



CHAPTER 9

Configuring PPP Support on the GGSN

The gateway GPRS support node (GGSN) supports the GPRS tunneling protocol (GTP) with the Point to Point Protocol (PPP) in three different ways. The different types of PPP support on the GGSN are differentiated by where the PPP endpoints occur within the network, whether Layer 2 Tunneling Protocol (L2TP) is in use, and where IP packet service occurs. This chapter describes the different methods of PPP support on the GGSN and how to configure those methods.

For a complete description 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.

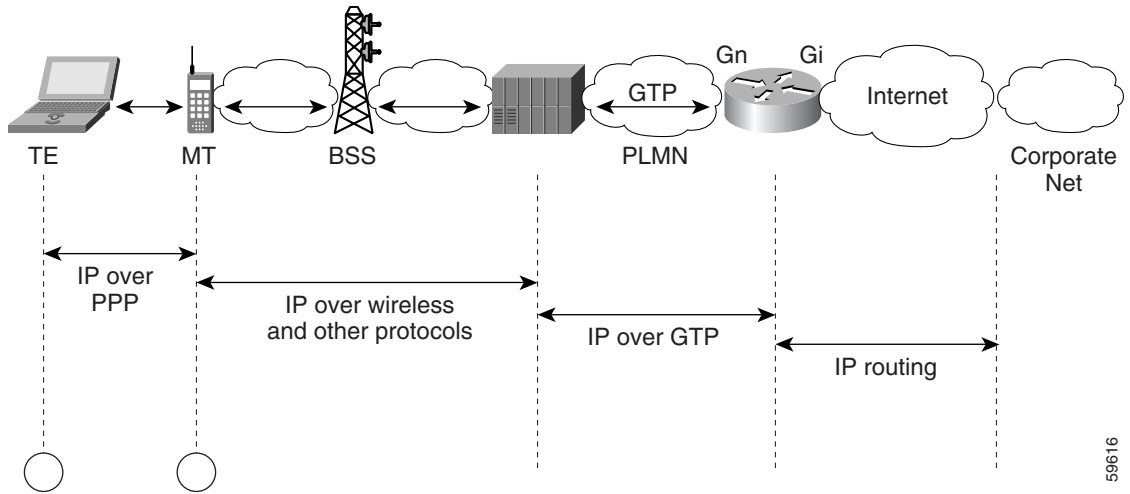
This chapter includes the following sections:

- [Overview of PPP Support on the GGSN, page 9-1](#)
 - [Configuring GTP-PPP Termination on the GGSN, page 9-3](#)
 - [Configuring GTP-PPP with L2TP on the GGSN, page 9-7](#)
 - [Configuring GTP-PPP Regeneration on the GGSN, page 9-14](#)
 - [Monitoring and Maintaining PPP on the GGSN, page 9-21](#)
 - [Configuration Examples, page 9-22](#)

Overview of PPP Support on the GGSN

Before GGSN Release 3.0, the GGSN supported a topology of IP over PPP between the terminal equipment (TE) and mobile termination (MT). Only IP packet services and routing were supported from the MT through the serving GPRS support node (SGSN), over the Gn interface and the GTP tunnel to the GGSN, and over the Gi interface to the corporate network. No PPP traffic flow was supported over the GTP tunnel or between the GGSN and the corporate network.

Figure 9-1 IP Over GTP Topology Without PPP Support on the GGSN



The PPP packet data protocol (PDP) type was added to the GSM standards in GSM 04.08 version 7.4.0 and GSM 09.60 version 7.0.0. PPP is a Layer 2 protocol that is widely used in a variety of WAN environments, including Frame Relay, ATM, and X.25 networks.

PPP provides security checking through the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), and it uses the IP Control Protocol (IPCP) sublayer to negotiate IP addresses. Perhaps the most important characteristic of PPP support within the general packet radio service/Universal Mobile Telecommunication System (GPRS/UMTS) network is PPP's tunneling capability through a virtual private data network (VPDN) using L2TP. Tunneling allows PPP sessions to be transported through public networks to a private corporate network, without any security exposure in the process. Authentication and dynamic IP address allocation can be performed at the edge of the corporate network.

The Cisco GGSN provides the following three methods of PPP support on the GGSN:

- GTP-PPP
- GTP-PPP with L2TP
- GTP-PPP Regeneration


Note

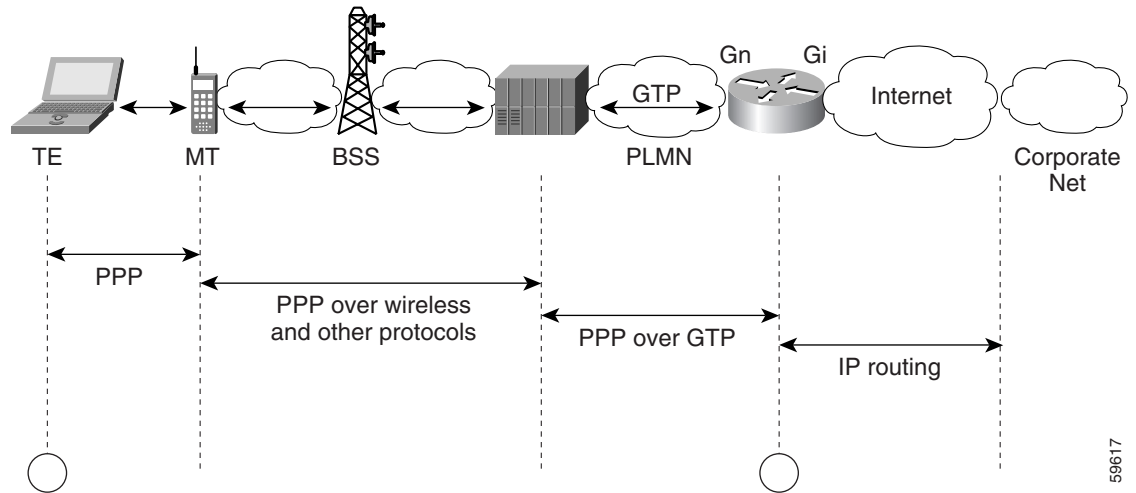

Note

Configuring GTP-PPP Termination on the GGSN

-
-
-
-

Overview of GTP-PPP Termination on the GGSN

Figure 9-2 PPP Over GTP Topology With PPP Termination at the GGSN



59617

Benefits

-
-
-

Preparing to Configure PPP over GTP on the GGSN

- - Be sure that users are configured on the RADIUS server using the complete username@domain format.
 - Specify the **no peer default ip address**

[“Configuring](#)

[Security on the GGSN”](#) chapter in this guide.

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**

```
aaa authorization network method_list
```

method_list

pool-name

onfiguration Task List

-
-
-

Configuring a Loopback Interface

	Command	Purpose
Step 1	Router(config)# interface loopback <i>interface-number</i>	<i>interface-number</i>
Step 2	Router(config-if)# ip address <i>ip-address mask</i> [secondary]	—Specifies the IP address of the interface in dotted decimal format. <i>mask</i> secondary

Configuring a PPP Virtual Template Interface

show running-config



<pre>interface virtual-template</pre>	<pre>ppp vtemplate</pre>
<pre>type number</pre>	<pre>type number</pre>
<p>Step 3</p> <pre>peer default ip address dhcp</pre> <pre>peer default ip address</pre> <pre>pool pool-name</pre>	
<p>Step 4</p>	<p>Note</p>
<p>Step 5</p> <pre>[] { [] }</pre>	<pre>[]—Enables PAP, CHAP, or both on the interface.</pre> <pre>—Name of the method list created with the command.</pre>



Associating the Virtual Template Interface for PPP on the GGSN

Command	Purpose
<code>gprs gtp ppp vtemplate</code>	Note

Configuring GTP-PPP with L2TP on the GGSN

•
•

Overview of GTP-PPP with L2TP on the GGSN

[Configuring a PPP Virtual Template Interface, page 9-12 \(Required\)](#)

[Associating the Virtual Template Interface for PPP on the GGSN, page 9-13 \(Required\)](#)

When you use L2TP services on the GGSN to the LNS in the corporate network, you need to configure the GGSN as a LAC by enabling VPDN services on the GGSN.

For more information about VPDN configuration and commands in the Cisco IOS software, refer to the *Cisco IOS Dial Technologies Configuration Guide Command Reference*

	<i>group-number</i>	
	Router(config- <i>vpdn</i>)# request-dialin	
	Router(config- <i>vpdn-req-in</i>)# protocol l2tp	
	domain	
Step 6	exit	
Step 7	<i>limit-number</i> <i>priority-number</i> <i>ip-address</i>	
Step 8		



You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the **vpdn enable**

Configuring AAA Services for L2TP Support



Note

Step 1

Command	Purpose
local aaa authorization network default	

<pre> aaa authorization network default } [...] </pre>	<p><i>list-name—</i></p> <p><i>group-name—</i></p> <p><i>group-name</i></p>
<pre> Router(config)# </pre>	<p><i>name</i></p> <p><i>ciscouser</i></p> <p><i>ciscouser@corporate1.com</i></p> <p><i>ciscouser@corporate2.com</i></p>





	<i>interface-number</i>
	<i>ip-address</i> <i>mask</i>







	<i>number</i>
	<i>number</i>
	<i>type number</i>
<i>protocol2</i>	<i>list-name</i> <i>protocol1</i>

<i>number</i>	

Configuring GTP-PPP Regeneration on the GGSN

•
•

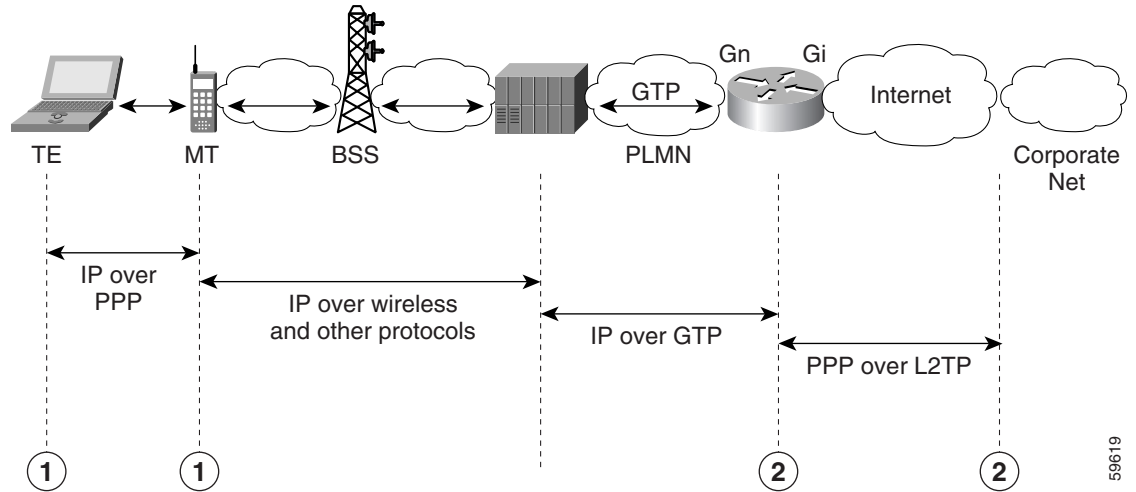
Overview of GTP-PPP Regeneration on the GGSN

Restrictions

•
•
•


Caution

Figure 9-4 PPP Regeneration Topology on the GGSN



59619

<i>characters</i>	<p>Available characters are %, -, @, \, #, and /. The default is @.</p> <p>If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).</p>
	Defines a VPDN group, and enters VPDN group configuration mode.
	Enables the router or instance of Cisco IOS software to request dial-in tunnels, and enters request dial-in VPDN subgroup configuration mode.
	Specifies use of the L2TP protocol for dial-in tunnels.
	Specifies that users with this domain name will be tunneled. Configure this command for every domain name you want to tunnel.
	Returns you to VPDN group configuration mode.
	Specifies the destination IP address for the tunnel.
	Specifies the local name that is used to authenticate the tunnel.

Step 9



Configuring AAA Services for L2TP Support

Before the VPDN stack on the GGSN opens an L2TP tunnel to an LNS, it tries to authorize the tunnel first. The GGSN consults its local database to perform this authorization. Therefore, you need to configure the appropriate AAA services for the GGSN to support L2TP tunnel authorization. Note that this is for authorization of the tunnel itself—not for user authorization.

This section describes only those commands required to implement authorization for L2TP support on the GGSN. It does not describe all of the tasks required to configure RADIUS and AAA support on the GGSN. For more information about enabling AAA services and configuring AAA server groups on the GGSN, see the “[Configuring Security on the GGSN](#)” chapter in this book.



Note

To correctly implement authentication and authorization services on the GGSN for L2TP support, you must configure the same methods and server groups for both.

To configure authorization for L2TP support on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1		(Optional) Specifies that the GGSN consults its local database, as defined by the command, for tunnel authorization.

Command	Purpose
Step 2	<p>Specifies one or more AAA methods for use on interfaces running PPP, where:</p> <ul style="list-style-type: none"> —Runs authorization for all network-related service requests, including SLIP1, PPP2, PPP NCPs3, and ARA4. —Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. Specifies the character string used to name the list of authentication methods tried when a user logs in. Uses a subset of RADIUS servers for authentication as defined by the command. <p>Note Be sure to use a method list and do not use the form of the command. For L2TP support, the must match the group that you specify in the command.</p>
Step 3	<p>Specifies the password to be used in CHAP caller identification, where is the name of the tunnel.</p> <p>Note Usernames in the form of , , and are considered to be three different entries.</p> <p>Repeat this step to add a username entry for each remote system from which the local router or access server requires authentication.</p>

**Note**

You can configure the L2TP tunnel parameters locally on the GGSN, or the tunnel parameters can be provided by a RADIUS server. If a RADIUS server is providing the tunnel parameters, then in this procedure you only need to configure the command on the GGSN.

Configuring a PPP Virtual Template Interface

To support IP over GTP with PPP regeneration, you must configure a virtual template interface on the GGSN that supports PPP encapsulation. Therefore, the GGSN will have two virtual template interfaces: one for GTP encapsulation and one for PPP encapsulation. The GGSN uses the PPP virtual template interface to create all PPP virtual access interfaces for PPP sessions on the GGSN.

Because PPP is the default encapsulation, it does not need to be explicitly configured, and it does not appear in the output for the interface.

Be aware that the configuration commands for the PPP virtual template interface to support PPP regeneration on the GGSN are different from the previous configurations shown for GTP over PPP support.

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

Command	Purpose
Step 1	<p>Creates a virtual template interface, where identifies the virtual template interface. This command enters you into interface configuration mode.</p> <p>Note This number must match the configured in the corresponding command.</p>
Step 2	<p>Specifies that the IP address for a particular interface is obtained via PPP/IPCP (IP Control Protocol) address negotiation.</p>
Step 3	<p>Disables creation of neighbor routes.</p>
Step 4	<p>Disables an IP address from being returned to a remote peer connecting to this interface.</p>
Step 5	<p>(Optional) Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation.</p> <p>Note PPP is the default encapsulation and does not appear in the output of the command for the virtual template interface unless you manually configure the command.</p>
Step 6	<p>Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.</p>

Associating the Virtual Template Interface for PPP Regeneration on the GGSN

Before you associate the virtual template interface for PPP regeneration, you must configure a virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the `virtual-template` command.

To associate the virtual template interface for PPP regeneration, use the following command in global configuration mode:

Command	Purpose
	Associates the virtual template interface that defines the PPP characteristics with support for the PPP regeneration on the GGSN. Note This number must match the configured in the corresponding command.

Configuring PPP Regeneration at an Access Point

To enable PPP regeneration on the GGSN, you must configure each access point for which you want to support PPP regeneration. There is no global configuration command for enabling PPP regeneration for all access points on the GGSN.

To create an access point and specify its type, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1		Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	<pre>Router(config-ap-list)# access-point-index</pre>	
	<pre>Router(config-access-point)# apn-name</pre>	

Step 4	<p>Note</p>
Step 5	<ul style="list-style-type: none"> • max-session • setup-time • verify-domain <p>request is rejected with the cause code “Service not supported.”</p> <p>—Configures the GGSN to use the access point name as the domain name with which it initiates an L2TP tunnel to the user when PPP-regeneration is being used.</p> <p>The <code>max-session</code> and <code>verify-domain</code> command configurations are mutually exclusive. When the <code>verify-domain</code> command is configured, domain verification cannot be performed.</p>

Monitoring and Maintaining PPP on the GGSN

Router#	
Router#	
Router#	
Router#	
Router#	
Router#	
Router# []	
Router#] []	
Router#] []	

Configuration Examples

-
- [GTP-PPP-Over-L2TP Configuration Example, page 9-24](#)
- [GTP-PPP Regeneration Configuration Example, page 9-25](#)
- [AAA Services for L2TP Configuration Example, page 9-26](#)

GTP-PPP Termination on the GGSN Configuration Examples

```

Building configuration...
Current configuration : 3521 bytes
!
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!

```

```
service gprs ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
!
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius gtp_ppp
server 172.16.0.2 auth-port 2001 acct-port 2002
!
! Configures authentication and authorization
! methods for PPP support.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group gtp_ppp
!
ip subnet-zero
!
! Configures a loopback interface
! for the PPP virtual template interface
!
interface Loopback2
ip address 10.88.0.4 255.255.0.0
!
...
!
! Configures a VT interface for
! GTP encapsulation
!
interface loopback 1
ip address 10.30.30.1 255.255.255.0
!
interface Virtual-Template1
ip unnumber loopback 1
encapsulation gtp
gprs access-point-list gprs
!
! Configures a VT interface for
! PPP encapsulation
!
interface Virtual-Template2
ip unnumbered Loopback2
no peer default ip address
ppp authentication pap
!
...
!
gprs access-point-list gprs
access-point 1
access-point-name gprs.cisco.com
aaa-group authentication gtp_ppp
aaa-group accounting gtp_ppp
exit
!
! Associates the PPP virtual template
! interface for use by the GGSN
!
```

```
gprs gtp ppp-vtemplate 2
gprs default charging-gateway 10.7.0.2
!
gprs memory threshold 512
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
!
end
```

-Over-L2TP Configuration Example

```
. . .
!
! Enables AAA globally
!
aaa new-model
!
aaa authorization network default local
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
 request-dialin
 protocol l2tp
 domain ppp-lns
 initiate-to ip 4.0.0.78 priority 1
 local name nas
!
! Configures a loopback interface
! for the PPP virtual template interface
!
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
interface Virtual-Template2
 description VT for PPP L2TP
 ip unnumbered Loopback2
 no peer default ip address
 no peer neighbor-route
 ppp authentication pap chap
!
```

```

gprs access-point-list gprs
  access-point 15
  access-point-name ppp-lns
  exit
!
! Associates the PPP virtual template
! interface for use by the GGSN
!
gprs gtp ppp vtemplate 2
!
. . .
!

```

GTP-PPP Regeneration Configuration Example

```

!
. . .
!
! Enables AAA globally
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
  request-dialin
  protocol l2tp
  domain ppp_regen1
  initiate-to ip 4.0.0.78 priority 1
  l2tp tunnel password 7 0114161648
!
! Configures a virtual template
! interface for PPP regeneration
!
interface Virtual-Template2
  description VT for PPP Regen
  ip address negotiated
  no peer neighbor-route
  no peer default ip address
  ppp authentication pap chap
!
gprs access-point-list gprs
  access-point 6
  access-point-name ppp_regen1
  ppp-regeneration
  exit
!
! Associates the PPP-regeneration
! virtual template interface for use by the GGSN
!
gprs gtp ppp-regeneration vtemplate 2

```

AAA Services for L2TP Configuration Example

```
! NOTE: You must configure the same methods and groups
! to support L2TP as shown by the
! aaa authentication ppp gtp_ppp
! and aaa authorization network gtp_ppp commands.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network default local
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group radius
username nas password 0 lab
username hgw password 0 lab
!
. . .
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
. . .
!
```