



CHAPTER 12

Configuring Dynamic Addressing on the GGSN

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



Note

The tasks in this chapter apply to IPv4 PDP contexts only. For information on IPv6 addressing, see [Chapter 4, “Configuring IPv6 PDP Support on the GGSN.”](#)

For complete descriptions of the GGSN commands in this chapter, refer to the *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, page 12-1](#)
- [Configuring DHCP on the GGSN, page 12-2](#)
- [Configuring MS Addressing via Local Pools on the GGSN, page 12-10](#)
- [Configuring MS Addressing via RADIUS, page 12-12](#)
- [Configuring the NBNS and DNS Address for an APN, page 12-13](#)

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, 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 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, page 12-3](#)
- [Configuring DHCP at the GGSN Global Configuration Level, page 12-4](#)
- [Configuring a Local DHCP Server, page 12-8](#)
- [Configuration Example, page 12-8](#)

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)# ip address-pool { dhcp-proxy-client local } | Specifies an IP address pool mechanism, where: <ul style="list-style-type: none"> • 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”. <p>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.</p> |
| Step 2 | Router(config)# ip dhcp-server { <i>ip-address</i> <i>name</i> } | Specifies the IP address or name of a DHCP server. |

| | Command | Purpose |
|--------|---|--|
| Step 3 | Router(config)# ip dhcp excluded address <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"> <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. <i>high-address</i>—(Optional) Specifies the last IP address in the excluded address range. |
| Step 4 | Router(config)# ip dhcp pool <i>name</i> | (Optional—Supports ip address-pool local 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)# network <i>network-number</i> [<i>mask</i> <i>/prefix-length</i>] | (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, 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 12-4](#) (Required)
- [Specifying a DHCP Server for All Access Points, page 12-5](#) (Optional)
- [Specifying a DHCP Server for a Particular Access Point, page 12-6](#) (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 <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)# ip address <i>ip-address mask</i> [secondary] | <p>Specifies an IP address for the interface, where:</p> <ul style="list-style-type: none"> • <i>ip-address</i>—Specifies the IP address of the interface in dotted decimal format. • <i>mask</i>—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. <p>Note 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 dhcp-gateway-address 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 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 | <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"> • 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. <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"> • <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. • <i>name</i>—Specifies the hostname of a DHCP server. The second (optional) <i>name</i> 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 | <pre>Router(config-access-point)# ip-address-pool {dhcp-proxy-client radius-client local <i>pool-name</i> 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"> • 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. <p>Note 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 <i>ip-address</i> [<i>ip-address</i>] [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"> • <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. • vrf—DHCP server uses the VPN routing and forwarding (VRF) table that is associated with the APN. |
| Step 3 | <pre>Router(config-access-point)# dhcp-gateway-address <i>ip-address</i></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>Note You must configure a corresponding loopback interface with the same IP address as the DHCP gateway address.</p> |

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** 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 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 | <pre>Router(config)#ip local pool {default pool-name low-ip-address [high-ip-address]} [recycle delay seconds]</pre> | <p>Configures a local pool of IP addresses to use when a remote peer connects to a point-to-point interface, where:</p> <ul style="list-style-type: none"> • default—Default local address pool is used if no other pool is named. • <i>pool-name</i>—Name of a specific local address pool. • <i>low-ip-address</i>—Lowest IP address in the pool. • <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. • 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 |
|---------------|---|---|
| Step 1 | <pre>Router(config-access-point)# ip-address-pool local pool-name</pre> | (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).

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 8-13.

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** access-point configuration command.

For more information about the **ip-address-pool** access-point configuration command, see [“Configuring Additional Real Access Point Options” section on page 8-20](#). For more information about configuring RADIUS, see the *Cisco IOS Security Configuration Guide*.

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** 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]
```

