networks
 10.99.101.0/24
Foreign agent is not enabled, no care-of address
0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
```

In the example above, NAT UDP tunneling support is enabled on the HA with a keepalive timer set at 60 seconds and forced UDP tunneling enabled.

Step 2 **show ip mobile binding**

Use this command to verify that the HA is configured to detect NAT, for example:

Example:

```
Router# show ip mobile binding nai mn@cisco.com
Mobility Binding List:
 mn@cisco.com (Bindings 1):
 Home Addr 10.99.101.1
 Care-of Addr 192.168.1.202, Src Addr 209.165.157
 Lifetime granted 00:03:00 (180), remaining 00:02:20
 Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
 Tunnel0 src 209.165.202.1 dest 209.165.157 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Service Options:
 NAT detect
```

Step 3 **show ip mobile visitor**

Use this command to verify that the MN is registering with the HA (at the FA), for example:

Example:

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
10.99.100.2:
 Interface FastEthernet3/0, MAC addr 00ff.ff80.002b
 IP src 10.99.100.2, dest 30.5.3.5, UDP src port 434
 HA addr 200.1.1.1, Identification BCE7E391.A09E8720
 Lifetime 01:00:00 (3600) Remaining 00:30:09
 Tunnel1 src 200.1.1.5, dest 200.1.1.1, reverse-allowed
 Routing Options - (T)Reverse Tunneling
```

Step 4 **show ip mobile tunnel**

Use this command to verify that UDP tunneling is established, for example:

Example:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
    src 10.30.30.1, dest 10.10.10.100
    src port 434, dest port 434
    encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/3
    FA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    7 packets output, 780 bytes
```

The following output shows that the mobile node-home agent tunnel is still IP-in-IP, but the foreign agent-home agent tunnel is UDP, for example:

Example:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
 src 200.1.1.1, dest 10.99.100.2
 encap IP/IP
, mode reverse-allowed, tunnel-users 1
 IP MTU 1460 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Tunnel1
 HA created, fast switching enabled, ICMP unreachable enabled
 11 packets input, 1002 bytes, 0 drops
 5 packets output, 600 bytes
Tunnel1:
 src 200.1.1.1, dest 200.1.1.5
 src port 434, dest port 434
 encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface GigabitEthernet0/2
 HA created, fast switching disabled, ICMP unreachable enabled
 11 packets input, 1222 bytes, 0 drops
 7 packets output, 916 bytes
```

In the following example, the MN has UDP tunneling established with the HA, for example:

Example:

```
Router# show ip mobile tunnel
Total mobile ip tunnels 1
Tunnel0:
    src 10.10.10.100, dest 10.10.10.50
    src port 434, dest port 434
    encap MIPUDP/IP
, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/1
    HA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    5 packets output, 600 bytes
```

Step 5 **debug ip mobile**

Use this command to verify the registration, authentication, and establishment of UDP tunneling of the MN with the FA (important lines in bold), for example:

Example:

```
Dec 31 12:34:25.707: UDP: rcvd src=10.10.10.10(434),dst=10.30.30.1(434), length=54
Dec 31 12:34:25.707: MobileIP: ParseRegExt type MHAE(32) addr 2000FEEC end 2000FF02
Dec 31 12:34:25.707: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.707: MobileIP: FA rcv registration for MN 10.10.10.10
 on Ethernet2/2 using  COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options sbdmg-T-identification
  C1BC0D4FB01AC0D8
Dec 31 12:34:25.707: MobileIP: Ethernet2/2 glean 10.10.10.10 accepted
Dec 31 12:34:25.707: MobileIP: Registration request byte count = 74
Dec 31 12:34:25.707: MobileIP: FA queued MN 10.10.10.10 in register table
Dec 31 12:34:25.707: MobileIP: Visitor registration timer started for MN 10.10.10.10,  lifetime 120
Dec 31 12:34:25.707: MobileIP: Adding UDP Tunnel req extension
Dec 31 12:34:25.707: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.707: MobileIP: MN 10.10.10.10 FHAE added to HA 10.10.10.100 using SPI 1000
```

```
Dec 31 12:34:25.707: MobileIP: FA forwarded registration for MN 10.10.10.10 to HA  10.10.10.100
Dec 31 12:34:25.715: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=94
Dec 31 12:34:25.715: MobileIP: ParseRegExt type NVSE(134) addr 20010B28 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MN-config NVSE(14) subtype 1 (MN prefix  length)
prefix length (24)
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 12 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type MHAE(32) addr 20010B36 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type UDPTUNREPE(44) addr 20010B4C end 20010B6A
Dec 31 12:34:25.715: Parsing UDP Tunnel Reply Extension - length 6
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:25.715: MobileIP: ParseRegExt type FHAE(34) addr 20010B54 end 20010B6A
Dec 31 12:34:25.715: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:25.715: MobileIP: FA rcv accept (0) reply for MN 10.10.10.10 on Ethernet2/3  using HA
10.10.10.100 lifetime 65535
Dec 31 12:34:25.719: MobileIP: Authenticating HA 10.10.10.100 using SPI 1000
Dec 31 12:34:25.719: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:25.719: MobileIP: Authenticated HA 10.10.10.100 using SPI 1000 and 16 byte  key
Dec 31 12:34:25.719: MobileIP: HA accepts UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Update visitor table for MN 10.10.10.10
Dec 31 12:34:25.719: MobileIP: Enabling UDP Tunneling
Dec 31 12:34:25.719: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.30.30.1 dst  10.10.10.100
Dec 31 12:34:25.719: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.30.30.1:0 -
10.10.10.100:0 with keep-alive 30
Dec 31 12:34:25.719: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:25.719: MobileIP: ARP entry for MN 10.10.10.10 using 10.10.10.10 inserted on  Ethernet2/2
Dec 31 12:34:25.719: MobileIP: FA route add 10.10.10.10 successful. Code = 0
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 added to ReverseTunnelTable of Ethernet2/2  (Entries
1)
Dec 31 12:34:25.719: MobileIP: FA dequeued MN 10.10.10.10 from register table
Dec 31 12:34:25.719: MobileIP: MN 10.10.10.10 using 10.10.10.10 visiting on Ethernet2/2 Dec 31
12:34:25.719: MobileIP: Reply in for MN 10.10.10.10 using 10.10.10.10, accepted
Dec 31 12:34:25.719: MobileIP: registration reply byte count = 84
Dec 31 12:34:25.719: MobileIP: FA forwarding reply to MN 10.10.10.10 (10.10.10.10 mac  0060.70ca.f021)
Dec 31 12:34:26.095: MobileIP: agent advertisement byte count = 48
Dec 31 12:34:26.095: MobileIP: Agent advertisement sent out Ethernet2/2: type=16, len=10,  seq=55,
lifetime=65535, flags=0x1580(rbhFmG-TU),
Dec 31 12:34:26.095: Care-of address: 10.30.30.1
Dec 31 12:34:26.719: MobileIP: swif coming up Tunnel0
!
Dec 31 12:34:35.719: UDP: sent src=10.30.30.1(434), dst=10.10.10.100(434)
Dec 31 12:34:35.719: UDP: rcvd src=10.10.10.100(434), dst=10.30.30.1(434), length=32d0
```

In the following example, the registration, authentication, and establishment of UDP tunneling of the MN with the HA is displayed:

Example:

```
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type UDPTUNREQE(144)
addr 2001E762 end 2001E780
Dec 31 12:34:26.167: MobileIP: Parsing UDP Tunnel Request Extension - length 6
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 6 to next
Dec 31 12:34:26.167: MobileIP: ParseRegExt type FHAE(34) addr 2001E76A end 2001E780
Dec 31 12:34:26.167: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.167: MobileIP: HA 167 rcv registration for MN 10.10.10.10 on Ethernet2/1  using
HomeAddr 10.10.10.10 COA 10.30.30.1 HA 10.10.10.100 lifetime 65535 options  sbdmg-T-identification
C1BC0D4FB01AC0D8
Dec 31 12:34:26.167: MobileIP: NAT detected SRC:10.10.10.50 COA: 10.30.30.1
Dec 31 12:34:26.167: MobileIP: UDP Tunnel Request accepted 10.10.10.50:434
Dec 31 12:34:26.167: MobileIP: Authenticating FA 10.30.30.1 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticated FA 10.30.30.1 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authenticating MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.167: MobileIP: Authentication algorithm MD5 and 16 byte key
```

```
Dec 31 12:34:26.167: MobileIP: Authenticated MN 10.10.10.10 using SPI 1000 and 16 byte key
Dec 31 12:34:26.167: MobileIP: Mobility binding for MN 10.10.10.10 created
Dec 31 12:34:26.167: MobileIP: NAT detected for MN 10.10.10.10. Terminating tunnel on  10.10.10.50
Dec 31 12:34:26.167: MobileIP: Tunnel0 (MIPUDP/IP) created with src 10.10.10.100 dst  10.10.10.50
Dec 31 12:34:26.167: MobileIP: Setting up UDP Keep-Alive Timer for tunnel 10.10.10.100:0 -
10.10.10.50:0 with keep-alive 30
Dec 31 12:34:26.167: MobileIP: Starting the tunnel keep-alive timer
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 Insert route for 10.10.10.10/255.255.255.255  via
gateway 10.10.10.50 on Tunnel0
Dec 31 12:34:26.167: MobileIP: MN 10.10.10.10 is now roaming
Dec 31 12:34:26.171: MobileIP: Gratuitous ARPs sent for MN 10.10.10.10 MAC 0002.fca5.bc39
Dec 31 12:34:26.171: MobileIP: Mask for address is 24
Dec 31 12:34:26.171: MobileIP: HA accepts registration from MN 10.10.10.10
Dec 31 12:34:26.171: MobileIP: Dynamic and Static Network Extension Length 0 - 0
Dec 31 12:34:26.171: MobileIP: Composed mobile network extension length:0
Dec 31 12:34:26.171: MobileIP: Added prefix length vse in reply
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 MHAE added to MN 10.10.10.10 using SPI 1000
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 FHAE added to FA 10.10.10.50 using SPI 1000
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 - HA sent reply to 10.10.10.50
Dec 31 12:34:26.171: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.171: MobileIP: MN 10.10.10.10 HHAE added to HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: ParseRegExt type CVSE(38) addr 2000128C end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HA red. version CVSE(6)
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 8 to next
Dec 31 12:34:26.175: MobileIP: ParseRegExt type HHAE(35) addr 20001298 end 200012AE
Dec 31 12:34:26.175: MobileIP: ParseRegExt skipping 20 to next
Dec 31 12:34:26.175: MobileIP: Authenticating HA 10.10.10.3 using SPI 1000
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and truncated key
Dec 31 12:34:26.175: MobileIP: Authentication algorithm MD5 and 16 byte key
Dec 31 12:34:26.175: MobileIP: Authenticated HA 10.10.10.3 using SPI 1000 and 16 byte key
Dec 31 12:34:27.167: MobileIP: swif coming up Tunnel0d0
```

In the following example, the force option is missing on the HA configuration, so the UDP tunneling request is rejected:

Example:

```
Router# debug ip mobile
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type NVSE(134) addr C368C6C
end C368
C9C
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type dynamic mobile-network
NVSE(9)
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 16 to next
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type MHAE(32) addr C368C7E
end C368C9C
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 20 to next
*Jun 6 20:49:28.147: MobileIP: ParseRegExt type UDPTUNREQE(144) addr
C368C94 end C368C9C
*Jun 6 20:49:28.147: MobileIP: Parsing UDP Tunnel Request Extension -
length 6
*Jun 6 20:49:28.147: MobileIP: ParseRegExt skipping 6 to next
*Jun 6 20:49:28.147: MobileIP: HA 143 rcv registration for MN
10.99.100.2 on Gi
gabitEthernet0/2 using HomeAddr 10.99.100.2 COA 200.1.1.5 HA 200.1.1.1
lifetime
3600 options sbdmg-T- identification BCE7E253A7CAF30C
*Jun 6 20:49:28.147: MobileIP: NAT not detected SRC:200.1.1.5 COA:
200.1.1.5
*Jun 6 20:49:28.147: MobileIP: Forced UDP Tunneling requested
*Jun 6 20:49:28.147: MobileIP: UDP Tunnel Request rejected
*Jun 6 20:49:28.147: MobileIP: HA rejects registration for MN
10.99.100.2 - registration id mismatch (133)
```

Configuration Examples for Mobile IP Support for RFC 3519 NAT Traversal

Home Agent Configuration Examples

The following example shows an active HA configuration.

```
ip mobile home-agent nat traversal keepalive 56 forced accept
ip mobile home-agent redundancy Phy1 virtual-network
ip mobile virtual-network 10.60.60.0 255.255.255.0 address 10.60.60.200
```

The following example shows a standby HA configuration.

```
ip mobile home-agent nat traversal keepalive 56 forced accept
ip mobile home-agent redundancy Phy1 virtual-network
ip mobile virtual-network 10.60.60.0 255.255.255.0 address 10.60.60.200
```

Foreign Agent Configuration Example

The following example shows the FA configuration on Ethernet interface 2/2. The FA does not use the 45-second keepalive interval unless the HA sends back a zero as the interval in the registration reply.

```
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent nat traversal keepalive 45 force
```

Firewall Configuration Example

The following example shows a configuration when a firewall is sitting between a FA and a HA. The firewall blocks IP-in-IP and GRE packets, but permits UDP packets. The HA and FA are configured to force the HA to use the UDP encapsulation.

HA Configuration

```
interface Loopback1
ip address 200.1.1.1 255.255.255.255
!
router mobile
!
! The following command set UDP keepalive interval to 60 second 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
```

Foreign Agent Configuration

```
interface Loopback1
ip address 10.1.1.5 255.255.255.255
!
interface FastEthernet3/0
ip address 10.5.3.5 255.255.255.0
ip irdp
ip irdp maxadvertinterval 9
ip irdp minadvertinterval 3
ip irdp holdtime 27
ip mobile foreign-service reverse-tunnel
!
ip mobile foreign-agent care-of Loopback1
!
! The following command forces the FA to request the HA to use UDP tunneling for MN. Without
 this command, the HA is configured to accept UDP tunneling. The HA will not use UDP tunneling
 if it is not NAT detected.
ip mobile foreign-agent nat traversal force
```

Mobile Router Configuration

```
interface Loopback1
!Description MR's home address.
ip address 10.99.100.2 255.255.255.255
!
interface FastEthernet0/0
description "802.11 Wi-Fi Link"
ip address 10.5.3.32 255.255.255.0
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
```

Cisco IOS Firewall

In the following example, an IP access-list is used to simulate the blocking of IP-in-IP and GRE packets.

```
!Input interface for the traffic coming from MR.
interface FastEthernet0/1
ip address 10.1.35.3 255.255.255.0
ip access-group Block-IPinIP-GRE-Packets in
!
ip access-list extended Block-IPinIP-GRE-Packets
deny ipinip any any
deny gre any any
permit ip any any
```

Additional References

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

Related Documents

Related Topic	Document Title
Generic routing encapsulation	Generic Routing Encapsulation, RFC 1701

Related Topic	Document Title
IP encapsulation	IP Encapsulation in IP, RFC 2003
Mobile IP overview and configuration	*"Configuring Mobile IP" chapter of the* Cisco IOS IP Configuration Guide , Release 12.3
Mobile IP traversal of NAT devices	Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519
Mobile IP command description and syntax	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3 T
NAT and Network Address Port Translation (NAPT) overview and configuration	• *"Configuring IP Addressing" chapter of the* Cisco IOS IP Configuration Guide , Release 12.3 • Cisco IOS IP Command Reference, Volume 1 of 4: IP Addressing and Services , Release 12.3 T • IP NAT Terminology and Considerations, RFC 2663 • Network Address Translation - Protocol Translation, RFC 2766

Standards

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

MIBs

MIBs	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

RFCs	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
Technical Assistance Center (TAC) home page, containing 30,000 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/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **debug ip mobile**
- **ip mobile foreign-agent nat traversal**
- **ip mobile home-agent nat traversal**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile tunnel**
- **show ip mobile visitor**

Glossary

care-of address--There are two types of care-of addresses: FA care-of addresses and collocated care-of addresses. An FA care-of address is a temporary, loaned IP address that an MN acquires from an FA agent advertisement. It is the exit point of the tunnel from the HA to the FA. A collocated care-of address is an address temporarily assigned to an MN interface that is assigned by DHCP or by manual configuration.

FA --foreign agent. An FA is a router on a foreign network that assists the MN in informing its HA of its current care-of address. The FA detunnels and delivers packets to the MN that were tunneled by the HA. The FA also acts as the default router for packets generated by the MN while it is connected to the foreign network.

forward tunnel --A tunnel that forwards packets toward the mobile node. It starts at the home agent and ends at the MN care-of address.

HA --home agent. An HA is a router on the home network of an MN that maintains an association between the home IP address of the MN and its *care-of address* , which is the current location of the MN on a foreign or visited network. The HA redirects packets by tunneling them to the MN while it is away from home.

MN --mobile node. An MN is a node, for example, a PDA, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This node can maintain ongoing communications while using only its home IP address.

NAT --Network Address Translation. NAT is a mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator. Basic NAT is a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, the source IP address and related fields such as IP, TCP, UDP, and ICMP header checksums are translated. For inbound packets, the destination IP address and the checksums as listed above are translated.

NAPT --Network Address Port Translation. NAPT translates transport identifier (for example, TCP and UDP port numbers, ICMP query identifiers). This allows the transport identifiers of a number of private hosts to be multiplexed into the transport identifiers of a single external address. NAPT allows a set of hosts to share a single external address. Note that NAPT can be combined with basic NAT so that a pool of external addresses are used in conjunction with port translation.

reverse tunnel --A tunnel that starts at the MN care-of address and terminates at the HA.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.