CHAPTER 10

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 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:

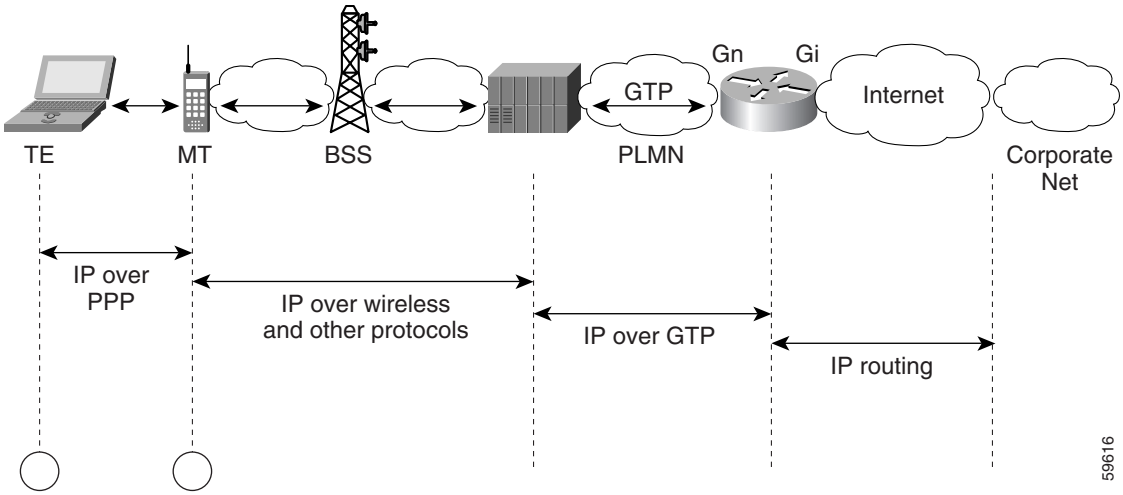
- Overview of PPP Support on the GGSN, page 10-1
- Configuring GTP-PPP Termination on the GGSN, page 10-3
- Configuring GTP-PPP with L2TP on the GGSN, page 10-7
- Configuring GTP-PPP Regeneration on the GGSN, page 10-14
- Monitoring and Maintaining PPP on the GGSN, page 10-21
- Configuration Examples, page 10-22

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 10-1 shows the implementation of IP over GTP without any PPP support within a GPRS network.

Figure 10-1 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 GTP-PPP and GTP-PPP Regeneration IPv6 PDP contexts are not supported.

Note Under optimal conditions, the GGSN supports 8000 PDP contexts when a PPP method is configured. However, the platform, amount of memory installed, method of PPP support configured, and rate of PDP context creation configured will all affect this number.

The following sections in this chapter describe each method in more detail and describe how to configure and verify each type of PPP support on the GGSN.

Configuring GTP-PPP Termination on the GGSN

This section provides an overview of and describes how to configure PPP over GTP on the GGSN. It includes the following topics:

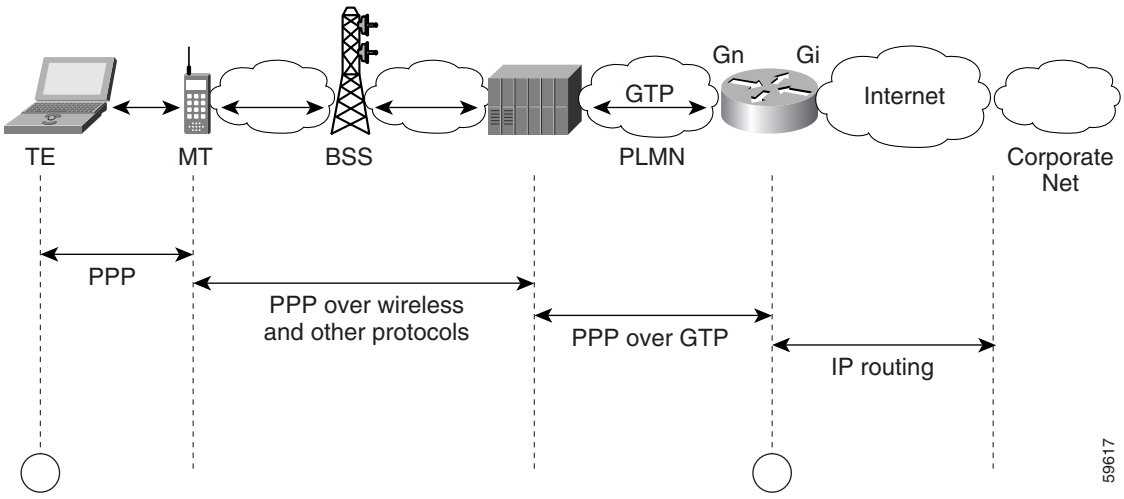
- Overview of GTP-PPP Termination on the GGSN, page 10-3
- Preparing to Configure PPP over GTP on the GGSN, page 10-4
- GTP-PPP Termination Configuration Task List, page 10-4
- GTP-PPP Termination on the GGSN Configuration Examples, page 10-22

Overview of GTP-PPP Termination on the GGSN

The GGSN supports the PPP PDP type over GTP without using L2TP. In this topology, the GGSN provides PPP support from the terminal equipment (TE) and mobile termination (MT) or mobile station (MS) through the SGSN, over the Gn interface and the GTP tunnel to the GGSN. The PPP endpoints are at the terminal equipment (TE) and the GGSN. IP routing occurs from the GGSN over the Gi interface to the corporate network.

Figure 10-2 shows the implementation of PPP over GTP without L2TP support within a GPRS network.

Figure 10-2 PPP Over GTP Topology With PPP Termination at the GGSN



Benefits

PPP over GTP support on the GGSN provides the following benefits:

- Different traffic types can be supported over GTP.
- Authentic negotiation of PPP options can occur for PPP endpoints (no need for proxy PPP negotiation).
- Provides the foundation for GTP to interwork with other PPP networking protocols, such as L2TP.

- Requirements for MT intelligence are simplified, with no need for support of a PPP stack on the MT.
- Additional session security is provided.
- Provides increased flexibility of IP address assignment to the TE.

Preparing to Configure PPP over GTP on the GGSN

Before you begin to configure PPP over GTP support on the GGSN, you need to determine the method that the GGSN will use to allocate IP addresses to users. There are certain configuration dependencies that are based on the method of IP address allocation that you want to support.

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

- 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 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** command at the PPP virtual template interface.
  - Specify the **aaa authorization network** *method_list* **none** command on the GGSN.
  - For more information about configuring DHCP services on the GGSN, see the "Configuring Dynamic Addressing on the GGSN" chapter in this guide.
- 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.

GTP-PPP Termination Configuration Task List

To configure PPP over GTP support on the GGSN, perform the following tasks:

- Configuring a Loopback Interface, page 10-5 (Recommended)
- Configuring a PPP Virtual Template Interface, page 10-5 (Required)
- Associating the Virtual Template Interface for PPP on the GGSN, page 10-7 (Required)

Configuring a Loopback Interface

We recommend that you configure the virtual template interface as unnumbered, and associate its IP numbering with a loopback interface.

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 that you can create. The GGSN uses loopback interfaces to support the configuration of several different features.

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.

Configuring a PPP Virtual Template Interface

To support PPP over GTP, 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.

We recommend that you configure the virtual template interface as unnumbered, and associate its IP numbering with a loopback interface.

Because it is the default, PPP encapsulation does not appear in the **show running-config** output for the interface.

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

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp vtemplate** command.
Step 2	`Router(config-if)# ip unnumbered` *type number*	Enables IP processing on the virtual template interface without assigning an explicit IP address to the interface, where *type* and *number* specify another interface for which the router is assigned an IP address. For the GGSN, this can be a Gi interface or a loopback interface. We recommend using a loopback interface.
Step 3	`Router(config-if)# no peer default ip address` (for RADIUS server) or `Router(config-if)# peer default ip address dhcp` (for DHCP server) or `Router(config-if)# peer default ip address pool` *pool-name* (for local pool)	Specifies the prior peer IP address pooling configuration for the interface. If you are using a RADIUS server for IP address allocation, then you need to disable peer IP address pooling.
Step 4	`Router(config-if)# encapsulation ppp`	(Optional) Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 5	`Router(config-if)# ppp authentication {pap [chap]} [default]`	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface, where • **pap** [**chap**]—Enables PAP, CHAP, or both on the interface. • **default**—Name of the method list created with the **aaa authentication ppp** command.

Associating the Virtual Template Interface for PPP on the GGSN

Before you associate the virtual template interface for PPP, you must configure the virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

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

Command	Purpose
`Router(config)# gprs gtp ppp vtemplate` *number*	Associates the virtual template interface that defines the PPP characteristics with support for the PPP PDP type over GTP on the GGSN. **Note** This number must match the *number* configured in the corresponding **interface virtual-template** command.

Configuring GTP-PPP with L2TP on the GGSN

This section provides an overview of and describes how to configure PPP over GTP with L2TP support on the GGSN. It includes the following topics:

- Overview of GTP-PPP with L2TP on the GGSN, page 10-7
- GTP-PPP With L2TP Configuration Task List, page 10-8

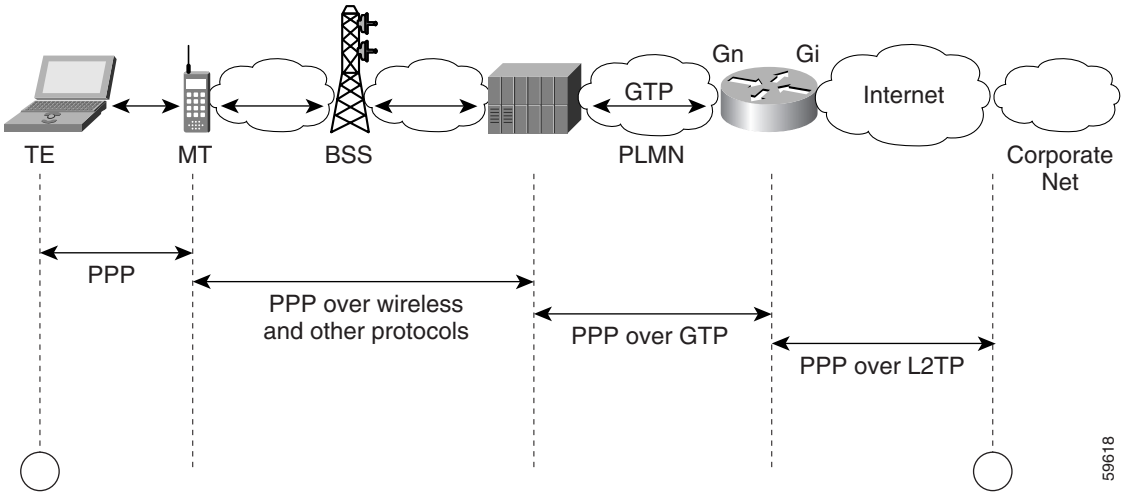
Overview of GTP-PPP with L2TP on the GGSN

The GGSN supports PPP over GTP using L2TP, without IP routing. The GGSN provides PPP support from the TE and MT through the SGSN, over the Gn interface and the GTP tunnel to the GGSN, and over the Gi interface and an L2TP tunnel to the corporate network. In this scenario, the PPP termination endpoints are at the TE and the L2TP network server (LNS) at the corporate network.

With L2TP support, packets are delivered to the LNS by routing L2TP- and PPP-encapsulated IP payload. Without L2TP, pure IP payload is routed to the LNS at the corporate network.

Figure 10-3 shows the implementation of PPP over GTP with L2TP support within a GPRS network.

Figure 10-3 PPP Over GTP With L2TP Topology on the GGSN



Benefits

PPP over GTP with L2TP support on the GGSN provides the following benefits:

- VPN security using L2TP tunnels provides secure delivery of user data over the public network to a corporate network.
- Real end-to-end PPP sessions, with authentication and address negotiation and assignment.
- Corporate networks can retain control over access to their servers and do not need to provide access by the GGSN to those servers.
- Configuration changes on corporate servers can occur without requiring an update to the GGSN.

Restrictions

The GGSN supports PPP over GTP with L2TP with the following restriction:

- At least one PPP authentication protocol must be enabled using the **ppp authentication** command in interface configuration mode.

GTP-PPP With L2TP Configuration Task List

Configuring GTP over PPP with L2TP requires many of the same configuration tasks as those required to configure GTP over PPP without L2TP, with some additional tasks to configure the GGSN as an L2TP access concentrator (LAC) and to configure authentication, authorization, and accounting (AAA) services.

To configure PPP over GTP with L2TP support on the GGSN, perform the following tasks:

- Configuring the GGSN as a LAC, page 10-9 (Required)
- Configuring AAA Services for L2TP Support, page 10-10 (Required)
- Configuring a Loopback Interface, page 10-11 (Recommended)

- Configuring a PPP Virtual Template Interface, page 10-12 (Required)
- Associating the Virtual Template Interface for PPP on the GGSN, page 10-13 (Required)

Configuring the GGSN as a LAC

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, see *Cisco IOS Dial Technologies Configuration Guide* and *Command Reference* publications.

To configure the GGSN as a LAC where the tunnel parameters are configured locally on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN on the router or instance of Cisco IOS software and directs the router to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present. **Note** Only this step is required if you are using a RADIUS server to provide tunnel parameters.
Step 2	`Router(config)# vpdn-group group-number`	Defines a VPDN group, and enters VPDN group configuration mode.
Step 3	`Router(config-vpdn)# request-dialin`	Enables the router or instance of Cisco IOS software to request dial-in tunnels, and enters request dial-in VPDN subgroup configuration mode.
Step 4	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the L2TP protocol for dial-in tunnels.
Step 5	`Router(config-vpdn-req-in)# domain domain-name`	Specifies that users with this domain name will be tunneled. Configure this command for every domain name you want to tunnel.
Step 6	`Router(config-vpdn-req-in)# exit`	Returns you to VPDN group configuration mode.
Step 7	`Router(config-vpdn)# initiate-to ip ip-address [limit limit-number] [priority priority-number]`	Specifies the destination IP address for the tunnel.
Step 8	`Router(config-vpdn)# local name name`	Specifies the local name that is used to authenticate the tunnel.

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 **vpdn enable** command on the GGSN.

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	`Router(config)# aaa authorization network default local`	(Optional) Specifies that the GGSN consults its local database, as defined by the **username** command, for tunnel authorization.

	Command	Purpose
Step 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	Specifies one or more AAA methods for use on interfaces running PPP, where: • **network**—Runs authorization for all network-related service requests, including SLIP1, PPP2, PPP NCPs3, and ARA4. • **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. • *list-name*—Specifies the character string used to name the list of authentication methods tried when a user logs in. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. **Note** Be sure to use a method list and do not use the **aaa authorization network default group radius** form of the command. For L2TP support, the *group-name* must match the group that you specify in the **aaa authentication ppp** command.
Step 3	`Router(config)# username name password secret`	Specifies the password to use in CHAP caller identification, where *name* is the name of the tunnel. **Note** Usernames in the form of *ciscouser*, *ciscouser@corporate1.com*, and *ciscouser@corporate2.com* are considered to be three different entries. Repeat this step to add a username entry for each remote system from which the local router or access server requires authentication.

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 **username** command on the GGSN.

Configuring a Loopback Interface

We recommend that you configure the virtual template interface as unnumbered and that you associate its IP numbering with a loopback interface.

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. The GGSN uses loopback interfaces to support the configuration of several different features.

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 IP addresses on the loopback interface are needed only for PPP PDPs that are not using L2TP. We recommend using IP addresses when PPP PDPs are destined to a domain that is not configured with L2TP.

Configuring a PPP Virtual Template Interface

To support PPP over GTP, 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.

Note If you are planning to support both GTP-PPP and GTP-PPP-L2TP (PPP PDPs with and without L2TP support), then you must use the same virtual template interface for PPP.

We recommend that you configure the virtual template interface as unnumbered and that you associate its IP numbering with a loopback interface.

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

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

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp vtemplate** command.
Step 2	`Router(config-if)# ip unnumbered` *type number*	Enables IP processing on the virtual template interface without assigning an explicit IP address to the interface, where *type* and *number* specify another interface for which the router is assigned an IP address. For the GGSN, this can be a Gi interface or a loopback interface. Cisco recommends using a loopback interface.
Step 3	`Router(config-if)# encapsulation ppp`	Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 4	`Router(config-if)# ppp authentication {`*protocol1* `[`*protocol2...*`]} [`**if-needed**`] [`*list-name* | **default**`] [`**callin**`] [`**one-time**`] [`**optional**`]`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

Associating the Virtual Template Interface for PPP on the GGSN

Before you associate the virtual template interface for PPP, you must configure the virtual template interface. The number that you configure for the virtual template interface must correspond to the number that you specify in the **gprs gtp ppp vtemplate** command.

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

Command	Purpose
`Router(config)# gprs gtp ppp vtemplate` *number*	Associates the virtual template interface that defines the PPP characteristics with support for the PPP PDP type over GTP on the GGSN. **Note** This number must match the *number* configured in the corresponding **interface virtual-template** command.

Configuring GTP-PPP Regeneration on the GGSN

This section provides an overview of and describes how to configure PPP over GTP with L2TP support on the GGSN. It includes the following topics:

- Overview of GTP-PPP Regeneration on the GGSN, page 10-14
- GTP-PPP Regeneration Configuration Task List, page 10-15

Overview of GTP-PPP Regeneration on the GGSN

The GGSN supports PPP in two different areas of the network, with two different sets of PPP endpoints, and supports IP over GTP in between. First, IP over PPP is in use between the TE and MT. From there, IP packet support occurs between the MT through the SGSN, over the Gn interface and the GTP tunnel to the GGSN. The GGSN initiates a new PPP session on the Gi interface over an L2TP tunnel to the corporate network. So, the second set of PPP endpoints occurs between the GGSN and the LNS at the corporate network.

PPP regeneration on the GGSN supports the use of an IP PDP type in combination with PPP and L2TP. For each IP PDP context that the GGSN receives at an access point that is configured to support PPP regeneration, the GGSN regenerates a PPP session. The GGSN encapsulates any tunnel packet data units (TPDUs) in PPP and L2TP headers as data traffic and forwards them to the LNS.

PPP regeneration on the GGSN implements VPN routing and forwarding (VRF) to handle overlapping IP addresses. A VRF routing table is automatically enabled at each access point name (APN) when you configure PPP regeneration at that APN.

PPP-Regeneration Scalability

With Cisco GGSN Release 8.0 and later, the GGSN allows PDPs regenerated to a PPP session to run on software interface description blocks (IDBs), which increases the number of supported sessions.

Anonymous User Access

Additionally, with Cisco GGSN Release8.0, anonymous user access support for PPP-regenerated PDPs enables PDPs to be created for users who cannot send a username and password. For example, WAP users cannot send a name and password.

When the **anonymous user** command in access-point user configuration mode is configured under an APN that is configured for PPP regeneration, when a Create PDP Context request is received for a PPP-regenerated PDP that contains no username and password in the PCO IE, the anonymous user configuration under that APN is sent to the LNS for authentication. If the PCO IE contains a username and password, the tunnel to the LNS is created using the supplied username and password, even though anonymous user is configured under the APN.

The username and password in the Create PDP Context request takes higher precedence than the anonymous user configuration.

For information about configuring anonymous user access under an APN, see the "Configuring Additional Real Access Point Options" section on page 9-20.

Restrictions

The GGSN supports PPP regeneration with the following restriction:

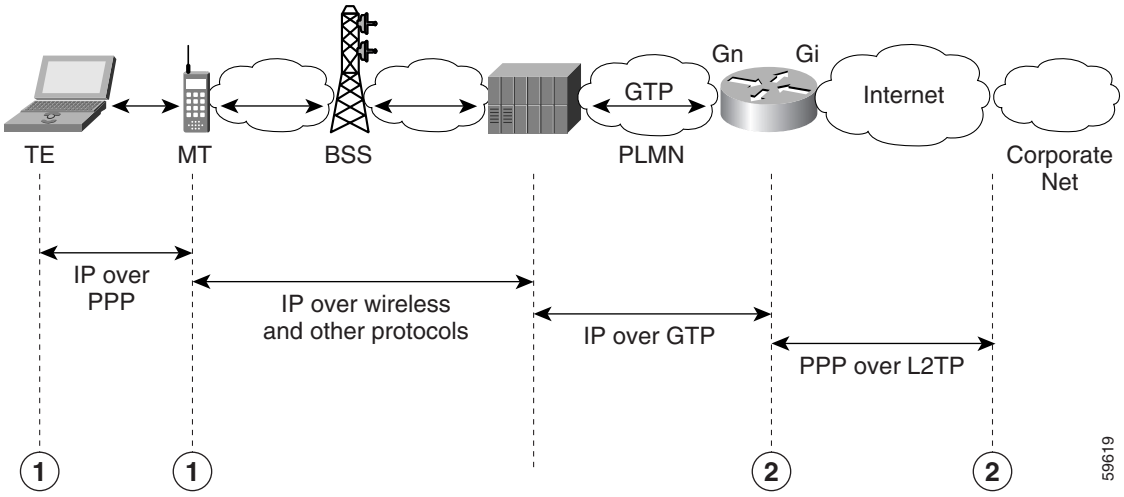
- Manual configuration of VRF is not supported.

- At least one PPP authentication protocol must be enabled using the **ppp authentication** command in interface configuration mode.
- Ensure that the **no peer default ip address** command is configured under the PPP-Regen virtual template.

Caution The creation of PPP-Regen contexts on the GGSN can lead to higher than usual CPU utilization on the GGSN when console logging is enabled (**logging console** command) and the link status log is not turned off under the PPP-Regen virtual template.

Figure 10-4 shows the implementation of PPP support within a GPRS network using PPP regeneration on the GGSN.

Figure 10-4 PPP Regeneration Topology on the GGSN



GTP-PPP Regeneration Configuration Task List

Configuring IP over GTP with PPP regeneration on the GGSN requires similar configuration tasks as those required to configure GTP over PPP with L2TP, with some exceptions in the implementation.

To configure GTP-PPP regeneration support on the GGSN, perform the following tasks:

- Configuring the GGSN as a LAC, page 10-16 (Required)
- Configuring AAA Services for L2TP Support, page 10-17 (Required)
- Configuring a PPP Virtual Template Interface, page 10-18 (Required)
- Associating the Virtual Template Interface for PPP Regeneration on the GGSN, page 10-20 (Required)
- Configuring PPP Regeneration at an Access Point, page 10-20 (Required)

Configuring the GGSN as a LAC

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, see *Cisco IOS Dial Technologies Configuration Guide* and *Command Reference* publications.

To configure the GGSN as a LAC where the tunnel parameters are configured locally on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN on the router or instance of Cisco IOS software and directs the router or instance to look for tunnel definitions in a local database and on a remote authorization server (home gateway), if one is present. **Note** Only this step is required if you are using a RADIUS server to provide tunnel parameters.
Step 2	`Router(config)# vpdn domain-delimiter` *characters* `[suffix | prefix]`	(Optional) Specifies the characters to use to delimit the domain prefix or domain suffix. Available characters are %, -, @, \ , #, and /. The default is @. **Note** If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
Step 3	`Router(config)# vpdn-group` *group-number*	Defines a VPDN group, and enters VPDN group configuration mode.
Step 4	`Router(config-vpdn)# request-dialin`	Enables the router or instance of Cisco IOS software to request dial-in tunnels, and enters request dial-in VPDN subgroup configuration mode.
Step 5	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies use of the L2TP protocol for dial-in tunnels.
Step 6	`Router(config-vpdn-req-in)# domain` *domain-name*	Specifies that users with this domain name will be tunneled. Configure this command for every domain name you want to tunnel.
Step 7	`Router(config-vpdn-req-in)# exit`	Returns you to VPDN group configuration mode.
Step 8	`Router(config-vpdn)# initiate-to ip` *ip-address* `[limit` *limit-number*`] [priority` *priority-number*`]`	Specifies the destination IP address for the tunnel.
Step 9	`Router(config-vpdn)# local name` *name*	Specifies the local name that is used to authenticate the tunnel.

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 **vpdn enable** command on the GGSN.

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	`Router(config)# aaa authorization network default local`	(Optional) Specifies that the GGSN consults its local database, as defined by the **username** command, for tunnel authorization.

	Command	Purpose
Step 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	Specifies one or more AAA methods for use on interfaces running PPP, where: • **network**—Runs authorization for all network-related service requests, including SLIP1, PPP2, PPP NCPs3, and ARA4. • **default**—Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in. • *list-name*—Specifies the character string used to name the list of authentication methods tried when a user logs in. • **group** *group-name*—Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command. **Note** Be sure to use a method list and do not use the **aaa authorization network default group radius** form of the command. For L2TP support, the *group-name* must match the group that you specify in the **aaa authentication ppp** command.
Step 3	`Router(config)# username name password secret`	Specifies the password to use in CHAP caller identification, where *name* is the name of the tunnel. **Note** Usernames in the form of *ciscouser*, *ciscouser@corporate1.com*, and *ciscouser@corporate2.com* are considered to be three different entries. Repeat this step to add a username entry for each remote system from which the local router or access server requires authentication.

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 **username** 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 **show running-config** 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	`Router(config)# interface virtual-template number`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command enters you into interface configuration mode. **Note** This number must match the *number* configured in the corresponding **gprs gtp ppp-regeneration vtemplate** command.
Step 2	`Router(config-if)# ip address negotiated`	Specifies that the IP address for a particular interface is obtained via PPP/IPCP (IP Control Protocol) address negotiation.
Step 3	`Router(config-if)# no peer neighbor-route`	Disables creation of neighbor routes.
Step 4	`Router(config-if)#no peer default ip address`	Disables an IP address from being returned to a remote peer connecting to this interface.
Step 5	`Router(config-if)# encapsulation ppp`	(Optional) Specifies PPP as the encapsulation type for packets transmitted over the virtual template interface. PPP is the default encapsulation. **Note** PPP is the default encapsulation and does not appear in the output of the **show running-config** command for the virtual template interface unless you manually configure the command.
Step 6	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] [optional]`	Enables at least one PPP authentication protocol and specifies the order in which the protocols are selected on the interface.

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 **gprs gtp ppp-regeneration vtemplate** command.

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

Command	Purpose
`Router(config)# gprs gtp ppp-regeneration vtemplate` *number*	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 *number* configured in the corresponding **interface virtual-template** 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	`Router(config)# gprs access-point-list` *list-name*	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	`Router(config-ap-list)# access-point` *access-point-index*	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	`Router(config-access-point)# access-point-name` *apn-name*	Specifies the access point network ID, which is commonly an Internet domain name. **Note** The *apn-name* must match the APN that is provisioned at the MS, home location register (HLR), and Domain Name System (DNS) server.

	Command	Purpose
Step 4	`Router(config-access-point)# access-mode transparent`	(Optional) Specifies that no security authorization or authentication is requested by the GGSN for this access point. **Note** Transparent access is the default value, but it must be *manually* configured to support PPP regeneration at the access point if the access mode was previously non-transparent.
Step 5	`Router(config-access-point)# ppp-regeneration [max-session number | setup-time seconds | verify-domain | fixed-domain]`	Enables an access point to support PPP regeneration, where: • **max-session** *number*—Specifies the maximum number of PPP regenerated sessions allowed at the access point. The default value is 65535. • **setup-time** *seconds*—Specifies the maximum amount of time (between 1 and 65535 seconds) within which a PPP regenerated session must be established. The default value is 60 seconds. • **verify-domain**—Configures the GGSN to verify the domain sent in the protocol configuration option (PCO) IE sent in a Create PDP Context request against the APN sent out by the user when PPP-regeneration is being used. If a mismatch occurs, the Create PDP Context request is rejected with the cause code "Service not supported." • **fixed-domain**—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. The **ppp-regeneration fixed-domain** and **ppp-regeneration verify-domain** command configurations are mutually exclusive. When the **ppp-regeneration fixed-domain** command is configured, domain verification cannot be performed.

Monitoring and Maintaining PPP on the GGSN

This section provides a summary list of the **show** commands that you can use to monitor the different aspects of PPP configuration on the GGSN. Not all of the **show** commands apply to every method of configuration.

Use the following privileged EXEC commands to monitor and maintain PPP status on the GGSN:

Command	Purpose
Router# **show derived-config interface virtual-access** *number*	Displays the PPP options that GTP has configured on the virtual access interface for PPP regenerated sessions.
Router# **show gprs gtp pdp-context all**	Displays all currently active PDP contexts.
Router# **show gprs gtp pdp-context path** *ip-address*	Displays all currently active PDP contexts for the specified SGSN path.
Router# **show gprs gtp pdp-context pdp-type ppp**	Displays all currently active PDP contexts that are transmitted using PPP.
Router# **show gprs gtp status**	Displays information about the current status of the GTP on the GGSN.
Router# **show interfaces virtual-access** *number* [**configuration**]	Displays status, traffic data, and configuration information about a specified virtual access interface.
Router# **show vpdn session** [**all** | **packets** | **sequence** | **state** | **timers** | **window**] [**interface** | **tunnel** | **username**]	Displays VPN session information including interface, tunnel, username, packets, status, and window statistics.
Router# **show vpdn tunnel** [**all** | **packets** | **state** | **summary** | **transport**] [**id** | **local-name** | **remote-name**]	Displays VPN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status.

Configuration Examples

This section provides configuration examples for the different types of PPP support on the GGSN. It includes the following examples:

- GTP-PPP Termination on the GGSN Configuration Examples, page 10-22
- GTP-PPP–Over–L2TP Configuration Example, page 10-24
- GTP-PPP Regeneration Configuration Example, page 10-25
- AAA Services for L2TP Configuration Example, page 10-26

GTP-PPP Termination on the GGSN Configuration Examples

The following example shows a GGSN configuration for GTP over PPP using PAP authentication using a RADIUS server at 172.16.0.2 to allocate IP addresses:

```
Router# show running-config
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
```

GTP-PPP–Over–L2TP Configuration Example

The following example shows a partial configuration of the GGSN to support PPP over GTP with L2TP. Tunnel parameters are configured locally on the GGSN and are not provided by a RADIUS server.

```
. . .
!
! 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

The following example shows a partial configuration of the GGSN to support IP over GTP with PPP regeneration on the GGSN. Tunnel parameters are configured locally on the GGSN and are not provided by a RADIUS server.

```
!
. . .
!
! 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

L2TP support is used on the GGSN to support both the PPP-over-GTP topology and the IP–over–GTP with PPP regeneration topology. The following examples shows a partial configuration of RADIUS and AAA services on the GGSN to provide L2TP support:

```
!
! 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
! method gtp_ppp and AAA server group gtp_ppp
! for PPP support.
!
! 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
!
. . .
!
```