Network Mobility (NEMO)

This chapter describes the system's support for NEMO and explains how it is configured. 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 *Cisco ASR 5500 Packet Data Network Gateway Administration Guide*, before using the procedures in this chapter.

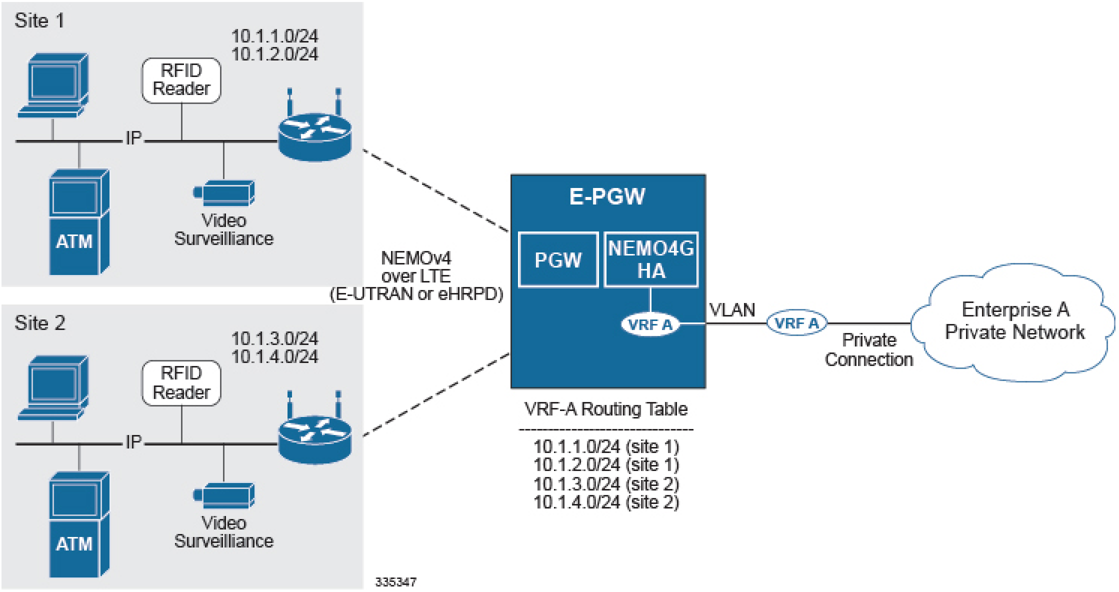
NEMO Overview

When enabled through a feature license key, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the P-GW platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

The following figure shows a high-level view of LTE NEMOv4 Architecture.

Figure 1: NEMO Overview



Use Cases

The following use cases are supported by NEMO in LTE:

1. **Stationary** - Applications, like branch offices, with a mobile router that does not require mobility.
2. **Nomadic** - Applications that use a mobile router that does not move while in service, but that may be moved to a different location and brought back on service (e.g. a kiosk showing up in a mall one day and in a different location the next day or month).
3. **Moveable** - Applications that need to maintain Dynamic Mobile Network Routing (DMNR) service operational while moving and crossing PDSN boundaries, such as public safety vehicles. Service continuity is handled by the mobility protocols (Mobile IP in 3G and GTP in LTE).

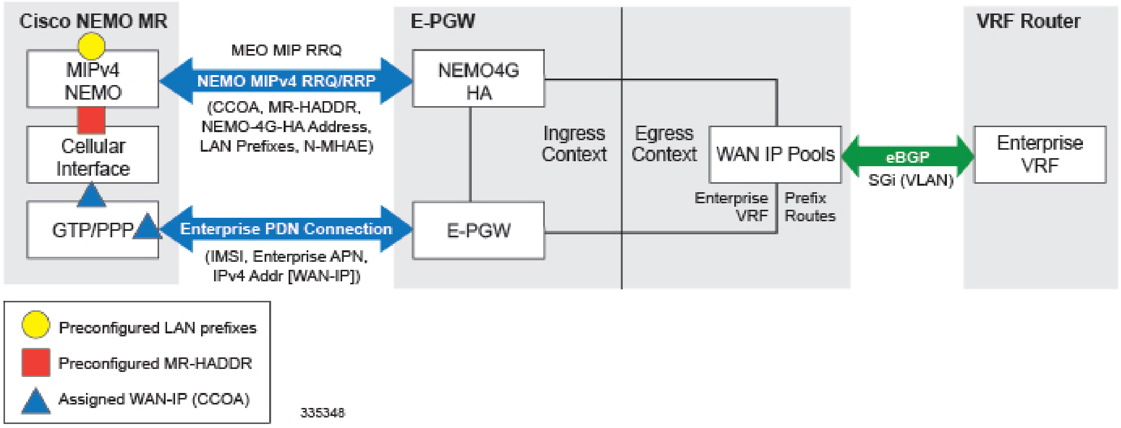
Features and Benefits

The system supports the usage of dynamically learned, overlapping customer prefixes. These prefixes are advertised via BGP.

MIPv4-based NEMO Control Plane

The following figure shows a high-level view of the NEMO control plane.

Figure 2: NEMO Control Plane



NEMO includes the following features:

- Collocated-Care-of-Address mode

  The Cisco NEMO MR is expected to use the Collocated-Care-of-Address mode to establish a NEMO MIPv4 session with NEMO4G-HA and as one of the IP endpoints of the NEMO GRE Tunnel for the transport of user traffic.

- MR-HADDR

  NEMO4G-HA supports a potential "dummy" MR-HADDR address that would be configured in every MR within the same Enterprise or across all served Enterprises (same IP address).

- Dynamic advertisement of WAN-IP Pools and learned LAN prefixes

  eBGP is used to advertise the Enterprise WAN-IP Pools and the LAN prefixes learned via NEMO for the associated Enterprise.

- N-MHAE credentials

  NEMO4G-HA supports local authentication for the NEMO MIPv4 RRQ based on preconfigured N-MHAE-SPI/KEY values on a per Enterprise basis (one unique set for all MRs belonging to the same Enterprise) or on a global basis (one unique set for all Enterprises).

- LAN prefixes
  - NEMO4G-HA accepts a minimum of zero LAN prefixes and a maximum of eight prefixes per mobile router. Anything beyond eight prefixes shall be silently discarded.
  - NEMO4G-HA supports any prefix length (including /32).
  - NEMO4G-HA supports dynamic prefix updates.
    - NEMO4G-HA removes from the associated Enterprise VRF routing table any prefixes that are not included in a scheduled or ad-hoc NEMO MIPv4 re-registration request from a given MR (assuming these were present in a previous NEMO MIPv4 RRQ). E-PGW shall update the external VRF router of the removal of such prefixes on the next eBGP update.
    - NEMO4G-HA accepts and installs any new prefixes that are included in a scheduled or ad-hoc NEMO MIPv4 re-registration request to the associated Enterprise VRF routing table, as long as it doesn't exceed the maximum number of supported prefixes per MR (up to eight). E-PGW shall update the external VRF router of the newly installed prefixes on the next eBGP update.

NEMO4G-HA shall accept NEMO MIPv4 RRQs that do not include any prefixes in the first initial RRQ and it shall accept prefixes advertised in subsequent RRQs.

- In case of a prefix whose IP address or mask is changed on the MR, the MR will remove the old IP address/mask and add the new IP address/mask prefix in a scheduled or ad-hoc NEMO MIPv4 re-registration request and NEMO4G-HA shall remove the old route and add the new route corresponding to the new prefix to the Enterprise VRF routing table

- Overlapping IP addressing

  NEMO4G-HA supports private and overlapping IP addressing across multiple Enterprises for the WAN IP pools, MR-HADDR, and LAN prefixes.

NEMO MR Authorization

NEMO4G-HA authorizes a NEMO MIPv4 session only if a NEMO permission has been assigned to the underlying PDN connection. NEMO permission should be assigned to the underlying PDN connection via either local configuration (APN parameter) or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter is supported to enable NEMO permission at the APN/PDN level within the P-GW service.

MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client.

NEMO4G-HA processes the first of three Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The three Cisco-specific NVSEs are placed after the MIPv4 "Identification" field and before the mandatory MIPv4 "Mobile-Home-Authentication-Extension." NEMO4G-HA accepts the LAN prefixes (up to eight) encoded in the first Cisco-specific NVSE (vendor-type = 9). NEMO4G-HA is not expected to process the other two Cisco-specific NVSEs with vendor-type = 49, which carry the Internal Interface ID of the MR's Roaming Interface and the MR's Roaming Interface Bandwidth in Kbps, respectively.

Cisco-specific NVSEs follow RFC 3025 "Mobile IP Vendor/Organization Specific Extensions."

GRE Encapsulation

User traffic shall be encapsulated over a GRE tunnel between the MR NEMO client and NEMO4G-HA. The IP endpoints of the GRE tunnel shall be the IPv4 assigned to the MR modem during the Enterprise PDN connection setup and the IPv4 address of the NEMO4G-HA service on the E-PGW.

NEMO4G-HA shall remove the GRE encapsulation before it forwards the outbound traffic towards the Enterprise VPN via the associated SGi VLAN interface. Inbound traffic received through the same SGi VLAN interface shall be encapsulated into a GRE tunnel before it's passed to the E-PGW service for forwarding to the MR through the proper GTP/PMIP tunnel.

Session Interactions

The following session interaction scenarios are supported between NEMO and the underlying PDN connection made over eHRPD or LTE access.

In the following circumstances, NEMO4G-HA shall withdraw the associated prefix routes from the Enterprise VRF routing table, update the eBGP neighbors and free up all internal resources allocated for the underlying PDN connection and NEMO session:

- When the eHRPD terminates the underlying PDN connection (PPP-VSNCP-Term-Req sent to MR and PMIP-BU with lifetime = 0 sent to E-PGW).
- When the MR terminates the PPP/PDN connection when accessing the network via eHRPD.
- After an eUTRAN (LTE) detach procedure initiated by the MR or MME.

NEMO4G-HA shall not be able to process any NEMO MIPv4 RRQs if there's no underlying PDN connection associated to those RRQs (PMIPv6 or GTP). In other words, NEMO MIPv4 RRQs can be accepted and processed only if an Enterprise PDN connection has been established with E-PGW by the mobile router.

NEMO4G-HA shall silently ignore NEMO MIPv4 RRQs if the underlying PDN connection associated to each of those RRQs does not have the NEMO permission indication. This applies to both eHRPD and LTE access.

NEMO4G-HA shall forward (not drop) user data using MIP or GRE tunneling (UDP/434 or IP Protocol/47, respectively) to the external enterprise VRF if such data is not destined to the NEMO4G-HA IP address. This applies to PDN connections that have or do not have the NEMO Permission indication. This shall also apply to both eHRPD and LTE access.

Any failure on either the authentication or authorize of a NEMO MIPv4 session shall not affect the underlying PDN connection established between the mobile router and the E-PGW via eHRPD or LTE. For example, if the security credentials do not match between the MR NEMO client and NEMO4G-HA, NEMO4G-HA can reject the NEMO MIPv4 RRQ, but the associated PDN connection shall not be terminated.

NEMO Session Timers

NEMO4G-HA uses the registration lifetime value locally configured, even though MR's may use the maximum possible value (65534).

NEMO4G-HA can process ad-hoc NEMO RRQ messages.

Enterprise-wide Route Limit Control

NEMO4G-HA supports a control mechanism to limit the maximum number of prefixes/routes that a given enterprise can register, including the pools for WAN IP assignments.

When the maximum number of routes is reached, a syslog message is generated. Once the number of routes goes under the limit, a syslog message is generated for notification.

Forced Fragmentation

E-PGW forces IP packet fragmentation even for IP packets with the DF-bit set.

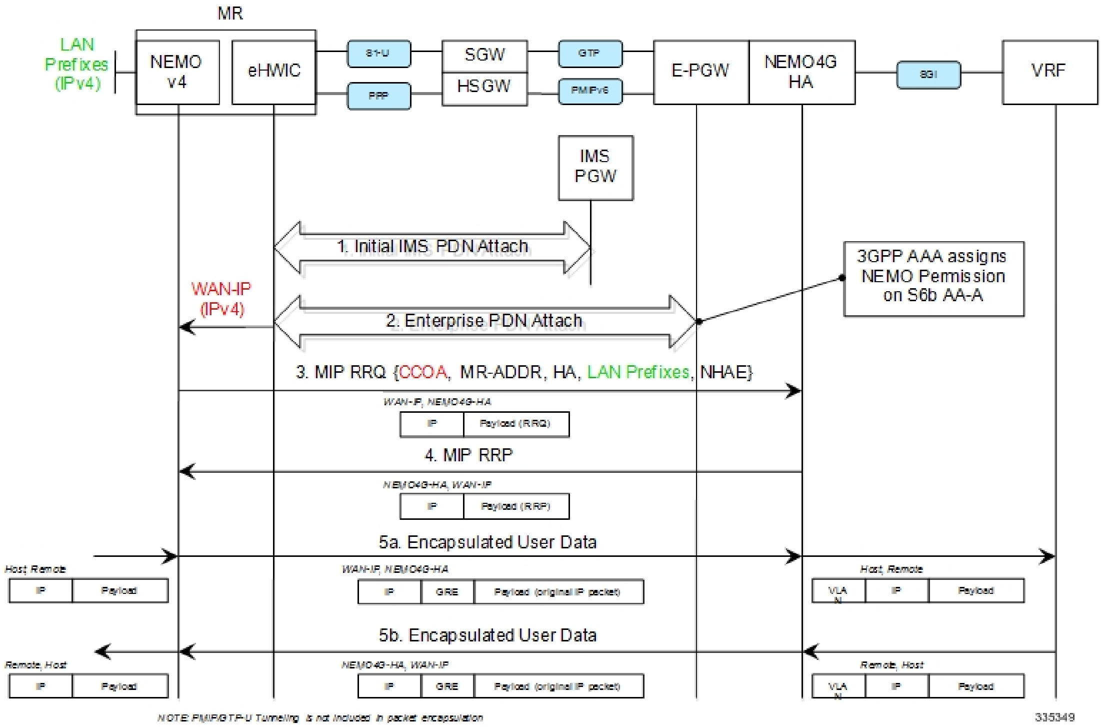
Redundancy/Reliability

The LTE NEMO solution supports intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.

LTE NEMO Call Flow

The following figure describes the call flow of the NEMOv4 solution.

Figure 3: NEMOv4 Call Flow



1. The Cisco MR eHWIC establishes first a connection to the IMS PDN to register to the LTE Network. The eHWIC's User Id must be properly provisioned on the HSS/SPR to be successfully authenticated.

2. After the Cisco MR eHWIC registers with the LTE network and establishes a connection to the IMS PDN, then it connects to the appropriate Enterprise PDN based on the locally configured Enterprise APN.

    - During the PDN authorization procedure using S6b, the 3GPP AAA assigns a NEMO permission via AVP. The AVP is also be available as an APN parameter on the E-PGW to allow NEMO service at the PDN/Enterprise level.

    - E-PGW assigns the MR eHWIC an IPv4 address from the Enterprise IPv4 pool assigned during PDN authentication.

    - E-PGW creates the proper flows internally to forward packets to the corresponding VRF external to the E-PGW platform using the IPv4 pool configuration on the egress context.

    - The MR eHWIC passed on the assigned IPv4 address to the NEMO application (also called WAN-IPv4 address).

3. The MR NEMO application initiates a Mobile IPv4 registration request (RRQ) using the following local configuration and the IPv4 address assigned to the eHWIC during the Enterprise PDN attach procedure (referred to as WAN-IP). The NEMO MIPv4 RRQ will be carried as a regular user packet over the mobility connection, either GTP in LTE and PPP/PMIPv6 in eHRPD. The NEMO MIPv4 RRQ includes the following key parameters:

- CCOA - IPv4 address assigned to the eHWIC modem during the Enterprise PDN connection setup (WAN-IP). The MR NEMO application will use the CCOA/WAN-IP address as the source of all NEMO packets sent to NEMO4G-HA (control and tunneled user traffic).
- MR-HADDR - Mandatory IPv4 address preconfigured in the MR NEMO application. MR-HADDR is normally used as the source of all NEMO control packets sent to the NEMO4G-HA. However, the MR NEMO application will use the CCOA as the source for all NEMO packets (control and tunneled user traffic). Therefore, NEMO4G-HA will ignore the preconfigured MR-HADDR included in the RRQ, but it will still include it in the NEMO MIPv4 RRP.
- Home Agent Address - Preconfigured IPv4 address that the MR NEMO application uses as the destination for all NEMO control and GRE tunneled user data (NEMO4G-HA's IPv4 Address).
- Explicit LAN Prefixes - Locally attached IPv4 networks preconfigured on the MR NEMO application. LAN prefixes will be encoded in the same Cisco NVSE extension currently used in the NEMO solution for 3G. The Cisco NVSE included in the NEMOv4 MIP RRQ is in the form of a TLV.
- N-MHAE - Mandatory NEMO MN-HA Authentication Extension that includes the SPI and the authenticator computed using a pre-shared Key. Both SPI and Key are preconfigured in the MR NEMO application as well.
- NEMO-Tunnel flags such as, but not limited to, "Reverse Tunnel," "Direct Termination," "Tunnel Encapsulation" = GRE.

4. NEMO4G-HA sends a MIP registration response (RRP) back to the MR after it performs the following tasks:
   - Authenticate the RRQ using the N-MHAE information included in the RRQ.
   - Authorize the NEMO service based on the NEMO permission attribute assigned to the associated Enterprise PDN connection.
   - Accept the prefixes advertised in the Cisco NVSE extension included in the NEMO MIPv4 RRQ.
     - The learned prefixes will have to adhere to the current rules of valid pool routes. The minimum valid mask length is /13 and pool routes can not include 0.0.0.0 or 255.255.255.255.
     - NEMO4G-HA will accept a minimum of 0 prefixes and a maximum of 8 prefixes. Anything beyond 8 prefixes will be silently discarded.
     - NEMO4G-HA will also check that the new resultant enterprise route count (total number of VRF routes) do not exceed the route limit potentially configured for the given enterprise. If the preconfigured route limit is exceeded, then NEMO4G-HA will reject the NEMO MIP RRQ. Otherwise, NEMO4G-HA will install the accepted prefixes in the internal VRF associated with the Enterprise PDN.
     - eBGP would then propagate the new NEMO routes to the external VRF as part of the next BGP update.
5. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table to route all traffic through the LTE connection.
   - Outbound packets are encapsulated over GRE using the CCOA/WAN-IP address as the source and the NEMO4G-HA-Service IPv4 address as the destination of the tunnel.

- Inbound packets are encapsulated over GRE as well from the NEMO4G-HA to the MR NEMO application. The source of the GRE tunnel is the NEMO4G-HA-Service IPv4 address and the destination is the CCOA/WAN-IP address.

Engineering Rules

- Up to 5,000 host routes spread across multiple VRFs per BGP process. Limited to 6,000 pool routes per chassis.
- Up to 2,048 VRFs per chassis.

Supported Standards

- IETF RFC 3025 (February 2001) "Mobile IP Vendor/Organization Specific Extensions"
- IETF RFC 1191 (November 1990) "Path MTU Discovery"

NEMO Configuration

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 configure the system for NEMO:

1. Create a VRF on the router and assign a VRF-ID by applying the example configuration in Create a VRF.
2. Set the neighbors and address family to exchange routing information with a peer router by applying the example configuration in Set Neighbors and Address Family, on page 9.
3. Redistribute connected routes between routing domains by applying the example configuration in Redistribute Connected Routes, on page 10.
4. Allow the P-GW to use the NEMO service by applying the example in Configure and Enable NEMO in APN Profile, on page 10.
5. Create a NEMO HA by applying the example in Create a NEMO HA, on page 10.
6. 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*.

Sample Configuration

```
context egress
interface corp1-outbound
   ip address 192.168.1.1 255.255.255.0
   exit
ip vrf corp1
ip pool corp1-test 10.1.1.1 255.255.255.0 private vrf corp1
nexthop-forwarding-address 192.168.1.2 overlap vlanid 50
router bgp 100
   address-family ipv4 vrfcorp1
      neighbor192.168.1.2 remote-as 300
      neighbor 192.168.1.2 allow-default-vrf-connection
      redistribute connected
      exit
   exit
context pgw
   apn nemo.corp1.com
      permission nemo
         ip context-name egress
         ip address pool name corp1_nemo_pool
         exit
      exit
context ingress
   interface corp1-inbound
      ip address 192.168.1.1 255.255.255.0
      exit
   ha-service nemo
      mn-ha-spi spi-number 100 encrypted secret 01abd002c82b4a2c
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address 38.0.0.2
      end
```

Create a VRF

Use this example to first create a VRF on the router and assign a VRF-ID.

```
configure
   context <context_name> -noconfirm
      ip vrf <vrf_name>
      ip pool <pool_name> <pool_address> private vrf <vrf_name>
      nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>
      end
```

Set Neighbors and Address Family

Use this example to set the neighbors and address family to exchange routing information with a peer router.

```
configure
   context <context_name>
```

```
ip vrf <vrf_name>
   router bgp <as_number>
   ip vrf <vrf_name>
      neighbor <ip_address> remote-as <AS_num>
      address-family <type>
      neighbor <ip_address> activate
      end
```

Redistribute Connected Routes

Use this example to redistribute connected routes between routing domains.

```
configure
   context <context_name>
      ip vrf <vrf_name>
         router bgp <as_number>
         ip vrf <vrf_name>
            address-family <type> vrf <vrf_name>
               redistribute connected
               exit
            redistribute connected
            end
```

Configure and Enable NEMO in APN Profile

Use this example to configure and enable NEMO in an APN profile.

```
configure
   context <context_name>
      apn <apn_name>
         permission nemo
         ip context-name <name>
         ip address pool name <pool_name>
         end
```

Create a NEMO HA

Use this example to create a NEMO HA.

```
configure
   context <context_name>
      ha-service <ha_service_name>
         mn-ha-spi spi-number <number> encrypted secret <enc_secret>
         authentication mn-aaa noauth
         encapsulation allow keyless-gre
         bind address <ip_address>
         end
```