



MIP NAT Traversal

This chapter describes support for MIP NAT traversal and how to enable it on the system. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.



Important

Use of MIP NAT traversal requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

- [Overview, on page 1](#)
- [Enabling MIP NAT Traversal, on page 3](#)

Overview

If a Mobile Node (MN) supports Mobile IP Network Address Translation (MIP NAT) traversal, it can indicate to the Home Agent (HA) that it is able to use MIP UDP tunneling when the HA sees that the Registration Request (RRQ) has traversed a NAT device.

The HA determines that the RRQ has passed through a NAT device by comparing the care-of-address in the RRQ with the source IP address of the RRQ. If they are different, and the D bit is set in the RRQ, then it indicates that the RRQ has passed through a NAT device.

If NAT is not detected but the Force (F) bit is set in the RRQ along with a UDP Tunnel Request, the HA rejects the call with the code 129 in the Registration Response (RRP). You can configure a parameter to force the HA to accept these types of requests for UDP tunneling in the absence of NAT.

When the D bit is not set and a mismatch occurs between the source address and the care-of-address, this could be a case when a mobile is registering through an FA using different addresses for signaling and data traffic. This registration behavior is allowed by the HA service.

The MN and HA negotiate UDP tunneling support during Mobile IP call setup. The MN includes a UDP Tunnel Request Extension in the RRQ sent to the HA. This extension optionally specifies the encapsulation type to be used as well (IP, GRE, or Minimal IP). The system only supports IP encapsulation at this time. Note also that the D bit must be set when UDP Tunneling is requested.

If the HA supports the requested form of tunneling, and the registration is successful, it responds with a UDP Tunnel Reply Extension in the RRP and specifies the keepalive interval the MN should use.

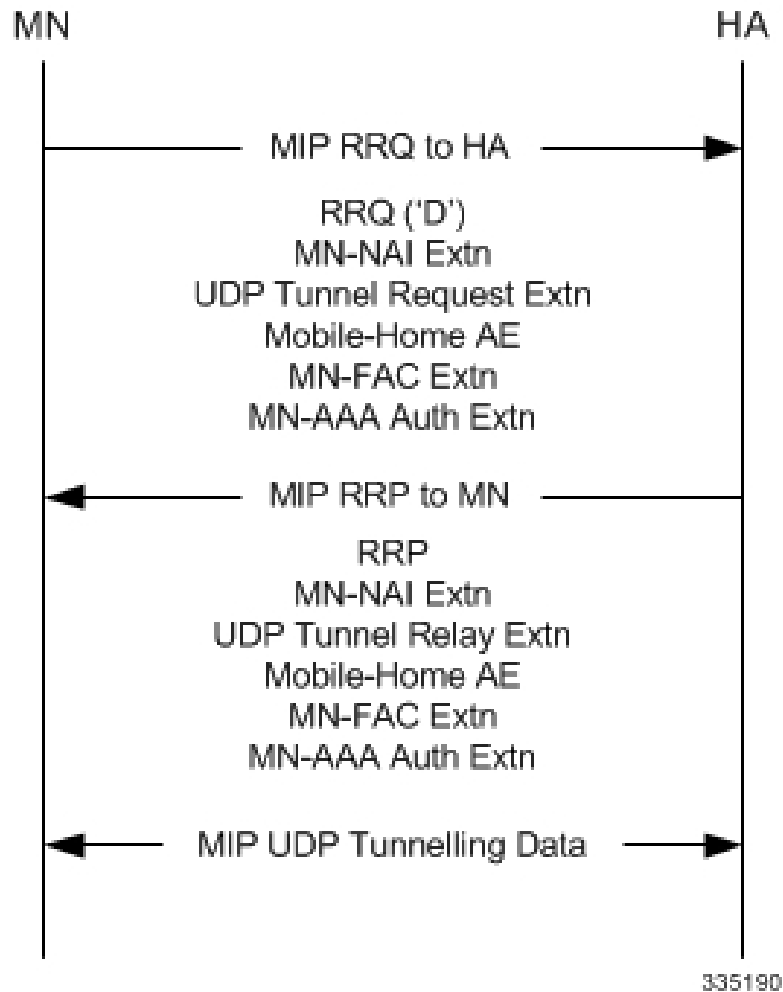
If HA does not accept the requested type of UDP tunneling, it ignores the UDP Tunnel Request extension and does not include the UDP Tunnel Reply extension in the Registration Reply. Error code 142 is used in the RRP to indicate to the MN that the requested UDP tunnel encapsulation is unavailable.

The UDP Tunnel Request extension is included in all initial, renewal, and handoff RRQ and RRP messages. The UDP Tunnel Request extension is not included in a Deregistration RRQ from the MN and the HA ignores them if they are included in Dereg RRQs received.

When MIP NAT Traversal is used, normally reverse tunneling is also used. However, this is not required by the HA.

An example of successful MIP UDP Tunneling negotiation is shown below.

Figure 1: MIP UDP Tunneling negotiation between MN and HA



The following table lists the various cases possible in UDP Tunneling negotiation during Mobile IP call establishment.

Table 1: MIP UDP Tunneling Negotiation Cases

Case	RRQ received at the HA	Action at HA
1	NAT detected, UDP Tunnel Request sent, NAT Traversal enabled	Accept call with IP-UDP tunneling, UDP Tunnel Reply included in RRP
2	NAT detected, UDP Tunnel Request sent, NAT Traversal disabled at the HA	Reject with code 129
3	NAT not detected, UDP Tunnel Request sent, F bit not set	Accept call with IP-IP tunneling, UDP Tunnel Reply not included
4	NAT not detected, UDP Tunnel Request sent, F bit set, forced UDP tunnel NOT allowed	Reject with code 129
5	NAT not detected, UDP Tunnel Request sent, F bit set, forced UDP tunnel allowed	Accept call with IP-UDP tunneling, UDP Tunnel Reply included in RRP
6	UDP Tunnel Request sent, D bit not set	Reject with code 134
7	NAT detected, UDP Tunnel Request not sent	Reject with code 129

Enabling MIP NAT Traversal

MIP NAT traversal must be enabled for the desired HA service on the system.



Important

Commands used in the configuration samples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

To enable MIP NAT traversal, set parameters by applying the following example configuration:

```
configure
context <context_name>
ha-service <name>
nat-traversal
end
```

Notes:

- Optionally, you can configure the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request by entering the following command: **nat-traversal force-accept**

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Viewing MIP NAT Traversal Statistics

Use the following commands in **exec mode** to list statistics that include information about MIP NAT Traversal:

- **monitor {protocol | subscriber}**- Use the MIP Tunnel option to trace IP-UDP tunneled datagrams.
- **show ha-service service_name** - Shows the MIP NAT Traversal configuration for the specified HA service.
- **show mipha statistics** - Lists IP-UDP tunnel statistics for Home Agent calls specified.
- **show mipha full** - Displays NAT, UPD, and encapsulation information for Home Agent calls specified.
- **show subscribers full** - Displays NAT, UPD, and encapsulation information for the subscribers specified.
- **{show | clear} subscribers ccoa-only** - Show or clear sessions for subscribers that registered a MIP colocated COA directly with the HA.
- **{show | clear} subscribers mip-udp-tunnel-only** - Show or clear sessions for subscribers that negotiated MIP UDP tunneling with the HA.

Refer to *Exec Mode Commands* chapter in the *Command Line Interface Reference* for details on using these commands.