

DHCP Service Configuration Mode Commands

The Dynamic Host Control Protocol (DHCP) Configuration Mode is used to create and manage DHCP service instances for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- allow, on page 2
- bind, on page 3
- default, on page 5
- dhcp chaddr-validate, on page 6
- dhcp client-identifier, on page 7
- dhcp deadtime, on page 9
- dhcp detect-dead-server, on page 10
- dhcp ip, on page 11
- dhcp server, on page 12
- dhcp server selection-algorithm, on page 14
- dhcpv6-client-unicast, on page 15
- end, on page 16
- exit, on page 16
- lease-duration, on page 16
- lease-time, on page 17
- max-retransmissions, on page 18
- retransmission-timeout, on page 19
- T1-threshold, on page 20
- T2-threshold, on page 20

allow

Allows the specified options on the DHCP service.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

`[ no ] allow { dhcp-client rapid-commit | dhcp-inform | dhcp-parameter-request-list-option { router | subnet-mask } | dhcp-relay-agent-auth-suboption | dhcp-relay-agent-option | dhcp-server rapid-commit }`

no

Disables an option on the DHCP service.

dhcp-client rapid-commit

Enables support of the rapid commit feature for DHCP client functionality, as defined in RFC 4039.

dhcp-inform

Enables the sending of DHCP inform after configuration for address recovery.

dhcp-parameter-request-list-option { router | subnet-mask }

Enables the sending of DHCP parameter request list option in all outgoing messages.

router: Send DHCP parameter request list option with router flag in all outgoing messages.

subnet-mask: Send DHCP parameter request list option with subnet mask flag in all outgoing messages.

dhcp-relay-agent-auth-suboption

Enables the sending of DHCP relay agent authentication suboption in all outgoing messages.

dhcp-relay-agent-option

Enables the sending of DHCP relay agent option in all outgoing messages.

dhcp-server rapid-commit

Enables support of the rapid commit feature for DHCP server functionality, as defined in RFC 4039.

Usage Guidelines Use this command to enable/disable options on the DHCP service.

Example

The following command enables support of the rapid commit feature for DHCP server functionality:

```
allow dhcp-server rapid-commit
```

bind

Binds the DHCP service to a logical IP interface facilitating the system's connection to the DHCP server. This command also configures traffic from the specified DHCP service bind address to use the specified Multiple Protocol Label Switching (MPLS) labels.

Product

ASN-GW

eWAG

GGSN

HA

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
bind address ip_address [ nexthop-forwarding-address nexthop_ip_address [
mpls-label input in_mpls_label_value output out_mpls_label_value1 [
out_mpls_label_value2 ] ] ]
no bind address ip_address
```

no

Removes a previously configured binding.

address *ip_address*

Specifies the IP address of an interface in the current context through which communication with the DHCP server occurs.

ip_address must be expressed in IPv4 dotted-decimal notation.

Important In the case of DeWAG service, this IP address must be the same as the IP address configured with the **dhcp server** CLI command under the same DHCP Service Configuration mode. Also, this IP address must match the DeWAG service's IP address so that the WLC can relay the DHCP unicast packets to the DeWAG service IP address and are processed by this DHCP service.

nexthop-forwarding-address *nexthop_ip_address*

Specifies the next hop gateway address for in MPLS network to which the packets with MPLS labels will be forwarded.

nexthop_ip_address must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Important In the case of DeWAG service, this option must not be configured.

mpls-label input *in_mpls_label_value*

Specifies the MPLS label to identify inbound traffic destined for the configured DHCP service bind address *ip_address*.

in_mpls_label_value is the MPLS label that will identify inbound traffic destined for the configured DHCP service and must be an integer from 16 through 1048575.

Important This keyword is license-enabled and available with valid MPLS feature license only.

Caution For DHCP over MPLS feature to work in StarOS 9.0 onward the **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started as a part of a DHCP over MPLS configuration. In release 9.0 onward this keyword is a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Important In the case of DeWAG, this option must not be configured.

output *out_mpls_label_value1* [*out_mpls_label_value2*]

Adds the MPLS label to the outbound traffic sent from the configured DHCP service bind address *ip_address*. The labels *out_mpls_label_value1* and *out_mpls_label_value2* identify the MPLS labels to be added to packets sent from the specified dhcp service bind address.

out_mpls_label_value1 is the inner output label and must be an integer from 16 through 1048575.

out_mpls_label_value2 is the outer output label and must be an integer from 16 through 1048575.

Important This keyword is license-enabled and available with valid MPLS feature license only.

Important In the case of DeWAG, this option must not be configured.

Usage Guidelines

Use this command to associate or tie the DHCP service to a specific logical IP address previously configured in the current context and bound to a port. Once bound, the logical IP address or interface is used in the giaddr field of the DHCP packets.

When this command is executed, the DHCP service is started and begins the process of requesting addresses from the DHCP server and storing them in cache memory for allocation to PDP contexts.

This command can also be used to configure MPLS labels for inbound and outbound traffic through this DHCP address.

Only one interface can be bound to a service.

For DHCP over MPLS feature to work in StarOS 9.0 onward **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started.

Caution As a part of DHCP over MPLS configuration, the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

The following command binds the DHCP service to the interface with an IP address of 1*192.51.1.210*:

```
bind address 192.51.1.210
```

default

Restores DHCP service parameters to their factory default settings.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
default { T1-threshold | T2-threshold | dhcp { chaddr-validate |
client-identifier | deadtime | detect-dead-server { consecutive-failures
 } | server selection-algorithm } | lease-duration | max-retransmissions
 | retransmission-timeout }
```

dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-algorithm }

Restores the following DHCP parameters to their respective default settings:

- **deadtime**: Default 10 minutes
- **detect-dead-server** { **consecutive-failures** }: Default 5
- **server-selection-algorithm**: Default First-server

lease-duration

Restores the lease-duration parameter to its default setting of 86400 seconds.

max-retransmissions

Restores the max-retransmissions parameter to its default setting of 5.

retransmission-timeout

Restores the retransmission-timeout parameter to its default setting of 3000 milli-seconds.

T1-threshold

Restores the T1-threshold parameter to its default setting of 50%.

T2-threshold

Restores the T2-threshold parameter to its default setting of 88%.

Usage Guidelines

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

Example

The following command restores the DHCP deadtime parameter to its default setting of 10 minutes:

```
default dhcp deadtime
```

dhcp chaddr-validate

Configures the behavior of the client hardware address (chaddr) validation in DHCP messages.

Product

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcp-service)#`

Syntax Description

`[ default | no ] dhcp chaddr-validate`

default

Validates the chaddr value received in a DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

no

Disables validation of the chaddr value received in DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

Important The chaddr information value in the DHCPACK message will be parsed but not be validated against the value maintained with client. The chaddr information value in DHCPACK will be ignored and not be stored internally.

Usage Guidelines

Use this command to configure behavior relating to the validation of chaddr information validation in the DHCPACK messages.

Example

The following command specifies that the chaddr will not be validated in the DHCP messages:

`no dhcp chaddr-validate`

dhcp client-identifier

Configures the behavior relating to inclusion of a client identifier DHCP option in DHCP messages.

Product

GGSN

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp client-identifier { ike-id | link-layer-identifier | mac-address | msisdn | none }
default dhcp client-identifier

default

Sets the behavior of DHCP client identifier to default – do not to include client identifier option in any DHCP message.

ike-id

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Specifies the Internet Key Exchange Protocol version 2 id of HNB as the DHCP client-identifier option in any DHCP message to DHCP server in Discover and Request messages.

Important This keyword is HNB-GW license controlled.

link-layer-identifier

Specifies the subscribers link-layer-identifier as the DHCP client-identifier option in the DHCP message,

mac-address

Specifies the subscribers mac-address as the DHCP client-identifier option in any DHCP message.

msisdn

Specifies that the subscriber's MSISDN be included in the client-identifier option of the relevant DHCP messages. Default: disabled

Important This keyword is GGSN and P-GW/SAEGW license controlled.

none

Specifies that DHCP client-identifier option would not be included in any DHCP messages. This is the default behavior. Default: enabled

Usage Guidelines

Use this command to configure behavior relating to inclusion or exclusion of DHCP client identifier option from DHCP messages.

Example

The following command specifies that DHCP client-identifier option be excluded from DHCP messages:

```
dhcp client-identifier none
```

dhcp deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCP server that was previously marked as down.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp deadtime *max_time*

max_time

Specifies the maximum amount of time (in minutes) to wait before communicating with a DHCP server that was previously unreachable. *max_time* is an integer value from 1 through 65535. Default: 10

Usage Guidelines

If the system is unable to communicate with a configured DHCP server, after a pre-configured number of failures the system marks the server as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.

Important If all DHCP servers are down, the system will immediately treat all DHCP servers as active, regardless of the deadtime that is specified.

Refer to the **dhcp detect-dead-server** and **max-retransmissions** commands for additional information on the process the system uses to mark a server as down.

Example

The following command configures the system to wait *20* minutes before attempting to re-communicate with a dhcp server that was marked as down:

```
dhcp deadtime 20
```

dhcp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCP server as down.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp detect-dead-server consecutive-failures *max_number*

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a DHCP server as down as an integer from 1 through 1000. Default: 5

Usage Guidelines

This command works in conjunction with the *max-retransmissions* parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.

The *max-retransmissions* parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.

If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority server again.

If the system receives a message from a DHCP server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow *8* consecutive communication failures with a DHCP server before it marks it as down:

```
dhcp detect-dead-server consecutive-failures 8
```

dhcp ip

Associates the specific DHCP service with a pre-configured Virtual Routing and Forwarding (VRF) Context instance for virtual routing and forwarding.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

[no] dhcp ip { vrf *vrf_name* **| skip-validation }**

no

Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

vrf_name

Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service. *vrf_name* is the name of a pre-configured VRF context configured in Context Configuration mode and associated with the IP Pool used by the DHCP service.

By default the VRF is NULL, which means that DHCP service is bound with binding address given by **bind address** command only.

skip-validation

Disables the IP validation for received IPv4 address from the external DHCP server.

Usage Guidelines

Use this command to enable the DHCP-over-MPLS support and to associate/disassociate a pre-configured VRF context to a DHCP service for this feature.

VRF is not a critical parameter for the DHCP Service but bind address is a critical parameter for DHCP Service, and while starting DHCP Service, if this command is configured, then the bind address should be present in that VRF, and If this command is not configured, bind address should be present in the context where DHCP Service is configured.

For the DHCP over MPLS feature to work in StarOS 9.0 onward this command must be configured in the DHCP service. Without this command the DHCP service using MPLS labels will not be started.



Caution As a part of this configuration the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

Following command associates VRF context instance *dhcp_vrf1* with this DHCP service:

```
dhcp ip vrf dhcp_vrf1
```

dhcp server

Configures DHCP servers with which the DHCP service is to communicate.

Product

ASN-GW

eWAG

GGSN

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
 [ no ] dhcp server { ip_address enable-discovery  { slot/port slot_port_number
 dhcp-node-id node_id }| port port_num [ priority priority ]
default dhcp port
```

default

Sets the default value of UDP port on DHCP server; 67 for DHCP messaging.

no

Deletes a previously configured DHCP server.

ip_address

Specifies the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.



Important In the case of DeWAG service, this IP address must be the same as the IP address configured with the **bind address** CLI command under the same DHCP Service Configuration mode.

enable-discovery { slot/port *slot_port_number* dhcp-node-id *node_id* }

Specifies the slot or port number of the UPF and the node Id of the DHCP server.

port *port_num*

Specifies the port number to send DHCP messages to non-standard UDP ports of the server if multiple servers are configured.

port_num is an integer from 0 through 65535.



Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.



Important While configuring HNB-GW for DHCP proxy support, operator must define 61610 as UDP port for DHCP server. The source port used by HNBGW will be standard DHCP port, irrespective of the server port that is configured.

priority *priority*

Specifies the priority of the server if multiple servers are configured.

priority is an integer from 1 through 1000. 1 is the highest priority.



Important In the case of DeWAG, this option must not be configured.

Usage Guidelines

Use this command to configure the DHCP server(s) that the system is to communicate with. Multiple servers can be configured each with their own priority. Up to 20 DHCP servers can be configured.

All DHCP messages are sent/received on UDP port 67.

Important If a server is removed, all calls having an IP address allocated from the server will be released.

Example

The following command configures a DHCP server with an IP address of *192.51.1.200* and a priority of *1*:

```
dhcp server 192.51.1.200 priority 1
```

dhcp server selection-algorithm

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Product

GGSN

ASN-GW

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
dhcp server selection-algorithm { first-server | round-robin | use-all }
```

first-server

Uses the first-server algorithm. This algorithm dictates that the system select the DHCP servers according to their priority starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable. Default: Enabled

round-robin

Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server's configured priority starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server. Default: Disabled

use-all

Default: Disabled

This algorithm dictates that the system to communicate with all the DHCP servers configured on system.

Usage Guidelines

Use this command to determine how configured DHCP servers are utilized by the system.

Example

The following command configures the DHCP service to use the round-robin selection algorithm:

```
dhcp server selection-algorithm round-robin
```

dhcpv6-client-unicast

Enables or disables the DHCPv6 client unicast or multicast mode towards the external DHCP server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > **context** *context_name* > **dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

{ enable | disable } dhcpv6-client-unicast slot/port *slot_port_number*

dhcpv6-client-unicast

Enables client to send messages on unicast address towards the server.

Usage Guidelines

Use this command to send messages on unicast address towards the server.

slot/port *slot_port_number*

Define the slot or port number for DHCPv6 client profile mulicast mode.

Example

The following command specifies that messages are sent on multicast address to external DHCP servers:

```
disable dhcpv6-client-unicastslot/port 1/11
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines Use this command to return to the parent configuration mode.

lease-duration

Configures the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.

Product GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

lease-duration min *min_time* **max** *max_time*

min *min_time*

Specifies the minimum acceptable lease time (in seconds) as an integer from 600 trough 3600. Default: 600

max *max_time*

Specifies the maximum acceptable lease time (in seconds) as an integer from 10800 through 4294967295. Default: 86400

Usage Guidelines

To reduce the call setup time, the system requests IP addresses from the DHCP server in blocks rather than on a call-by-call basis. Each address received has a corresponding lease time, or time that it is valid. The values configured by command represent the minimum and maximum times that the system allows and negotiates for the lease(s).

If the DHCP server responds with values that are out of the range specified by the min and max values, the system accumulates warning statistics. Responses that fall below the minimum value are rejected by the system and the system contacts the DHCP server with the next highest priority. Responses that are greater than the maximum value are accepted.

When half of the lease time has expired, the system automatically requests a lease renewal from the DHCP server. This is configured using the **T1-threshold** command.

Example

The following command configures the minimum allowable lease time for the system to be *1000* and the maximum to be *36000*:

```
lease-duration min 1000 max 36000
```

lease-time

Configures the local DHCP Server lease time in seconds.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

lease-time *time*
default lease-time

default

Returns the command to its default setting of 600.

time

Specifies the IP address lease time from the local DHCP server (in seconds) as an integer from 600 through 4294967295. Default: 600

Usage Guidelines

Use this command to configure the lease time of the IP address from the local DHCP server.

Example

The following command sets the lease time of the IP address from the local DHCP server to 20 minutes (1200 seconds):

```
lease-time 1200
```

max-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCP server before it is considered a failure.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

max-retransmissions *max_number*

max_number

Specifies the maximum number of re-attempts the system tries when no response is received from a DHCP server. *max_number* is an integer from 1 through 20. Default: 5

Usage Guidelines

This command works in conjunction with the **dhcp detect-dead-server** parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.

When the value specified by this parameter is met, a failure is logged. The **dhcp detect-dead-server** command specifies the number of consecutive failures that could occur before the server is marked as down.

In addition, the **retransmission-timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of times the system re-attempts communication with a DHCP server that is unresponsive to *5*:

```
max-retransmissions 5
```

retransmission-timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the DHCP server.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

retransmission-timeout *time*

time

Specifies the time that the system waits (in milliseconds) before reattempting communication with the DHCP server. *time* is an integer from 100 through 20000. Default: 10000

Usage Guidelines

This command works in conjunction with the **max-retransmissions** command to establish a limit on the number of times that communication with a DHCP server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *1000* milliseconds:

```
retransmission-timeout 1000
```

T1-threshold

Configures the DHCP T1 timer as a percentage of the allocated IP address lease.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

T1-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "RENEWING". *percentage* is an integer from 40 through 66. Default: 50

Usage Guidelines

This command is used to identify the time at which a subscriber must renew their DHCP lease as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 40%, then the subscriber would enter the RENEWING state after 4800 seconds.

Example

The following command configures the T1 threshold to *40*%:

```
T1-threshold 40
```

T2-threshold

Configures the DHCP T2 timer as a percentage of the allocated IP address lease.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

T2-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "REBINDING". *percentage* is an integer from 67 through 99. Default: 88

Usage Guidelines

This command is used to identify the time at which a subscriber re-binds their DHCP leased IP address as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 70%, then the subscriber would enter the REBINDING state after 8400 seconds.

Example

The following command configures the T2 threshold to *70*%:

T2-threshold 70 *70*