



## Configuring Dynamic Addressing on the GGSN

---

This chapter describes how to configure dynamic IP addressing on the gateway GRPS support node (GGSN).

For a complete description of the GGSN commands in this chapter, refer to the *Cisco GGSN Release 5.2 Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- [Overview of Dynamic IP Addressing on the GGSN, page 11-1](#)
- [Configuring DHCP on the GGSN, page 11-2](#)
- [Configuring MS Addressing via Local Pools on the GGSN, page 11-9](#)
- [Configuring MS Addressing via RADIUS on the GGSN, page 11-11](#)
- [Configuring IP Overlapping Address Pools, page 11-11](#)
- [Configuring the NBNS and DNS Address for an APN, page 11-15](#)

### Overview of Dynamic IP Addressing on the GGSN

There are three methods for configuring the GGSN to assign IP addresses to mobile station users who need to access the public data network (PDN): Dynamic Host Configuration Protocol (DHCP) allocation, Remote Authentication Dial-In User Service (RADIUS) allocation, and local IP address pool allocation configured at the access point name (APN).

A method of dynamic IP addressing can be configured either globally or at the access-point configuration level.

Be sure that the following configuration guidelines are met to support the type of IP address allocation in use on your network:

- DHCP IP address allocation
  - Be sure that you configure the scope of the addresses to be allocated on the same subnet as the loopback interface.
  - Do not configure an IP address for users on the RADIUS server.
  - Specify the **peer default ip address dhcp** command at the PPP virtual template interface.
  - Specify the **aaa authorization network method\_list none** command on the GGSN.

- RADIUS IP address allocation
  - Be sure that users are configured on the RADIUS server using the complete username@domain format.
  - Specify the **no peer default ip address** command at the PPP Virtual Template interface.
  - For more information about configuring RADIUS services on the GGSN, see the “[Configuring Security on the GGSN](#)” chapter in this book.
- Local pool IP address allocation
  - Be sure to configure a local pool using the **ip local pool** command.
  - Specify the **aaa authorization network method\_list none** command on the GGSN.
  - Specify the **peer default ip address pool pool-name** command.

**Note**

On the Catalyst 6500 / Cisco 7600 platform, dynamic address allocation using the DHCP or RADIUS server methods requires that the DHCP or RADIUS server be Layer 3 routeable from the Supervisor/MSFC2.

## Configuring DHCP on the GGSN

You can use local DHCP services within the Cisco IOS software, or you can configure the GGSN to use an external DHCP server such as the Cisco Network Registrar (CNR). For information about configuring internal DHCP services in the Cisco IOS software, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

The DHCP server can be specified in two ways:

- At the global configuration level, using the **gprs default dhcp-server** command
- At the access-point configuration level, using the **dhcp-server** command

To configure DHCP support on the GGSN, you must configure either the **gprs default ip-address-pool** global configuration command or the **ip-address-pool** access-point configuration command with the **dhcp-proxy-client** keyword option.

After you configure the access point for DHCP proxy client services, use the **dhcp-server** access-point configuration command to specify a DHCP server.

Use the *ip-address* argument to specify the IP address of the DHCP server. The second, optional *ip-address* argument can be used to specify the IP address of a backup DHCP server to be used in the event that the primary DHCP server is unavailable. If you do not specify a backup DHCP server, then no backup DHCP server is available.

If you specify a DHCP server at the access-point level by using the **dhcp-server** command, then the server address specified at the access point overrides the address specified at the global level. If you do not specify a DHCP server address at the access-point level, then the address specified at the global level is used.

Therefore, you can have a global address setting and also one or more local access-point level settings if you need to use different DHCP servers for different access points.

Use the **vrf** keyword when the DHCP server itself is located within the address space of a VRF interface on the GGSN. If the DHCP server is located within the VRF address space, then the corresponding loopback interface for the **dhcp-gateway-address** must also be configured within the VRF address space.

This section contains the following information:

- [Configuring DHCP Server Communication Globally, page 11-3](#)
- [Configuring DHCP at the GGSN Global Configuration Level, page 11-4](#)
- [Configuring a Local DHCP Server, page 11-8](#)
- [Configuration Example, page 11-8](#)

## Configuring DHCP Server Communication Globally

This section describes how to configure a global DHCP server host that the GGSN can use to assign IP addresses to mobile users. You can configure additional DHCP server communication at the GGSN global configuration level.

To globally configure DHCP server communication on the router or instance of Cisco IOS software, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip address-pool</b> { <b>dhcp-proxy-client</b>   <b>local</b> }	Specifies an IP address pool mechanism, where: <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—Specifies the router or instance of Cisco IOS software as the proxy-client between a third-party DHCP server and peers connecting to the router or IOS instance.</li> <li>• <b>local</b>—Specifies the local address pool named “default”.</li> </ul> <p><b>Note</b> There is no default option for the <b>ip address-pool</b> command. If you configure a local address pool using the <b>local</b> keyword, you can also configure the optional commands in Step 4 and Step 5.</p>
Step 2	Router(config)# <b>ip dhcp-server</b> { <i>ip-address</i>   <i>name</i> }	Specifies the IP address or name of a DHCP server.
Step 3	Router(config)# <b>ip dhcp excluded address</b> <i>low-address</i> [ <i>high-address</i> ]	(Optional) Specifies IP addresses that a DHCP server should not assign to DHCP clients, where: <ul style="list-style-type: none"> <li>• <i>low-address</i>—Specifies the first IP address in an excluded address range. This address is typically the address of the DHCP server itself.</li> <li>• <i>high-address</i>—(Optional) Specifies the last IP address in the excluded address range.</li> </ul>

	Command	Purpose
Step 4	Router(config)# <b>ip dhcp pool</b> <i>name</i>	(Optional—Supports <b>ip address-pool local</b> command only.) Configures a DHCP address pool, and enters DHCP pool configuration mode, where <i>name</i> can be either a symbolic string (such as “engineering”) or an integer (such as 0).
Step 5	Router(config-dhcp)# <b>network</b> <i>network-number</i> [ <i>mask</i>   <i>/prefix-length</i> ]	(Optional—Supports <b>ip address-pool local</b> command only.) Specifies the subnet network number and mask of the DHCP address pool.  The prefix length specifies the number of bits in the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

For more information about configuring global DHCP services, refer to the *Cisco IOS IP Configuration Guide*, *Cisco IOS IP Command References*, and the *Cisco IOS Dial Technologies Command Reference* publications.

## Configuring DHCP at the GGSN Global Configuration Level

To complete the DHCP configuration for the GGSN, you can configure DHCP at the GGSN global configuration level. When you configure DHCP at the GGSN configuration level, you can configure DHCP server communication for all access points or for a specific access point.

Configuring DHCP at the GGSN configuration level includes the following tasks:

- [Configuring a Loopback Interface, page 11-4](#) (Required)
- [Specifying a DHCP Server for All Access Points, page 11-5](#) (Optional)
- [Specifying a DHCP Server for a Particular Access Point, page 11-6](#) (Optional)

### Configuring a Loopback Interface

When you configure a DHCP gateway address for DHCP services at an access point, and when you are supporting unique supernets across all access points on the GGSN for DHCP, then you must configure a loopback interface for each unique network.

A loopback interface is a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The interface number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.

To configure a loopback interface on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>interface loopback</b> <i>interface-number</i>	Defines a loopback interface on the GGSN, where <i>interface-number</i> identifies the loopback interface.
Step 2	Router(config-if)# <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]	<p>Specifies an IP address for the interface, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of the interface in dotted decimal format.</li> <li>• <i>mask</i>—Specifies a subnet mask in dotted decimal format.</li> <li>• <b>secondary</b>—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> <p><b>Note</b> The <i>ip-address</i> corresponds to the IP address of the DHCP gateway address at the access point. The mask should be 255.255.255.255 to match the <b>dhcp-gateway-address</b> value exactly.</p>

## Specifying a DHCP Server for All Access Points

When processing DHCP address allocation, the GGSN software first checks to see whether a DHCP server has been specified at the access-point configuration level. If a server has been specified, the GGSN uses the DHCP server specified at the access point. If no DHCP server is specified at the access-point configuration level, then the GGSN uses the default GGSN DHCP server.

To specify a DHCP server for all GGSN access points, use the following commands, beginning in global configuration mode:

Command	Purpose	
Step 1	<pre>Router(config)# gprs default ip-address-pool {dhcp-proxy-client   radius-client   disable}</pre>	<p>Specifies a dynamic address allocation method using IP address pools for the GGSN, where:</p> <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—Specifies that the GGSN dynamically acquires IP addresses for a mobile station (MS) from a DHCP server. Use this keyword to enable DHCP services.</li> <li>• <b>radius-client</b>—Specifies that the GGSN dynamically acquires IP addresses for an MS from a RADIUS server.</li> <li>• <b>disable</b>—Disables dynamic address allocation by the GGSN.</li> </ul> <p>There is no default option for this command.</p>
Step 2	<pre>Router(config)# gprs default dhcp-server {ip-address   name} [{ip-address   name}]</pre>	<p>Specifies a primary (and backup) DHCP server from which the GGSN obtains IP address leases for mobile users, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.</li> <li>• <i>name</i>—Specifies the host name of a DHCP server. The second (optional) <i>name</i> argument specifies the host name of a backup DHCP server.</li> </ul>

## Specifying a DHCP Server for a Particular Access Point

To override the default DHCP server configured for all access points, you can specify a different DHCP server for a particular access point. Or, if you choose not to configure a default GGSN DHCP server, you can specify a DHCP server at each access point.

To specify a DHCP server for a particular access point, use the following commands, beginning in access-point configuration mode:

	Command	Purpose
Step 1	<pre>Router(config-access-point)# ip-address-pool {dhcp-proxy-client   radius-client   local pool-name   disable}</pre>	<p>(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>dhcp-proxy-client</b>—DHCP server provides the IP address pool.</li> <li>• <b>radius-client</b>—RADIUS server provides the IP address pool.</li> <li>• <b>local</b>—Specifies that a local pool provides the IP address. This option requires that a local pool has been configured using the <b>ip local pool</b> global configuration command.</li> <li>• <b>disable</b>—Turns off dynamic address allocation.</li> </ul> <p><b>Note</b> If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.</p>
Step 2	<pre>Router(config-access-point)# dhcp-server [ip-address] [ip-address] [vrf]</pre>	<p>Specifies a primary (and backup) DHCP server that the GGSN uses at a particular access point to obtain IP address leases for mobile users for access to a PDN, where:</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i>—Specifies the IP address of a DHCP server. The second (optional) <i>ip-address</i> argument specifies the IP address of a backup DHCP server.</li> <li>• <b>vrf</b>—DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the APN.</li> </ul>
Step 3	<pre>Router(config-access-point)# dhcp-gateway-address ip-address</pre>	<p>Specifies the subnet in which the DHCP server should return addresses for DHCP requests for MS users entering a particular PDN access point.</p> <p><b>Note</b> You must configure a corresponding loopback interface with the same IP address as the DHCP gateway address.</p>

## Configuring a Local DHCP Server



### Note

Using a local DHCP Server is not recommended on the Catalyst 6500 / Cisco 7600 platform.

Although most networks use external DHCP servers, such as that available through the Cisco Network Registrar (CNR), you can also configure internal DHCP services on the GGSN. If you use local DHCP services on the GGSN, then there are a couple of commands that you should configure to improve the internal DHCP response times.

To optimize local DHCP services on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip dhcp ping packets 0</b>	Specifies that the Cisco IOS DHCP Server sends 0 packets to a pool address as part of a ping operation.
Step 2	Router(config)# <b>ip dhcp ping timeout 100</b>	Specifies that the Cisco IOS DHCP Server waits for a ping reply from an address pool for 100 milliseconds.

## Configuration Example

The following example shows a VRF configuration for vpn3 (without tunneling) using the **ip vrf** global configuration command. Because the **ip vrf** command establishes both VRF and CEF routing tables, notice that **ip cef** also is configured at the global configuration level to enable CEF switching at all of the interfaces.

The following other configuration elements must also associate the same VRF named vpn3:

- FastEthernet0/0 is configured as the Gi interface using the **ip vrf forwarding** interface configuration command.
- Access-point 2 implements VRF using the **vrf** command access-point configuration command.

The DHCP server at access-point 2 also is configured to support VRF. Notice that access-point 1 uses the same DHCP server, but is not supporting the VRF address space. The IP addresses for access-point 1 will apply to the global routing table:

```

aaa new-model
!
aaa group server radius foo
  server 10.2.3.4
  server 10.6.7.8
!
aaa authentication ppp foo group foo
aaa authorization network foo group foo
aaa accounting network foo start-stop group foo
!
ip cef
!
ip vrf vpn3
  rd 300:3
!
interface Loopback1
  ip address 10.30.30.30 255.255.255.255
!
interface Loopback2

```



```
ip vrf forwarding vpn3
ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
ip vrf forwarding vpn3
ip address 10.50.0.1 255.255.0.0
duplex half
!
interface FastEthernet1/0
ip address 10.70.0.1 255.255.0.0
duplex half
!
interface loopback 1
ip address 10.8.0.1 255.255.255.0
!
interface Virtual-Template1
ip unnumber loopback 1
encapsulation gtp
gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
access-point 1
access-point-name gprs.pdn.com
ip-address-pool dhcp-proxy-client
dhcp-server 10.200.0.5
dhcp-gateway-address 10.30.30.30
network-request-activation
exit
!
access-point 2
access-point-name gprs.pdn2.com
access-mode non-transparent
ip-address-pool dhcp-proxy-client
dhcp-server 10.100.0.5 10.100.0.6 vrf
dhcp-gateway-address 10.27.27.27
aaa-group authentication foo
vrf vpn3
exit
!
gprs default ip-address-pool dhcp-proxy-client
gprs gtp ip udp ignore checksum
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

## Configuring MS Addressing via Local Pools on the GGSN

As the number of PDP contexts increases, allocating IP addresses via locally-configured address pools improves the PDP context activation rate. Whether or not addresses are allocated to MSs using local pools is specified at the access-point configuration level and requires that a local pool or pools of IP address have been configured on the GGSN using the **ip local pool** configuration command.

To configure a local IP address pool, use the following command in global configuration mode:

Step 1	Command	Purpose
	<pre>Router(config)#ip local pool {default   pool-name low-ip-address [high-ip-address]}</pre>	<p>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, where:</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Defaults local address pool that is used if no other pool is named.</li> <li>• <i>pool-name</i>—Name of a specific local address pool.</li> <li>• <i>low-ip-address</i>—Lowest IP address in the pool.</li> <li>• <i>high-ip-address</i>—(Optional) Highest IP address in the pool. If this value is omitted, only the low-ip-address IP address argument is included in the local pool.</li> </ul>

To configure a local IP address pool allocation on an access-point, use the following command in access-point configuration mode:

Step 1	Command	Purpose
	<pre>Router(config-access-point)# ip-address-pool local pool-name</pre>	<p>(Optional) Specifies that a local pool provides the IP address.</p> <p>This option requires that the address range be configured using the <b>aggregate</b> access point configuration command.</p>



**Note**

Using VRF at the access point, you can configure APNs that use the same IP address pool (overlapping addresses). However, on the Catalyst 6500 / Cisco 7600 platform, VRF is not supported on the Supervisor II / MSFC2. Therefore, if using a Supervisor II, you must tunnel the encapsulated VRF traffic through the Supervisor using a GRE tunnel.

For more information on configuring VPN access via VRF from an access point, see the [“VPN Access Using VRF Configuration Task Lists”](#) section on page 7-16.

The Catalyst 6500 / Cisco 7600 Sup720 supports VRF.

## Configuration Example

The following is a configuration example of a local address pool configured at the APN.

```
!  
ip local pool local_pool1 128.1.0.1 128.1.255.254  
!  
access-point 1  
access-point-name gprs.pdn.com  
ip-address-pool local local_pool1  
aggregate 128.1.0.0/16  
exit
```

## Configuring MS Addressing via RADIUS on the GGSN

Dynamic IP addressing via a RADIUS server is configured at the access-point configuration level using the **ip-address-pool** access-point configuration command.

For more information about the **ip-address-pool** access-point configuration command, see [“Configuring Other Access Point Options” section on page 7-25](#). For more information about configuring RADIUS, see the *Cisco IOS Security Configuration Guide*.

## Configuring IP Overlapping Address Pools

The IP Overlapping Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

IP Overlapping Address Pools gives greater flexibility in assigning IP addresses dynamically. It allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

With Cisco IOS Release 12.3(2)XB and later, the GGSN supports the concept of an IP address group to support multiple IP address spaces and still allow the verification of nonoverlapping IP address pools within a pool group. Pool names must be unique within the GGSN. The pool name carries an implicit group identifier because that pool name can be associated only with one group. Pools without an explicit group name are considered members of the base system group and are processed in the same manner as the original IP pool implementation.

Existing configurations are not affected by the new pool feature. The “group” concept is an extension of the existing **ip local pool** command. Processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

To configure a local IP address pool group and verify that it exists, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)#ip local pool {default   pool-name low-ip-address [high-ip-address]}</pre> <p><b>Example:</b></p> <pre>GGSN(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000</pre>	<p>Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, where:</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Defaults local address pool that is used if no other pool is named.</li> <li>• <i>pool-name</i>—Name of a specific local address pool.</li> <li>• <i>low-ip-address</i>—Lowest IP address in the pool.</li> <li>• <i>high-ip-address</i>—(Optional) Highest IP address in the pool. If this value is omitted, only the low-ip-address IP address argument is included in the local pool.</li> </ul>
Step 2	<pre>Router(config)# show ip local pool [poolname   [group group-name]]</pre> <p><b>Example:</b></p> <pre>GGSN(config)# show ip local pool group testgroup testpool</pre>	<p>Displays statistics for any defined IP address pools.</p>

## Configuration Examples

The following are configuration examples for configuring IP overlapping address pools.

- [Defining Local Address Pooling as the Global Default, page 11-12](#)
- [Configuring Multiple Ranges of IP Addresses into One Pool Example, page 11-12](#)
- [Configuring IP Overlapping Address Pools on a GGSN on the Catalyst 6500 / Cisco 7600 Platform with Supervisor II / MSFC2 Example, page 11-13](#)

### Defining Local Address Pooling as the Global Default

The following example shows how to configure local pooling as the global default mechanism:

```
ip address-pool local ip local pool default 192.169.15.15 192.68.15.16
```

### Configuring Multiple Ranges of IP Addresses into One Pool Example

The following example shows how to configure two ranges of IP addresses for one IP address pool:

```
ip local pool default 192.169.10.10 192.169.10.20
ip local pool default 192.169.50.25 192.169.50.50
```

## Configuring IP Overlapping Address Pools on a GGSN on the Catalyst 6500 / Cisco 7600 Platform with Supervisor II / MSFC2 Example

The following example shows how to configure IP overlapping address pools on the Catalyst 6500 / Cisco 7600 platform

The following examples also show a partial configuration for two VPNs (vpn1 and vpn2) and their associated GRE tunnel configurations (Tunnel1 and Tunnel2).

On the GGSN:

```

service gprs ggsn
!
hostname 6500-7-2
!
ip cef
!
ip vrf vpn1
  description GRE Tunnel 1
  rd 100:1
!
ip vrf vpn2
  description GRE Tunnel 3
  rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface Tunnel1
 description VRF-GRE to PDN 7500(13) Fa0/1
 ip vrf forwarding vpn1
 ip address 50.50.52.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 165.2.1.13
!
interface Tunnel2
 description VRF-GRE to PDN PDN 7200(12) Fa3/0
 ip vrf forwarding vpn2
 ip address 80.80.82.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
router ospf 10
 network 10.1.2.0 0.0.0.255 area 10
 network 150.1.0.0 0.0.255.255 area 10
!
ip local pool vpn1_pool 100.2.0.1 100.2.255.255 group vpn1
ip local pool vpn2_pool 100.2.0.1 100.2.255.255 group vpn2

```

```
ip route vrf vpn1 0.0.0.0 255.255.255.0 Tunnel1
ip route vrf vpn2 0.0.0.0 255.255.255.0 Tunnel2
```

```
gprs access-point-list gprs
  access-point 1
    access-point-name apn.vrf1.com
    access-mode non-transparent
    aaa-group authentication ipdbfms
    ip-address-pool local vpn1_pool
    vrf vpn1
    !
  access-point 2
    access-point-name apn.vrf2.com
    access-mode non-transparent
    aaa-group authentication ipdbfms
    ip-address-pool local vpn2_pool
    vrf vpn2
    !
```

Related configuration on the Supervisor / MSFC2:

```
interface FastEthernet9/5
  no ip address
  switchport
  switchport access vlan 167
  no cdp enable
  !
interface FastEthernet9/10
  no ip address
  switchport
  switchport access vlan 165
  no cdp enable
  !
interface Vlan165
  ip address 165.1.1.1 255.255.0.0
  !
interface Vlan167
  ip address 167.1.1.1 255.255.0.0
  !
! provides route to tunnel endpoints on GGSNs
router ospf 10
  network 10.1.2.0 0.0.0.255 area 10
  !
! routes to tunnel endpoints on PDN
!
ip route 165.2.0.0 255.255.0.0 165.1.1.13
ip route 167.2.0.0 255.255.0.0 167.1.1.12
```

## Configuring the NBNS and DNS Address for an APN

You can configure a primary and secondary NetBIOS Name Service (NBNS) and domain name system (DNS) under an APN. This feature is benefits address allocation schemes where there is no mechanism to obtain these address. Also, for a RADIUS-based allocation scheme, it prevents the operator from having to configure a NBNS and DNS under each user profile.

The NBNS and DNS addresses can come from three possible sources: DHCP server, RADIUS server, or local APN configuration. The criterium for selecting the addresses depends on the IP address allocation scheme configured under the APN. Depending on the configuration, the criterium for selecting the DNS and NBNS addresses is as follows:

1. DHCP-based IP address allocation scheme (local and external)—NBNS address returned from the DHCP server is sent to the MS. If the DHCP server does not return an NBNS address, the local APN configuration is used.
2. RADIUS-based IP address allocation scheme—NBNS address returned from the RADIUS server (in Access-Accept responses) is used. If the RADIUS server does not return an NBNS address, the local APN configuration is used.
3. Local IP Address Pool-based IP address allocation scheme—Local APN configuration is used.
4. Static IP Addresses—Local APN configuration is used.

**Note**

---

The GGSN sends NBNS and DNS addresses in the create PDP response only if the MS is requesting the DNS address in the PCO IE.

---

To specify a primary (and backup) NBNS to be sent in create PDP responses at the access point, use the **nbns primary** access-point configuration command. To remove the NBNS from the access-point configuration, use the **no** form of this command

```
nbns primary ip-address [secondary ip-address]
```

To specify a primary (and backup) DNS to be sent in create PDP responses at the access point, use the **dns primary** access-point configuration command. To remove the DNS from the access-point configuration, use the **no** form of this command

```
dns primary ip-address [secondary ip-address]
```

