NEMOv4 with Multi-VRFs

This chapter describes the system's support for Network Mobility V4 (NEMOv4) with Multi-VRFs 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 respective product Administration Guide, before using the procedures in this chapter.

NEMO Overview

The existing design of HA NEMOv4 has been extended to support multiple enterprise network being connected from one Mobile Router. A Mobile Router (MR) can be configured with devices/subnets to seamlessly access multiple enterprize VRFs, and the network traffic targeted for those different VRFs will share same MIP tunnel without compromising the privacy and security. Each VRF works independently through the MR and HA services.

This is done by separating the VRFs at the NEMO registration time, each VRF will be furnished with own set of GRE keys for the bidirectional traffic between MR and HA.

The following figure shows a high-level view of Multi-VRF Support.

Figure 1: Multi-VRF-Support
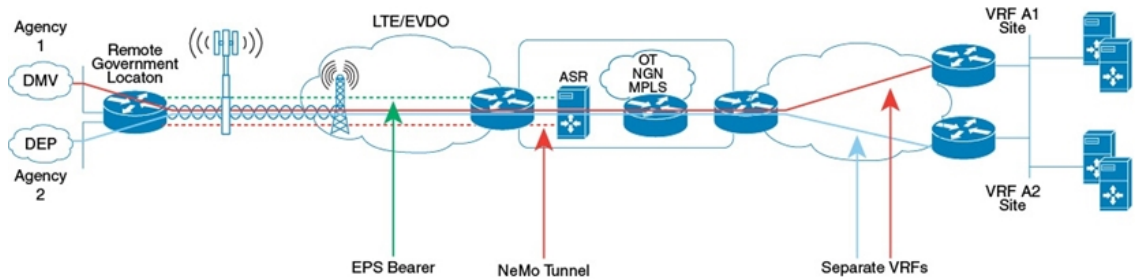
Use Cases

The following use cases are supported by NEMO Multi-VRF. Multi-VRF provides a simplified CPE/UE configuration, strong privacy and separation between networks, without impacting an organization's IP addressing or routing designs or protocols. :

1. **Multi-Agency:** A Remote Government location that supports multiple agencies which require overlapping IP addresses and privacy.

2. **Multi-Tenant:** Multiple customers using a single mobile router/access line, across any network, with special affinity for LTE, allowing the service provider to provide multi-tenant services at a location. For example, multi-tenant buildings, fast food restaurants with multiple companies.

3. **Machine-to-Machine (M2M):** Allows multiple services or machines to share a mobile router or access line within a single Kiosk/ATM/multi-function device. For exmaple, ATM, retail kiosk, vending machines, automobiles, trucks, trains, planes, mobile setups/shows.

4. **Guest Access:** Allows corporate access and guest/Internet access to share a mobile router/access line, or to share a mobile router. For example, Retail store, restaurant, entertainment venue, planes, trains, cars (separate from car functions), Teleworker/Home.

5. **SMB/Residential Gateway:** Allows multiple SMB office or residential services/devices to share a mobile router/access line within a single residential home router. For example, Homes, Teleworker, doctor offices, real estate offices, small businesses, temporary sites.
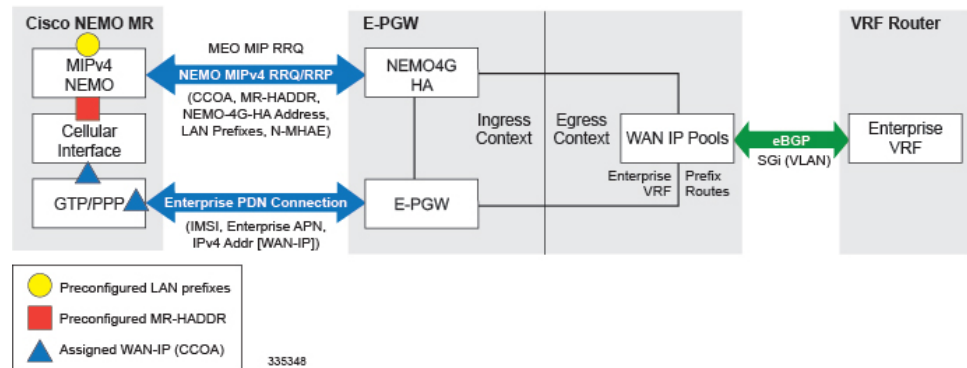
Features and Benefits

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). NEMO4G-HA supports the registration for Mobile Router services.

- 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 16 prefixes per mobile router. Anything beyond 16 prefixes shall be silently discarded.

    - NEMO4G-HA supports any prefix length (including /12 to /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). HA/PGW/GGSN 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 16). HA/PGW/GGSN 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 Multi-VRF feature support private and overlapping IP addressing across multiple Enterprise network being connected from a Mobile Router. A Mobile Router (MR) can be configured with devices/subnets to seamlessly access multiple enterprise VRFs, and the network traffic targeted for those different VRFs shall share same MIP tunnel without compromising the privacy and security. Each VRF works independently through the MR and HA services.

- **Multi-VRF Support**

The Multi-VRF Support feature enables a service provider to support two or more Virtual Private Networks (VPNs), where the IP addresses can overlap several VPNs. The Multi-VRF Support feature uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more interfaces with each virtual routing and forwarding (VRF) instance.

NEMO4G-HA supports Multi-VRF within the same Mobile Router, for which the signaling and forwarding mechanism has been extended. Each enterprise network is associated with its own VRF. Both MR and HA share common vrf-names. MR and HA services are enhanced to support Cisco NVSE extension for NEMO with multiple VRF.

Multi-VRF NEMO includes the following features:

- A new Cisco NVSE carries VRF tags as part of the registration signaling. The Mobile Network Prefixes (MNP) are associated with these VRF tags. Furthermore, a GRE key associated with the VRF is embedded to this new NVSE, in order to provide VRF traffic segregation between the MR ISR and the NEMO-HA ASR 5500 during data forwarding. Note, there may be multiple MNPs for one GRE key, but not one MNP for multiple GRE keys.

- The CLI config with the vrf-list and/or default VRF with IP Pool does not automatically enable multi-VRF.

  Multi-VRF takes effect only if:

  - MR sends in RRQ with the new NVSE format.
  - The specific VRF name is authorized with the ip-pool config. (the default VRF is always authorized, so vrf-list is NOT required to support multi-vrf, all the old config could support multi-vrf without any change. If an IP Pool or vrf-list is changed, it takes effect only for future new calls.

☞

Important　Next-hop forwarding is not supported by Multi-VRF with 15.0. Only MPLS is supported.

- Home Agent on receiving the Mobile IP Registration Request from the mobile router with the above NVSE, and after a successful authentication learns about the dynamic mobile networks associated with the mobile router from the Dynamic Network extension in the Registration Request. If the

request is authorized, a Registration Reply with the Mobile Router Multi-VRF NVSE extension is sent.

- The Home Agent supports the following:

    - Dynamic Mobile Network Prefix (MNP) updates for an authorized VRF.
    - VRF addition/deletion of VRF's from the authorization list without requiring mobile pool reconfiguration.
    - MNP's of any length, including /32.
    - Geo-redundancy (ICSR) for NEMO Multi-VRF.
    - Mapping of a mobile pool to a list of authorized VRF's.
    - Multiple VRF authorization lists for 1 APN or Subscriber Profile.

- The Home Agent on receiving a packet from the tunnel shall use the GRE key for VRF forwarding the packet towards the enterprise.
- On receiving a packet from the enterprise towards the MR, the VRF key associated with the interface IDB shall be used as the GRE key.

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 through either local configuration (APN parameter) or for CDMA via subscriber profile or based on a NEMO permission AVP assigned by the 3GPP AAA during the PDN authorization. For local configuration, a new APN parameter or for CDMA via subscriber profile is supported to enable NEMO permission at the APN/PDN level within the HA/PGW/GGSN service. VRF authorization is needed. The multi-vrf authorization is done by comparing RRQ's each VRF name with the ip-pool's Default VRF or names defined by the vrf-list.

MIPv4 NEMO Protocol

NEMO4G-HA processes a Mobile IPv4 NEMO Registration Request (RRQ) received from the MR NEMO client. The RRQ shall carry multiple NVSEs to reflect the multiple VRFs and multi-tenant Prefixes per MR.

Overlapping MNPs are allowed, if they are associated with different VRF. MNP must be different if same VRF name is used on either one MR or across all MRs. Though per customer request, HA does not explicitly deny a request with such misconfiguration.

NEMO4G-HA processes the maximum of 16 Cisco-specific MIPv4 Extensions of type Normal Vendor/Org Specific Extension (NVSE) that are included in the MIPv4 NEMO RRQ. The Cisco NVSE carries VRF tags as part of the registration signaling. A GRE key associated with the VRF shall be embedded to this new NVSE, in order to provide VRF traffic segregation between the MR ISR and the NEMO-HA ASR 5500 during data forwarding. Note, there may be multiple MNPs for one GRE key, but not one MNP with multiple GREs. The Mobile Network Prefixes (MNP) will need to be associated with these VRF tags.

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 HA/PGW/GGSN.

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 HA/PGW/GGSN 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 CDMA MIP or eHRPD or LTE access.

The mobile router on receiving a packet to from the tunnel shall use the GRE key to identify the tunnel instance. After decap, the packet shall be forwarded towards the mobile networks, based on the route lookup in the specific VRF context.

On receiving a packet from the mobile network, the default-route in the specific VRF context (associated with that input interface) shall be used and the packet encap shall get the correct GRE key.

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 HA/PGW/GGSN).

- 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 HA/PGW/GGSN 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 CDMA, 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 HA/PGW/GGSN 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. And no further routes are accepted into the VRF route table. NEMO MIP RRQ is rejected accept for Multi-VRF NEMO in which case the NEMO MIP RRQ is accepted but offending VRF denied.

Forced Fragmentation

HA/PGW/GGSN forces IP packet fragmentation even for IP packets with the DF-bit set from enterprise to mobile. From mobile to enterprise DF-bit is honored.
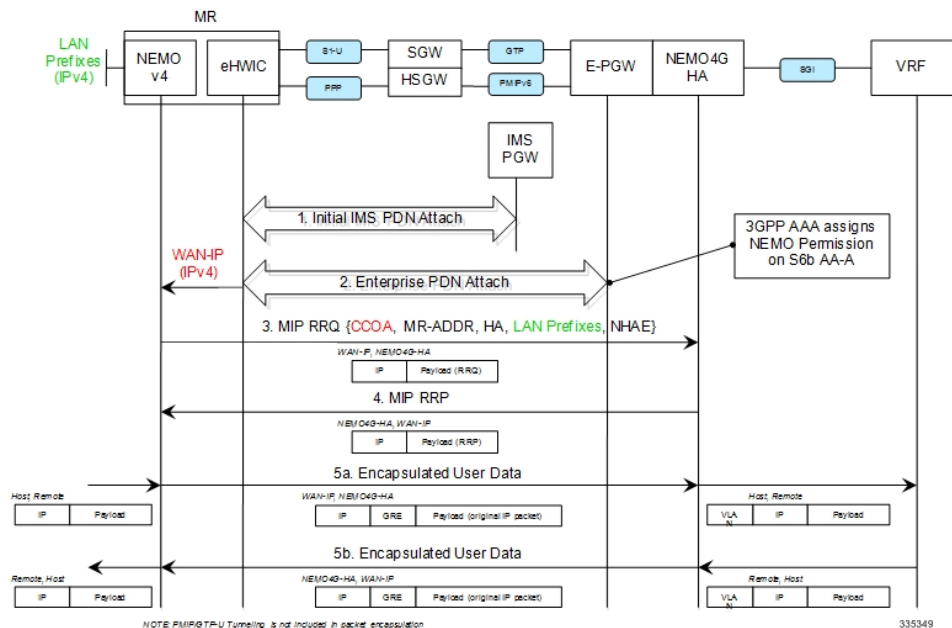
Redundancy/Reliability

CDMA, eHRPD and LTE all support intra-chassis Session Redundancy (SR) and Inter-Chassis Session Redundancy (ICSR) functionalities.

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 HA/PGW/GGSN to allow NEMO service at the PDN/Enterprise level.

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

   - HA/PGW/GGSN creates the proper flows internally to forward packets to the corresponding VRF external to the HA/PGW/GGSN 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 shall 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:

   - MNP - NVSE contains the Mobile Network Prefixes(MNP), a tag designating the VRF instance, and a GRE key (for downlink traffic) associated with the VRF. When the HA/PGW/GGSN receives the RRQ with the NVSE, it shall examine the MNPs. Assuming that there is no error conditions (e.g. overlapping MNPs in the same VRF), it shall insert the MNPs in the VRF routing table with the same identifier (i.e. VRF name) as the VRF tag in the NVSE. A routing entry is added to direct the downlink traffic toward each MNP to a tunnel with the GRE key, which is based on the value learned from the NVSE.

   - 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.

    - Confirm the MNPs are accepted in the VRF forwarding table.

    - 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 16 prefixes. Anything beyond 16 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. a. The VRF's GRE, which is in the RRP that the MR received from HA, is used for this data packet.

   b. Upon receiving the NEMO MIP RRP, the MR will install a default route (0.0.0.0/0) in its routing table (associated with the VRF tag in the NVSE) to direct uplink traffic to a tunnel with the GRE key, which is based on the value learned from the NVSE, to route all traffic through the CDMA/LTE/GGSN connection. The VRF's GRE that is contained in the RRQ to HA from MR is used to wrap the data.

      - 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.

Fault and Fault Reporting

HA tries to accommodate the variety of RRQ without issuing failures. However, if failure occurs, different level of logging message are logged And the E-XGW will return RRP with error code 0 but not include the failed VRFs or MNPs.

Multi-VRF error handling is close to non-VRF environment. However, the following scenarios are considered as errors:

- **MR is not authorized for NEMO service, but has valid security association:**

  If the MR is not authorized for the NEMO service, but has a valid security association. HA/PGW/GGSN shall silently discard the registration request.

- **Misconfiguration or unauthorized VRF:**

  There may be an issue with a single VSE due to misconfiguration of a VRF name or simply the VRF may not be authorized. Upon receipt of the MR RRQ, the HA/PGW/GGSN shall reply with RRP, with status value of 0 (Accepted), but the NVSE for the failed VRF shall not be included in the reply. The missing NVSE in the RRP serves as a hint to the MR that the given VRF was not accepted. This behavior allows the other VRFs to be accepted (status code 0) and unaffected by the errant VSE.

  The MR shall set up forwarding only for the accepted VPN/subnets. It shall not set up tunnel forwarding for the rejected VPN/prefixes.

  MR shall continue to include all the VSE's in the subsequent re-registration RRQ, including the customer VRF that was not in the previous RRP response.

  Where ALL NVSEs are problematic, if the status code remains as 0 (Acccepted) with no NVSE included in the NEMO MIP RRP, the status code shall not revert to 129.

- **Single VRF exceeds the maximum route-limit at HA/PGW/GGSN:**

  A Multi-VRF enabled Mobile Router registers NVSEs, and a specific VSE is carrying MNPs which exceeds the total maximum configurable route-limit for associated VRF at the HA/PGW/GGSN. In this particular case, the HA/PGW/GGSN shall respond with status code of 0 (Accepted) in the RRP, but the problematic NVSE shall not be included in the RRP reply. The missing RRP provides hint there was a problem with the VRF.

- **A single MR attempts to register more than 16 MNPs:**

  If more than 16 MNPs are configured for MR registration, the HA/PGW/GGSN shall accept the partial prefix set, up to 16. The accepted MNPs are echoed in the RRP.

  ☞

  Important   ASR 5500 NEMO HA dynamically updates the VRF routing tables accordingly by processing ONLY the first 16 MNPs in the RRQ. Because the ordering of the MNPs in RRQ may not be ensured by MR, every time, a different set of 16 MNPs MAY be registered by ASR 5500 NEMO HA.

Errors Pertaining to VRFs: The error message does not indicate which VRF has caused the failure. To know the VRF that has caused the failure, print all the requesting VRFs for errors. A denied VRF does not result in a RRQ failure if the other VRFs are accepted. The following scenarios, but not limited to, are considered as failures:

- IP pool refers to a named **framed-route-vrf-list**, but there is no **vrf-list** defined in the context.
- The context defined **vrf-list** with a named VRF, but no vrf is defined with that name.
- The context defined **vrf-list** with more than 16 VRF names.
- The RRQ NVSE contains a VRF that is neither the Default VRF on HA, nor in the **framedrouter-vrf-list**. A default VRF of IP pool is specified by its **vrf** parameter.
- The RRQ NVSE contains a VRF name longer than 63 bytes. The VPN system pre-allocated 64 bytes for the NULL terminated string. The error for the VRF name that is longer than 63 bytes is returned.

The following scenarios are not considered as errors, as HA is able to make a decision and achieve the best usability:

- IP pool does not define a value for **vrf** parameter, whether a **framed-route-vrf-list** is specified or not. The value specified by IP pool\'s **vrf** parameter is called Default VRF, where IP address is advertised in when the input **vrf** is unnamed. When this parameter is not specified, Default VRF is its current context.

- The RRQ NVSE contains a VRF without a name, or empty name. All the prefixes in this VRF are treated as for the implied Default VRF in the IP Pool.
- The RRQ NVSE contains a VRF name that matched with the Default VRF but is not a member of the **framed-router-vrf-list**. This is due to the fact that the Default VRF is always authorized.
- The RRQ contains more than 16 prefixes in total, regardless of how many VRFs are they in. HA will ignore those prefixes after 16. This ensures that the existing non-vrf or unnamed vrf features are unaffected.
- When IP pool does not specify the **framed-router-vrf-list** parameter or list is specified but empty, both work with the current behavior. The following special rules apply:

  - RRQ NVSE may contain no VRF. Then no authorization will take place, the Default VRF will be directly used for IP pool.
  - RRQ NVSE contains only one VRF which has the **vrf** setting for authorization. The Default VRF is used to advertise the IP address.

Engineering Rules

- Up to 300 virtual routing tables per context and 64 BGP peers per context.
- Up to 5k host routes spread across multiple VRFs per BGP process. Limited to 6000 pool routes per chassis.
- Upto 2048 VRFs per chassis
- Per MR:

  - 0~16 VRF per one MR/CPE
  - One NVSE per one VRF
  - Upto 16 MNPs per VRF

- 1~16 VRF per one vrf-list
- 0~63 bytes VRF names in ASCII text

Supported Standards

- IETF RFC 5177 (April 2008) "Mobile IPv4 NEMO Extensions,"
- IETF RFC 3025 (February 2001) "Mobile IP Vendor/Organization Specific Extensions"
- IETF RFC 3115 (April 2001) "Mobile IP Vendor/Organization Specific Extensions"

Configuring NEMOv4 Multi VRF

ASR 5500 provides some CLI commands with this new feature.

NEMO Multi-VRF Egress

```
config
   context <egress1>
      ip vrf <vrf-name1>
         ip maximum-routes 4998
      exit
```

```
        ip vrf <vrf-name2>
            ip maximum-routes 4998
        exit
        ip vrf <vrf-name3>
            ip maximum-routes 4998
        exit
        ip vrf-list <vrf_list_1> permit <vrf-name1>
        ip vrf-list <vrf_list_1> permit <vrf-name2>
        ip vrf-list <vrf_list_1> permit <vrf-name3>
        mpls bgp forwarding
        ip pool <poolname1-b> <ipaddress> private 0 srp-activate group-name
<customer1> vrf <vrfname1> policy policy framed-route-vrf-list <vrf_list_1>
allow-static-allocation
        router bgp 1
            router-id <ipaddress>
            neighbor <ipaddress> remote-as 1001
            neighbor <ipaddress> remote-as 1001
            address-family <vpnv4>
                neighbor <ipaddress> activate
                neighbor <ipaddress> send-community both
                neighbor <ipaddress> activate
                neighbor <ipaddress> send-community both
            exit
            ip vrf <vrfname1>
                route-distinguisher 1 1
              route-target export 1 1
                route-target import 1 1
        exit
        address-family ipv4 vrf  <vrfname1>
            redistribute connected
            redistribute static
        exit
        ip vrf <vrfname2>
            route-distinguisher 2 2
            route-target export 2 2
            route-target import 2 2
        exit
        address-family <ipv4> vrf <vrfname2>
              redistribute connected
              redistribute static
          exit
        ip vrf <vrfname3>
            route-distinguisher 3 3
            route-target export 3 3
            route-target import 3 3
        exit
          address-family <ipv4> vrf <vrfname3>
            redistribute connected
            redistribute static
          exit
```