CHAPTER 13

Configuring Dynamic Addressing on the GGSN

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

Note Dynamic IP addressing is not supported for IPv6 and PPP PDP types. Therefore, the tasks in this chapter apply to IPv4 PDP contexts only. For information on IPv6 addressing, see Chapter 5, "Configuring IPv6 PDP Support on the GGSN."

For complete descriptions of the GGSN commands in this chapter, see *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. 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

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) or downloaded.

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 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 engine.

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, see *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** command in global configuration mode or the **ip-address-pool** command in access-point configuration mode with the **dhcp-proxy-client** keyword option.

After you configure the access point for DHCP proxy client services, use the **dhcp-server** command in access-point configuration mode 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 use 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

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)# ip address-pool {dhcp-proxy-client | local}`	Specifies an IP address pool mechanism, where: • **dhcp-proxy-client**—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. • **local**—Specifies the local address pool named "default". **Note** There is no default option for the **ip address-pool** command. If you configure a local address pool using the **local** keyword, you can also configure the optional commands in Step 4 and Step 5.
Step 2	`Router(config)# ip dhcp-server {ip-address | name}`	Specifies the IP address or name of a DHCP server.

	Command	Purpose
Step 3	`Router(config)# ip dhcp excluded address low-address [high-address]`	(Optional) Specifies IP addresses that a DHCP server should not assign to DHCP clients, where: • *low-address*—Specifies the first IP address in an excluded address range. This address is typically the address of the DHCP server itself. • *high-address*—(Optional) Specifies the last IP address in the excluded address range.
Step 4	`Router(config)# ip dhcp pool name`	(Optional—Supports **ip address-pool local** command only.) Configures a DHCP address pool, and enters DHCP pool configuration mode, where *name* can be either a symbolic string (such as "engineering") or an integer (such as 0).
Step 5	`Router(config-dhcp)# network network-number [mask | /prefix-length]`	(Optional—Supports **ip address-pool local** 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, see *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 13-4 (Required)
- Specifying a DHCP Server for All Access Points, page 13-5 (Optional)
- Specifying a DHCP Server for a Particular Access Point, page 13-6 (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)# interface loopback` *interface-number*	Defines a loopback interface on the GGSN, where *interface-number* identifies the loopback interface.
Step 2	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	Specifies an IP address for the interface, where: • *ip-address*—Specifies the IP address of the interface in dotted decimal format. • *mask*—Specifies a subnet mask in dotted decimal format. • **secondary**—Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** The *ip-address* 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 **dhcp-gateway-address** value exactly.

Specifying a DHCP Server for All Access Points

When processing DHCP address allocation, the GGSN software first checks to see whether a DHCP server is specified at the access-point configuration level. If a server is 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	`Router(config)# gprs default ip-address-pool {dhcp-proxy-client | radius-client | disable}`	Specifies a dynamic address allocation method using IP address pools for the GGSN, where: • **dhcp-proxy-client**—Specifies that the GGSN dynamically acquires IP addresses for a mobile station (MS) from a DHCP server. Use this keyword to enable DHCP services. • **radius-client**—Specifies that the GGSN dynamically acquires IP addresses for an MS from a RADIUS server. • **disable**—Disables dynamic address allocation by the GGSN. There is no default option for this command.
Step 2	`Router(config)# gprs default dhcp-server {`*ip-address* `|` *name*`} [{`*ip-address* `|` *name*`}]`	Specifies a primary (and backup) DHCP server from which the GGSN obtains IP address leases for mobile users, where: • *ip-address*—Specifies the IP address of a DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server. • *name*—Specifies the hostname of a DHCP server. The second (optional) *name* argument specifies the hostname of a backup DHCP server.

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	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: • **dhcp-proxy-client**—DHCP server provides the IP address pool. • **radius-client**—RADIUS server provides the IP address pool. • **local**—Specifies that a local pool provides the IP address. This option requires that a local pool is configured using the **ip local pool** command in global configuration mode. • **disable**—Turns off dynamic address allocation. **Note** If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.
Step 2	`Router(config-access-point)# dhcp-server {ip-address} [ip-address] [vrf]`	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: • *ip-address*—Specifies the IP address of a DHCP server. The second (optional) *ip-address* argument specifies the IP address of a backup DHCP server. • **vrf**—DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the APN.
Step 3	`Router(config-access-point)# dhcp-gateway-address ip-address`	Specifies the subnet in which the DHCP server should return addresses for DHCP requests for MS users entering a particular PDN access point. **Note** You must configure a corresponding loopback interface with the same IP address as the DHCP gateway address.

Configuring a Local DHCP Server

Note We do not recommend using a local DHCP server on the 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)# ip dhcp ping packets 0`	Specifies that the Cisco IOS DHCP Server sends 0 packets to a pool address as part of a ping operation.
Step 2	`Router(config)# ip dhcp ping timeout 100`	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** command in global configuration mode. 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** command in interface configuration mode.
- Access-point 2 implements VRF using the **vrf** command access-point configuration mode.

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 abc
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
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 abc
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
!
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.

Holdback Timer

The IP local pool holdback timer feature (**recycle delay** keyword option) enables you to configure a specific amount of time a newly released IP address is held before being made available for reassignment. This ensures that an IP address recently released after a PDP session is deleted is not reassigned to another PDP context before the IP-to-user relationship is deleted from all back-end components of the system. If an IP address is reassigned to a new PDP context immediately, the back-end system could incorrectly associate the new user with the record of the previous user, therefore erroneously associating the charging and service access of the new user to the previous user.

The holdback functionality is provided by the support of a new timestamp field added to the pool element data structure. When a request to allocate a specific address is made, if the address is available for reassignment, the current time is checked against the timestamp field of the element. If that number is equal to, or exceeds the number of seconds configured for the recycle delay, the address is reassigned.

When a request is made to allocate the first free address from the free queue, the difference between the current timestamp and the timestamp stored for the element is calculated. If the number is equal to, or exceeds, the configured recycle delay, the address is allocated. If the number is not equal to, or does not exceed the configured recycle delay, the address is not allocated for that request. (The free queue is a first-in first-out [FIFO] queue. Therefore, all other elements will have a great recycle delay than the first element.)

When an address assignment is blocked because an IP address is held for some time, a count of blocked address assignments that is maintained for the local pool is incremented.

Note The holdback timer feature does not support IPv6 local pools.

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

	Command	Purpose
Step 1	`Router(config)#ip local pool {default | pool-name low-ip-address [high-ip-address]} [recycle delay seconds]`	Configures a local pool of IP addresses to use when a remote peer connects to a point-to-point interface, where: • **default**—Default local address pool is used if no other pool is named. • *pool-name*—Name of a specific local address pool. • *low-ip-address*—Lowest IP address in the pool. • *high-ip-address*—(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. • **recycle delay** *seconds*—(Optional) The time, in seconds, addresses should be held before making them available for reassignment.

To assign a local pool to an access-point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# ip-address-pool local pool-name`	(Optional) Specifies that a local pool provides the IP address.

Note Using VRF at the access point, you can configure APNs that use the same IP address pool (overlapping addresses).

Fore more information on configuring VPN access via VRF from an access point, see the "VPN Access Using VRF Configuration Task Lists" section on page 9-13.

To verify the local pool configure, use the **show ip local** [*pool name*] command in privileged EXEC mode:

```
Router#show ip local pool
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Router #show ip local pool poolA
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Available addresses:
10.8.8.1
10.8.8.2
10.8.8.3
10.8.8.4
10.8.8.5

Inuse addresses:
None

Held addresses: Time Remaining
None
```

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

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

For more information about the ip-address-pool access-point configuration command, see "Configuring Additional Real Access Point Options" section on page 9-20. For more information about configuring RADIUS, see *Cisco IOS Security Configuration Guide*.

Configuring Overlapping Local IP Address Pools

The Overlapping Local IP 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.

Overlapping Local IP 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 non overlapping 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	`Router(config)#ip local pool {default | pool-name} [low-ip-address [high-ip-address]] [group group-name]`
	
	Example:
	`GGSN(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000`
		Configures a local pool of IP addresses to use when a remote peer connects to a point-to-point interface, where:
		• **default**—Defaults local address pool that is used if no other pool is named.
		• *pool-name*—Name of a specific local address pool.
		• *low-ip-address*—Lowest IP address in the pool.
		• *high-ip-address*—(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.
		• **group** *group-name*—(Optional) Creates a pool group.

Step 2	`Router(config)# show ip local pool [poolname | [group group-name]]`
	
	Example:
	`GGSN(config)# show ip local pool group testgroup testpool`
		Displays statistics for any defined IP address pools.

Overlapping Local IP Address Pools Configuration Examples

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

- Defining Local Address Pooling as the Global Default, page 13-14
- Configuring Multiple Ranges of IP Addresses into One Pool Example, page 13-14
- Configuring IP Overlapping Address Pools on a GGSN on the Cisco 7600 Platform with Supervisor II / MSFC2 Example, page 13-14

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 Cisco 7600 Platform with Supervisor II / MSFC2 Example

The following example shows how to configure IP overlapping address pools on the 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 7600-7-2
!
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 x(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 criterion for selecting the addresses depends on the IP address allocation scheme configured under the APN. Depending on the configuration, the criterion 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** command in access-point configuration mode. 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** command in access-point configuration mode. To remove the DNS from the access-point configuration, use the **no** form of this command

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

Using Dynamic IP Address Management on the Cisco GGSN

With Cisco GGSN Release 10.0 and later, the Dynamic IP Address Management feature enables dynamic IP address allocation to support operators who might not initially know the IP address range of a subscriber, and therefore, the routing table cannot be preconfigured on the supervisor module to provide the proper routing of downlink traffic.

Cisco GGSN Release 10.0 and later introduces a *subnet manager* function that enables the dynamic creation of subnet routes . This enables multiple host routesto be aggregated into a single subnet route. Dynamic subnet routes are created only in an eGGSN implementation when Cisco CSG2 is present. Dynamic subnets cannot be created in a non-eGGSN implementation.

When configuring dynamic IP address management:

- Routing entries are dynamically created.
- OSPF routing protocol is used to propagate dynamic routes from the PCOP to the supervisor in a non-eGGSN implementation. In an eGGSN implementation, OSPF on the Cisco CSG2 propagates the routes to the supervisor.
- Dynamic subnet creation is only supported in an eGGSN implementation when a Cisco CSG2 is present and reduces the total number of dynamic routing entries.
- In both eGGSN and non eGGSN implementations, pre-existing aggregate route schemes are supported.
- Dynamic routes are synchronized to the standby GGSN.

Subnet Management in an Enhanced GGSN Implementation

In an eGGSN implementation with the Cisco CSG2, when a default subnet mask is specified under an APN, dynamic subnet creation is automatically enabled.

During the create PDP context process, once the IP address of a subscriber is determined (via a local pool, DHCP, or RADIUS), the Cisco GGSN subnet manager attempts to match the IP address with one of the configured aggregate routes. The aggregate routes can be under the APN, or globally defined if **aggregate auto** is enabled.

The selection rules give the highest priority to Framed-IP-Address/Mask attributes in Radius Access Requests, followed by APN aggregate routes, and then global aggregate routes. If none of those are matched, the Cisco GGSN applies the APN default subnet mask, if configured, to generate a dynamic subnet route. If you have not configured a default subnet mask under an APN, the Cisco GGSN uses the host route.

Once the route is determined, the Cisco GGSN invokes a Cisco CSG2 *load balancing* (see "Configuring Cisco CSG2 Load Balancing" section on page 8-43). The Cisco CSG2 load balancing determines the serving Cisco CSG2 for the given subscriber IP address and subnet mask. The same Cisco CSG2 is selected across Cisco SAMIs if the Cisco CSG2 and subscriber IP address and subnet mask configuration is identical in the same APN.

When the Cisco CSG2 is selected, the Cisco GGSN sends the Accounting-Start messages to the selected Cisco CSG2, along with a new route-info VSA that includes the subscriber IP address and subnet mask. The Cisco CSG2 propagates the subnet route to the supervisor via OSPF.

Subnet Management in an Non Enhanced GGSN Implementation

Dynamic subnet creation is disable in a non-eGGSN implementation. If a default subnet mask is configured under an APN, it is ignored.

During the create PDP context processing, when the IP address of a subscriber is determined (via local pool, DHCP, or RADIUS), the subnet manager attempts to match the IP address with one of the configured aggregate routes. The aggregate rouates can be under the APN, or globally defined if aggregate-auto is enabled.

The selection rules give the highest priority to Framed-IP-Address/Mask attributes in Radius Access Requests, followed by APN aggregate routes, and then global aggregate routes. If none of those match, a host route is created.

The Cisco GGSN propagates the downlink route to the supervisor.

Enabling Mobile Routes on the GGSN

To support dynamic IP address management, before the creation of any PDP contexts, you must configure the **router mobile** command in global configuration mode on the Cisco GGSN to enable mobile routes.

Note The **router mobile** command is an existing Cisco IOS command that is used in a Cisco GGSN and Cisco CSG2 implementation to *only* enable the dynamic IP address manager feature. The Cisco GGSN utilization of the **router mobile** command is not related to any other Cisco IOS **router mobile** command usage. No other routing mobile subcommand is supported on the Cisco GGSN.

In the service-aware GGSN implementation, the **router mobile** command in global configuration mode enables the GGSN to manage routing entries for subscribers more efficiently. These entries are idefintified by the leter “M” in the routing table displayed using the **show ip route** command. When OSPF is enabled, these routing entries can be propagated to a routing peer.

To enable mobile routes on the Cisco GGSN, use the following command:

Command	Purpose
`Router(config)# router mobile`	Enables mobile routes on the Cisco GGSN.

To display the routes, use **show ip route** command in privileged EXEC mode:

```
GGSN-8#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C       20.1.1.23 is directly connected, Loopback1
     23.0.0.0/16 is subnetted, 1 subnets
M       23.23.0.0 [1/0] via 0.0.0.0, 00:17:11, Virtual-Access3
```

Configuring a Default Subnet Mask for Dynamic Subnet Management

To configure a default subnet mask under an APN, and enable dynamic IP address management in an eGGSN implementation with a Cisco CSG2, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# aggregate 0.0.0.0 sub-mask`	Configures a default subnet mask for subnet management and enables dynamic subnet creation.

Disabling Route Propagation from the Cisco GGSN to the Supervisor

By default, route distribution is enabled. However, for an eGGSN implementation, OSPF route redistribution is not required and should be disabled because the Cisco CSG2 propagates downlink routes to the supervisor.

To configure the Cisco GGSN to not propagate downlink routes to the supervisor, use the following command in access-point configuration mode:

	Command	Purpose
Step 3	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client [no-redistribute] | local pool-name | disable}`	Specifies a dynamic address allocation method using IP address pools for the current access point, where: • **dhcp-proxy-client—**The access point IP address pool is allocated using a DHCP server • **radius-client**—The access point IP address pool is allocated using a RADIUS server. Optionally, specify the **no-redistribute** keyword option to disable • route propagation from the Cisco GGSN to the supervisor. • **local**—The access point IP address pool is allocated using a locally configured address pool. • **disable**—Disables dynamic address allocation for this access point.

Configuration Examples

The following are dynamic ip address management configuration examples:

```
gprs access-point-list gprs
  access-point 1
   access-point-name static-ip
   access-mode non-transparent
   aaa-accounting interim update
   aaa-group authentication ra_aaa
   aaa-group accounting ra_aaa
   csg-group csg1
```

```
 csg-group csg2
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 2
 access-point-name dhcp-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool dhcp-proxy-client
 csg-group csg1
 aggregate 0.0.0.0 255.255.0.0
 dhcp-server 172.64.110.38
 dhcp-gateway-address 172.69.69.1
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 3
 access-point-name radius-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool radius-client no-redistribute
 csg-group csg1
 aggregate 0.0.0.0 255.255.0.0
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 !
access-point 4
 access-point-name localpool-ip
 access-mode non-transparent
 aaa-accounting interim update
 aaa-group authentication ra_aaa
 aaa-group accounting ra_aaa
 ip-address-pool local ra_localpool
 csg-group csg1
 aggregate 0.0.0.0 255.255.255.255
 gtp response-message wait-accounting
 charging profile any 1 override
 service-aware
 advertise downlink next-hop 7.19.18.103
 !
access-point 5
 access-point-name dhcpvrf-ip
 ip-address-pool dhcp-proxy-client
 csg-group csg1
 dhcp-server 172.64.110.38
 dhcp-gateway-address 169.69.69.1
 !
access-point 6
 access-point-name dhcp-ip2
 ip-address-pool dhcp-proxy-client
 aggregate 172.0.0.0 255.0.0.0
 dhcp-server 172.64.110.38
 dhcp-gateway-address 172.69.69.1
 !
!
```