Cisco ASR 5000 Series Packet Data Gateway/Tunnel Termination Gateway Administration Guide

Version 10.0

Last Updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22999-01

Cisco ASR 5000 Series Packet Data Gateway/Tunnel Termination Gateway Administration Guide

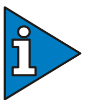
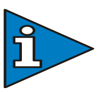
CONTENTS

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

IMPORTANT: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
PDG/TTG Overview

This chapter contains general overview information about the PDG/TTG (Packet Data Gateway/Tunnel Termination Gateway), including:

Product Description

The Cisco® ASR 5000 Chassis provides 3GPP wireless carriers with a flexible solution that functions as a PDG/TTG (Packet Data Gateway/Tunnel Termination Gateway) in 3GPP UMTS wireless voice and data networks. The PDG/TTG consists of new software for the ASR 5000.

The PDG/TTG enables mobile operators to provide Fixed Mobile Convergence (FMC) services to subscribers with dual-mode handsets and dual-mode access cards via WiFi access points. The PDG/TTG makes it possible for operators to provide secure access to the operator's 3GPP network from a non-secure network, reduce the load on the macro wireless network, enhance in-building wireless coverage, and make use of existing backhaul infrastructure to reduce the cost of carrying wireless calls.

This PDG/TTG software release provides TTG functionality. The TTG is a network element that enables 3GPP PDG functionality for existing GGSN deployments. The TTG and the subset of existing GGSN functions work together to provide PDG functionality to the subscriber UEs in the WLAN.

IMPORTANT: This PDG/TTG software release provides TTG functionality only. PDG functionality is not supported in this release.

Summary of TTG Features and Functions

The TTG features and functions include:

- PDG service
- TTG mode
- IKEv2 and IP Security (IPSec) encryption
- Multiple digital certificate selection based on APN
- Subscriber traffic policing for IPSec access
- DSCP marking for IPSec access
- WLAN access control
- RADIUS and Diameter support
- EAP fast re-authentication
- Pseudonym NAI support
- Multiple APN support for IPSec access
- Lawful intercept
- IMS emergency call handling
- IPSec Session recovery support

- Congestion control
- Bulk statistics
- Threshold crossing alerts (TCAs)

Product Specifications

The following information is located in this section:

- Licenses
- Hardware Requirements
- Operating System Requirements

Licenses

The PDG/TTG is a licensed product. For information about PDG/TTG licenses, contact your sales representative.

Hardware Requirements

Information in this section describes the hardware required to run the PDG/TTG software.

Platforms

The PDG/TTG operates on the ASR 5000.

Components

The following application and line cards are required to support the PDG/TTG on an ASR 5000:

- **System Management Cards (SMCs)**: Provides full system control and management of all cards within the ASR 5000. Up to two SMC can be installed; one active, one redundant.
- **Packet Services Cards (PSCs/PSC2s)**: Within the ASR 5000, PSCs/PSC2s provide high-speed, multi-threaded PDP context processing capabilities for 2.5G SGSN, 3G SGSN, and GGSN services. Up to 14 PSCs/PSC2s can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs)**: Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, central office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Ethernet 10/100 and/or Ethernet 1000 Line Cards:** Installed directly behind PSCs, these cards provide the physical interfaces to elements in the operator's network. Up to 26 line cards should be installed for a fully loaded system with 13 active PSCs/PSC2s, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s do not require line cards.
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards

and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs/PSC2s.

IMPORTANT: Additional information pertaining to each of the application and line cards required to support GPRS/UMTS wireless data services is located in the *Hardware Platform Overview* chapter of the *Product Overview Guide.*

Operating System Requirements

The PDG/TTG is available for the ASR 5000 running StarOS Release 9.0 or later.

Network Deployment(s) and Interfaces

This section describes the PDG/TTG as it functions as a TTG in a GPRS/UMTS data network.

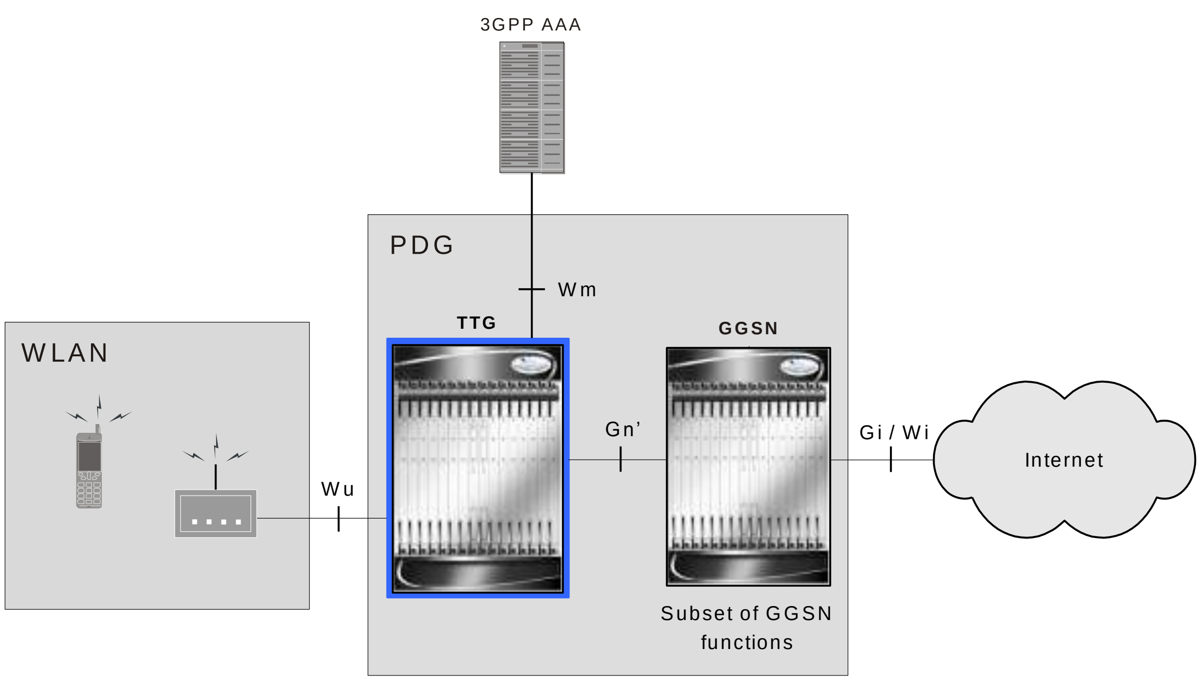
The TTG in a GPRS/UMTS Data Network

The TTG is a GPRS/UMTS network element that enables the implementation of PDG functionality in existing GGSN deployments. It achieves this by using a subset of the Gn reference point called the Gn' (Gn prime) reference point.

The Gn' reference point provides the means by which GPRS mobile operators can implement PDG functionality by re-using existing infrastructure, including currently deployed GGSNs, to offer new services to current subscribers.

The following figure shows a PDG implementation that uses existing GGSN functionality. This implementation includes the PDG/TTG functioning as a TTG and a currently-deployed GGSN. In this implementation, only a subset of the GGSN functionality is used.

Figure 1. The TTG in a PDG Implementation



In the implementation above, the TTG terminates an IPSec tunnel for each WLAN UE subscriber session established over the Wu reference point. The TTG also establishes a corresponding GTP (GPRS Tunneling Protocol) tunnel over the Gn' reference point to the GGSN. The TTG and the subset of GGSN functions work together to provide PDG functionality to the UEs in the WLAN.

GTP (GPRS Tunneling Protocol) is the primary protocol used in the GPRS core network. It allows subscribers in a UMTS network to move from place to place while continuing to connect to the Internet as if from one location at the GGSN. It does this by carrying the subscriber's data from the subscriber's current SGSN to the GGSN that is handling the subscriber's session.

The TTG functions as an SGSN in the GPRS/UMTS network to provide an SGTP (SGSN GPRS Tunneling Protocol) service. The SGTP service enables the TTG to use GTP over the Gn' interface to carry packet data between itself and the GGSN.

TTG Logical Network Interfaces (Reference Points)

The following table provides descriptions of the logical network interfaces supported by the TTG in a GPRS/UMTS data network.

Table 1. TTG Logical Network Interfaces

Interface	Description
Wu	The reference point between the WLAN UE and the TTG. The Wu interface carries the IPSec tunnels between the UEs in the WLAN and the TTG. The IPSec tunnels carry the ESP (Encapsulating Security Payload) packets between the UEs and the TTG.
Wm	The reference point between the TTG and the 3GPP AAA server.
Gn'	The reference point between the TTG and the GGSN. To provide PDG functionality in existing GGSN deployments, the TTG functions as an SGSN. For every IPSec tunnel that is established between the TTG and a WLAN UE, the TTG initiates a PDP context and a corresponding GTP tunnel over the Gn' interface to the GGSN. The TTG forwards the W-APN and IMSI of the WLAN UE to the GGSN in the Create-PDP-Context-Request message. The following messages are supported over the Gn' reference point: • Create PDP Context Request / Response • Update PDP Context Request / Response • Delete PDP Context Request / Response • Error Indication • Version Not Supported • GTP Payload Forwarding • GTP Echo

Features and Functionality

This section describes the features and functions supported by the PDG/TTG software.

The following features are supported and described in this section:

- PDG Service
- TTG Mode
- IP Security (IPSec) Encryption
- Multiple Digital Certificate Selection Based on APN
- Subscriber Traffic Policing for IPSec Access
- DSCP Marking for IPSec Access
- WLAN Access Control
- RADIUS and Diameter Support
- EAP Fast Re-authentication Support
- Pseudonym NAI Support
- Multiple APN Support for IPSec Access
- Lawful Intercept
- IMS Emergency Call Handling
- IPSec Session Recovery Support
- Congestion Control
- Bulk Statistics
- Threshold Crossing Alerts

PDG Service

In this software release, the PDG service provides TTG functionality to enable the implementation of PDG functionality in existing GGSN deployments.

During configuration, you create the PDG service in a PDG context, which is a routing domain on the ASR 5000. PDG context and service configuration includes the following main steps:

- **Configure the IPv4 address for the service:** This is the IP address of the TTG to which the UEs in the WLAN attempt to connect. The UEs send IKEv2 messages to this IP address, and the TTG uses the IP address to listen for these messages.

- **Configure the name of the crypto template for IKEv2/IPSec:** A crypto template is used to define an IKEv2/IPSec policy. It includes IKEv2 and IPSec parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service.

The crypto template includes the following:

- **The name of the EAP profile:** The EAP profile defines the EAP methods and associated parameters.
- **Multiple authentication support:** Multiple authentication is specified as a part of crypto template configuration.
- **IKEv2 and IPSec transform sets:** Transform set defines the negotiable algorithms for IKE SAs and Child SAs.
- **The setup timeout value:** This parameter specifies the session setup timeout timer value. The TTG terminates a UE connection attempt if the UE does not establish a successful connection within the specified timeout period.
- **Max-sessions:** This parameter sets the maximum number of subscriber sessions allowed by this PDG service.
- **SGTP context and service:** You create an SGTP context and service to enable GPRS Tunneling Protocol (GTP) on the TTG to use for sending packet data between the TTG and the GGSN.

TTG Mode

TTG mode uses IKEv2/IPsec tunnels to deliver packet data services over untrusted WiFi access networks with connectivity to the Internet or managed networks.

In TTG mode, the system terminates an IPSec tunnel for each WLAN UE subscriber session established over the Wu reference point. The TTG also establishes a corresponding GTP (GPRS Tunneling Protocol) tunnel over the Gn' reference point to the GGSN. The TTG and a subset of GGSN functions work together to provide PDG functionality to the WLAN UEs.

IP Security (IPSec) Encryption

The PDG/TTG supports IKEv2 and IPSec encryption using IPv4 addressing. IKEv2 and IPSec encryption enables network domain security for all IP packet-switched networks in order to provide confidentiality, integrity, authentication, and anti-replay protection. These capabilities are insured through use of cryptographic techniques.

IKEv2 and IP Security (IPSec) encryption, including support for:

- **IKEv2 encryption protocols:** AES-CBC with 128 bits, AES-CBC with 256 bits, 3DES-CBC, and DES-CBC
- **IKEv2 pseudo-random functions:** PRF-HMAC-SHA1, PRF-HMAC-MD5
- **IKEv2 integrity:** HMAC-SHA1-96, HMAC-MD5
- **IKEv2 Diffie-Hellman groups:** 1, 2, 5, and 14
- **IPSec ESP (Encapsulating Security Payload) encryption:** AES-CBC with 128 bits, AES-CBC with 256 bits, 3DES-CBC, and DES-CBC
- **IPSec integrity:** HMAC-SHA1-96, HMAC-MD5
- **IKEv2 and IPSec rekeying**

Multiple Digital Certificate Selection Based on APN

Selecting digital certificates based on APN allows you to apply digital certificates per the requirements of each APN and associated packet data network. A digital certificate is an electronic credit card that establishes a subscriber's credentials when doing business or other transactions on the Internet. Some digital certificates conform to ITU-T standard X.509 for a Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, among other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

During session establishment, the PDG/TTG can select a digital certificate from multiple certificates based on the APN (Access Point Name). The selected certificate is associated with the APN that the WLAN UE includes in the IDr payload of the first IKE_AUTH_REQ message.

When configuring APN-based certificate selection, ensure that the certificate names match the associated APNs exactly. The PDG/TTG can then examine each APN received in the IDr payload and select the correct certificate.

The PDG/TTG generates an SNMP notification when the certificate is within 30 days of expiration and approximately once a day until a new certificate is provided. Operators need to generate a new certificate and then configure the new certificate using the system's CLI. The certificate is then used for all new sessions.

Subscriber Traffic Policing for IPSec Access

Traffic policing allows you to manage bandwidth usage on the network and limit bandwidth allowances to subscribers.

Traffic policing enables the configuring and enforcing of bandwidth limitations on individual subscribers of a particular traffic class in 3GPP service. Bandwidth enforcement is configured and enforced independently in the downlink and uplink directions.

When configured in the Subscriber Configuration Mode of the system's CLI, the PDG/TTG performs traffic policing. However, if the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the QoS values from the GGSN.

A Token Bucket Algorithm (a modified trTCM) [RFC2698] is used to implement the traffic policing feature. The following criteria is used when determining how to mark a packet:

- **Committed Data Rate (CDR):** The guaranteed rate (in bits per second) at which packets can be transmitted/received for the subscriber during the sampling interval. Note that the committed (or guaranteed) data rate does not apply to the Interactive and Background traffic classes.
- **Peak Data Rate (PDR):** The maximum rate (in bits per second) that subscriber packets can be transmitted/received for the subscriber during the sampling interval.

Using negotiated QoS data rates, the system calculates the burst size, which is the maximum number of bytes that can be transmitted/received for the subscriber during the sampling interval for both committed and peak rate conditions. The committed burst size (CBS) and peak burst size (PBS) for each subscriber depends on the guaranteed bit rate (GBR) and maximum bit rate (MBR) respectively. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". The burst size is the bucket size used by the Token Bucket Algorithm.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size.

After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- If there are not enough tokens in the PBS bucket to allow a packet to pass, the packet is considered to be in violation and is marked "red" and the violation counter is incremented by one.
- If there are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS "bucket", then the packet is considered to be in excess and is marked "yellow", the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- If there are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked "green" and the CBS and PBS buckets are decremented by the packet size.

The system can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop:** The offending packet is discarded.
- **Transmit:** The offending packet is passed.
- **Lower the IP Precedence:** The packet's ToS octet is set to "0", thus downgrading it to Best Effort, prior to passing the packet.

Different actions can be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.

DSCP Marking for IPSec Access

The DSCP (Differentiated Service Code Point) marking feature provides support for more granular configuration of DSCP marking.

The PDG/TTG functioning as a TTG can perform DSCP marking of packets sent over the Wu interface in the downlink direction to the WLAN UEs and over the Gn' interface in the uplink direction to the GGSN.

In the PDG Service Configuration Mode of the system's CLI, you use the **`ip qos-dscp`** command to control DSCP markings for downlink packets sent over the Wu interface in IPSec tunnels, and use the **`ip gnp-qos-dscp`** command to control DSCP markings for uplink packets sent over the Gn' interface in GTP tunnels.

The Diffserv markings are applied to the IP header of every transmitted subscriber data packet. DSCP levels can be assigned to specific traffic patterns in order to ensure that the data packets are delivered according to the precedence with which they are tagged. The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest).

For the interactive traffic class, the PDG/TTG supports per-gateway service and per-APN configurable DSCP marking for uplink and downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The following matrix can be used to determine the Diffserv markings used based on the configured traffic class and Allocation/Retention Priority:

Table 2. Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21

Allocation Priority	1	2	3
3	af21	af21	af21

WLAN Access Control

The PDG/TTG enables WLAN access control by enabling you to limit the number of IKEv2/IPSec tunnels per subscriber session.

In the PDG Service Configuration Mode of the system's CLI, the **`max-tunnels-per-ue`** command can be used to specify the maximum number of IKEv2/IPSec tunnels per subscriber session.

The number of tunnels per UE is limited by the NSAPI (Network Service Access Point Identifier) range, which is 5 to 15. Hence, the configurable maximum number of tunnels is 11, within the range of 1 to 11, with a default value of 11.

RADIUS and Diameter Support

RADIUS and Diameter support on the PDG/TTG provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscribers. The benefits of using AAA are:

- Higher flexibility for subscriber access control
- Better accounting, charging, and reporting options
- Industry standard RADIUS and Diameter authentication

The Remote Authentication Dial-In User Service (RADIUS) and Diameter protocols can be used to provide AAA functionality for subscribers. The PDG/TTG supports EAP authentication based on both RADIUS and Diameter protocols.

The AAA functionality on the PDG/TTG provides a wide range of configuration options via AAA server groups, which allow a number of RADIUS/Diameter parameters to be configured in support of the PDG service.

Currently, two types of authentication load-balancing methods are supported: first-server and round-robin. The first-server method sends requests to the highest priority active server. A request will be sent to a different server only if the highest priority server is not reachable. With the round-robin method, requests are sent to all active servers in a round-robin fashion.

The PDG/TTG can detect the status of the AAA servers. Status checking is enabled by configuration in the AAA Server Group Configuration Mode of the system CLI. Once an AAA server is detected to be down, it is kept in the down state up to a configurable duration of time called the dead-time period. After the dead-time period expires, the AAA server is eligible to be retried. If a subsequent request is directed to that server and the server properly responds to the request, the system makes the server active again.

The PDG/TTG generates accounting messages on successful session establishment. For a TTG session, the system creates an IPsec SA for a subscriber session after it creates the GTP tunnel to the GGSN over the Gn' interface. The TTG sends an accounting START message to the AAA server after successful completion of both GTP tunnel creation on the Gn' interface and IPsec SA creation on the Wu interface.

IMPORTANT: For more information on AAA configuration, refer to the *AAA Interface Administration and Reference.*

EAP Fast Re-authentication Support

When subscriber authentication is performed frequently, it can lead to a high network load, especially when the number of currently connected subscribers is high. To address this issue, the PDG/TTG can employ fast re-authentication, which is a more efficient method than the full authentication.

Fast re-authentication is an EAP (Extensible Authentication Protocol) exchange that is based on keys derived from a preceding full authentication exchange. The fast re-authentication mechanism can be used during both EAP-AKA and EAP-SIM authentication.

When fast re-authentication is enabled, the PDG/TTG receives a fast re-auth ID from the UE in the IDi payload of the IKE_AUTH_REQ message. The PDG/TTG sends the fast re-auth ID to the AAA server in an Authentication Request message to initiate fast re-authentication.

During fast re-authentication, the PDG/TTG handles two separate IKE/IPSec SAs, one for the original session and one for re-authentication. The re-authentication SA remains for a very short period until the fast re-authentication is successful. After the successful fast re-authentication, the PDG/TTG assigns the UE with the same IP address. The SGTP service running on the PDG/TTG identifies the original session and replicates the same session using the same IP address assignment. The PDG/TTG then deletes the original session SA.

The AAA server fall backs to full authentication in the following scenarios:

- When the AAA server does not support fast re-authentication.
- When the number of times a fast re-authentication is allowed after a successful full authentication exceeds the limit configured on the AAA server.
- When the EAP server does not have the permanent subscriber identity to perform a fast re-authentication.

Pseudonym NAI Support

The PDG/TTG supports the use of pseudonym NAIs (Network Access Identifiers) to protect the identity of subscribers against tracing from unauthorized access networks.

Pseudonym NAIs are allocated to the WLAN UEs by the EAP server along with the last successful full authentication. The EAP server maintains the mapping of pseudonym-to-permanent identity for each subscriber. The UEs store this mapping in non-volatile memory to save it across reboots, and then use the pseudonym NAI instead of the permanent one in responses to identity requests from the EAP server.

Multiple APN Support for IPSec Access

The PDG/TTG supports multiple wireless APNs for the same UE (the same IMSI) for use during subscriber authentication.

To support subscribers while they attempt to access multiple services, the PDG/TTG enables multiple subscriber authorizations via multiple wireless APNs. Each time a UE attempts to access a service, the PDG/TTG receives a new APN from the UE in the IDr payload of its first IKE_AUTH_REQ message, and the PDG/TTG initiates a new authorization as a distinct session.

Lawful Intercept

The PDG/TTG supports lawful interception (LI) of subscriber session information to provide telecommunication service providers (TSPs) with a mechanism to assist law enforcement agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

Law Enforcement Agencies (LEAs) provide one or more Telecommunication Service Providers (TSPs) with court orders or warrants requesting the monitoring of a particular target. The targets are identified by information such as their Network Access Identifier (NAI), Mobile Station Integrated Services Digital Network (MSISDN) number, or International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the PDG/TTG serves as an access function (AF) and performs monitoring for either new PDP contexts ("camp-on") or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface.

Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

For more information about the Lawful Intercept feature, see the *Lawful Intercept Configuration Guide.*

IMS Emergency Call Handling

The PDG/TTG supports IMS emergency call handling per 3GPP TS 33.234. This feature is enabled by configuring a special WLAN access point name (W-APN), which includes a W-APN network identifier for emergency calls (sos, for example), and can be configured with no authentication.

The DNSs in the network are configured to resolve the special W-APN to the IP address of the PDG/TTG. When a WLAN UE initiates an IMS emergency call, the UE sends a W-APN that includes the same W-APN network identifier (sos) as the one that is configured on the PDG/TTG. This W-APN network identifier is prefixed to the W-APN operator identifier per 3GPP TS 23.003. The W-APN operator identifier sent by the UE must match the PLMN ID (MCC and MNC) that is configured on the PDG/TTG (visited network). When the PDG/TTG receives the W-APN from the UE in the IDr, the PDG/TTG marks the call as an emergency call and proceeds with call establishment, even in the event of an authentication or EAP failure from the AAA/EAP server.

If the PDG/TTG detects that an old IKE SA for the special W-APN already exists, it deletes the IKE SA and sends an INFORMATIONAL message with a Delete payload to the WLAN UE to delete the old IKE SA on the UE.

IPSec Session Recovery Support

The IPSec session recovery feature is a licensed feature. It provides seamless failover and nearly instantaneous reconstruction of subscriber session information in the event of a hardware or software fault within the same chassis, preventing a fully-connected user session from being dropped. For information about the required software license for this feature, contact your sales representative.

IPSec session recovery is performed by mirroring key software processes (the IPSec manager, session manager, and AAA manager, for example) on the PDG/TTG. These mirrored processes remain in an idle state (in standby mode), where they perform no processing until they may be needed in the case of a software failure (a session manager task aborts, for example). The system spawns new instances of standby mode sessions and AAA managers for each active control processor being used.

Additionally, other key system-level software tasks such as VPN manager are performed on a physically separate Packet Services Card (PSC/PSC2) to ensure that a double software fault (the session manager and the VPN manager fail at same time on same card, for example) cannot occur. The PSC/PSC2 used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled. At a minimum, four PSCs/PSC2s (3 active and 1 standby) are required on the chassis to support the IPSec session recovery feature.

IMPORTANT: For more information about session recovery support, refer to *Session Recovery* in the *System Enhanced Feature Configuration Guide.*

Congestion Control

Congestion control allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition.

Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds:** Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.

A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.

- **Port Utilization Thresholds:** If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
- **Port-specific Thresholds:** If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
- **Service Congestion Policies:** Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

IMPORTANT: For more information on congestion control, refer to the *System Enhanced Feature Configuration Guide.*

Bulk Statistics

Bulk statistics allow operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. The following is a partial list of supported schemas:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **PDG**: Provides PDG service statistics
- **APN**: Provides Access Point Name statistics

The system supports the configuration of up to four sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics Server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

IMPORTANT: For more information on bulk statistic configuration, refer to the *Configuring and Maintaining Bulk Statistics* chapter of the *System Administration Guide.*

Threshold Crossing Alerts

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outages. Typically, these conditions are temporary (i.e., high CPU utilization or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports threshold crossing alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP trap would be sent.

The following thresholding models are supported by the system:

- **Alert:** A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm:** Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.
- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated messages pertaining to the condition of a monitored value are generated with a severity level of WARNING. Logs are supported in both the Alert and the Alarm models.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered outstanding until a the condition no longer exists or a condition clear alarm is generated. Outstanding alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.

IMPORTANT: For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

Features Not Supported in This Release

The following features are not supported in this PDG/TTG software release:

- Session recovery
- Link aggregation
- IPv6
- MPLS
- NAT
- Firewall
- Peer-to-Peer

How the PDG/TTG Works

This section describes the PDG/TTG functioning as a TTG during connection establishment.

TTG Connection Establishment Call Flow

The call flow in the figure below shows the message flow during connection establishment. The table that follows the figure describes each step in the call flow.

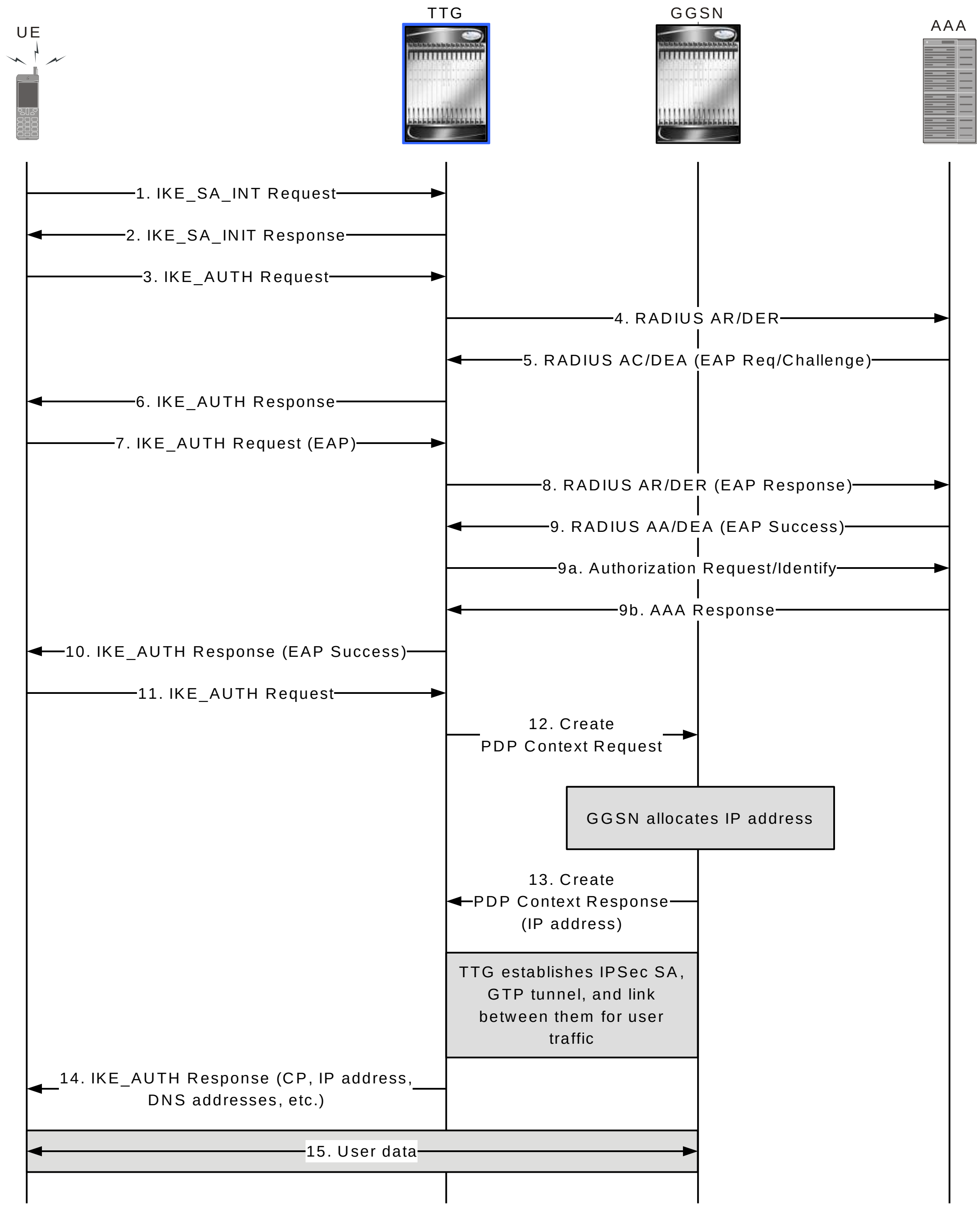


Table 3. TTG Connection Establishment Call Flow

Step	Description
1.	After receiving the IP address of the TTG from the WiFi access point, the UE initiates an IKEv2/IPSec tunnel by sending an IKE_SA_INIT Request to the TTG. The UE includes the SA, KE, Ni, and NAT-Detection Notify payloads in the IKEv2 exchange.

Step	Description
2.	The TTG processes the IKE_SA_INIT request for the appropriate PDG/TTG service (bound by the destination IP address in the IKEv2 INIT Request). The TTG responds with an IKE_SA_INIT Response with the SA, KE, and Nr payloads, and NAT-Detection Notify payloads. The TTG will start the IKEv2 setup timer when sending the IKE_SA_INIT Response. With the IKEv2 SA INIT exchanges, the WLAN UE negotiates cryptographic algorithms, exchanges the nonce, and performs a Diffie-Hellman exchange.
3.	Upon receiving a successful IKE_SA_INIT Response from the TTG, the UE sends an IKE_ AUTH Request for the first EAP-AKA authentication. The UE also includes an IDi payload, which contains the NAI, SA, TSi, TSr, CP (requesting an IP address and DNS address) payloads. The IDr payload is the requested W-APN. The UE does not include AUTH payload to indicate that it will use the EAP method. The NAI can either be from the IMSI or a pseudonym.
4.	Upon receiving the IKE_AUTH Request from UE, the TTG sends an Authentication Request (RADIUS Access Request or DER) message to the AAA server. The TTG sends the Authentication Request message with an EAP (Identity Response) AVP to the AAA Server, including the user identity and W-APN.The W-APN information is included in the called-station-id RADIUS attribute in all Access-Request messages towards the AAA server. The TTG includes a parameter indicating that the authentication is being performed for tunnel establishment. This helps the AAA server to distinguish between authentications for WLAN access and authentications for tunnel setup. The TTG starts the session setup timer upon receiving the IKE_AUTH Request from the UE. Note that the TTG sends the W-APN received in the IDr payload in IKEv2 messages as is to the AAA server. This helps the AAA server to look up the authorization database based on the W-APN name. When sending messages to the HLR (or HSS), the AAA server maps the W-APN name into the real APN configured in the HLR (or HSS).
5.	The AAA server initiates the authentication challenge. The user identity is not requested again, as in a normal authentication process, because there is the certainty that the user identity received in the EAP Identity Response message has not been modified or replaced by any intermediate node. This is because the user identity is received via an IKEv2 secure channel which can only be decrypted and authenticated by the end points (the TTG and the WLAN UE). The TTG receives a DEA with a Result-Code AVP specifying to continue EAP authentication. For RADIUS, this is an access challenge message. The TTG accepts EAP-Payload AVP contents.
6.	The TTG sends an IKE_ AUTH Response back to the UE in the EAP payload. Depending upon the configuration, the TTG can include IDr (TTG-ID) and CERT payloads. The TTG allows IDr and CERT configurations in the PDG service. If the PDG service is configured to do so, the TTG can also include an AUTH payload in IKE_AUTH Response. The UE receives the IKE_AUTH Response from TTG.
7.	Upon receiving the IKE_AUTH Response from the TTG, the UE processes the exchange and sends a new IKE_AUTH Request with an EAP payload. The TTG receives the new IKE_AUTH Request from the UE.
8.	The TTG sends a DER (or RADIUS AR) message to the AAA server. This DER message contains the EAP-Payload AVP with an EAP-AKA challenge or EAP-SIM challenge response and challenge received from the UE.

Step	Description
9.	The AAA server sends the DEA back to the TTG with Result-Code AVP as Success. The EAP-Payload AVP message also contains an EAP result code as Success. The TTG also receives the MSK (keying materials) from the AAA server, which is used for further key computation. When using Diameter, the MSK is encapsulated in the EAP-Master-Session-Key parameter. The AAA server also includes several authorization AVPs. When the checks for an IMS emergency call fail, the AAA Server also sends an Authentication Answer that includes an EAP Failure to the TTG. Note that steps 9a. and 9b. (described below) may not be required if authorization attributes or AVPs are present in the Access-Accept message containing the EAP-Success. As explained in step 5 above, if the W-APN is present in all the Access-Request messages from the TTG to the AAA server, the AAA server can use the W-APN to look up the authorization database to retrieve the parameters. If the TTG has done the W-APN-to-real-APN mapping and includes the mapped APN in the AAA messages, then the TTG perform steps 10a. and 10b., and include the W-APN in a separate message after successful EAP-authentication. 9a. The TTG sends an Authorization Request message with an empty EAP AVP, but containing the W-APN, to the AAA server. The AAA server checks the user's subscription information whether the user is authorized to establish a tunnel.The IKE SA counter for that W-APN is incremented. If the maximum number of IKE SAs for that W-APN is exceeded, the AAA server sends an indication to the TTG that established the oldest active IKE SA (it could be the same TTG or a different one) to delete the oldest established IKE SA. The AAA server then updates the counters tracking the active IKE SAs for the W-APN accordingly. 9b. The AAA server sends the AA-Answer to the TTG. The AAA server sends the IMSI within the AA-Answer.
10.	The TTG sends the IKE_AUTH Response back to UE with the EAP payload.
11.	The UE sends the final IKE_AUTH Request with the AUTH payload computed from the keys. The TTG uses the MSK to generate the AUTH parameters in order to authenticate the IKE_SA_INIT phase messages. These first two messages had not been authenticated before as there was no key material available yet. When used over IKEv2, the shared secret generated in an EAP exchange (the MSK) is used to generate the AUTH parameters. The TTG processes the IKE_AUTH Request, checks the validity of AUTH payload, and initiates PDP context activation with the GGSN.
12.	The TTG sends a Create PDP Context Request to the GGSN. The GGSN processes the request and assigns an IP address to the UE.
13.	The GGSN sends a Create PDP Context Response to the TTG. The TTG sets up an IPsec SA.
14.	The TTG sends an IKE_AUTH Response with the AUTH payload computed from the MSK. The TTG assigns the IP address received from the GGSN to the UE in the configuration payload along with DNS addresses and other parameters.
15.	The TTG session/IPSec SA is fully established and ready for data transfer.

Supported Standards

The PDG/TTG complies with the following standards.

- 3GPP References
- IETF References

3GPP References

- 3GPP TS 22.234 (V8.1.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 7)".
- 3GPP TS 23.003 (V7.9.0): "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 7)".
- 3GPP TS 23.234 (V6.10.0 and V7.5.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)".
- 3GPP TS 23.327 (V8.4.0): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems (Release 8)".
- 3GPP TS 24.234 (V8.3.0): "Group Core Network and Terminals; 3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3 (Release 8)".
- 3GPP TS 29.060 (V7.9.0): "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 7)".
- 3GPP TS 29.234 (V8.1.0): "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (Release 8)".
- 3GPP TS 32.252 (V7.0.0): "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Wireless Local Area Network (WLAN) charging (Release 7)".
- 3GPP TS 33.234 (V6.9.0): "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3G Security; Wireless Local Area Network (WLAN) interworking security (Release 6)".

IETF References

- RFC 2104 (February 1997): “HMAC: Keyed-Hashing for Message Authentication”.
- RFC 2246 (January 1999): “The TLS Protocol, Version 1.0”.
- RFC 2401 (November 1998): “Security Architecture for the Internet Protocol”.
- RFC 2403 (November 1998): “The Use of HMAC-MD5-96 within ESP and AH”.
- RFC 2404 (November 1998): “The Use of HMAC-SHA-1-96 within ESP and AH”.
- RFC 2405 (November 1998): “The ESP DES-CBC Cipher Algorithm With Explicit IV”.
- RFC 2451 (November 1998): “The ESP CBC-Mode Cipher Algorithms”.
- RFC 3526 (May 2003): “More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)”.
- RFC 3539: (June 2003): “Authentication, Authorization and Accounting (AAA) Transport Profile”.
- RFC 3602 (September 2003): “The AES-CBC Cipher Algorithm and Its Use with IPSec”.
- RFC 3706 (February 2004): “A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers”.
- RFC 4186 (January 2006): “Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”.
- RFC 4187 (January 2006): “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”.
- RFC 4301 (December 2005): “Security Architecture for the Internet Protocol”.
- RFC 4302 (December 2005): “IP Authentication Header”.
- RFC 4303 (December 2005): “IP Encapsulating Security Payload (ESP)”.
- RFC 4305 (December 2005): “Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”.
- RFC 4306 (December 2005): “Internet Key Exchange (IKEv2) Protocol”.
- RFC 4307 (December 2005): “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)”.
- RFC 4308 (December 2005): “Cryptographic Suites for IPSec”.
- RFC 4478 (April 2006): “Repeated Authentication in Internet Key Exchange (IKEv2) Protocol”.
- RFC 4718 (October 2006): “IKEv2 Clarifications and Implementation Guidelines”.
- RFC 4835 (April 2007): “Cryptographic Algorithm Implementation RFC Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”.

Chapter 2
PDG/TTG Configuration

This chapter provides configuration instructions for the PDG/TTG (Packet Data Gateway/Tunnel Termination Gateway).

IMPORTANT: Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational.

The following section is included in this chapter:

Configuring the System to Perform as a TTG

This section provides a high-level series of steps and associated configuration file examples for configuring the system to perform as a TTG in a test environment. For a configuration example without the instructions, refer to Appendix B, Sample Configuration Files.

Information provided in this section includes the following:

- Required Information
- TTG Configuration

Required Information

The following sections describe the minimum amount of information required to configure and make the TTG operational in the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context.

Table 4. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet mask	IPv4 address assigned to the interface. Multiple addresses and subnet masks are needed if multiple interfaces will be configured.
Physical Ethernet port number	The physical Ethernet port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.

Required Information	Description
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as ftpd and/or telnetd.

Required PDG Context Configuration Information

The following table lists the information that is required to configure the PDG context.

Table 5. Required Information for PDG Context Configuration

Required Information	Description
PDG context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the PDG context is recognized by the system.
Configuration for the Secure Interface to the UEs in the WLAN	
WLAN interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the Wu interface that carries IPSec tunnels between the UEs in the WLAN and the PDG/TTG.
AAA interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the Wm interface between the AAA server and the PDG/TTG.
Loopback interface	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the PDG/TTG loopback interface.
IP addresses and subnet masks	IPv4 addresses and subnet masks assigned to the WLAN, AAA, and loopback interfaces above.
Physical Ethernet port numbers	The physical Ethernet port to which the PDG interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	The gateway IP address for configuring the IP route from the PDG interface to the WLAN.
AAA configuration information	Identify the IP addresses of the RADIUS/Diameter server.
EAP profile name(s) (required for the EAP authentication method)	The name(s) of the EAP profile(s) to be used for UE authentication.
IKEv2 transform set name(s)	The name(s) of the IKEv2 transform set(s) to be used.

Required Information	Description
IPSec transform set name(s)	The name(s) of the IPSec transform set(s) to be used.
Crypto template name(s)	The name(s) of the IKEv2 crypto template(s) to be used.

Required PDG Service Configuration Information

The following table lists the information that is required to configure the PDG service.

Table 6. Required Information for PDG Service Configuration

Required Information	Description
PDG service name	The name of the PDG service, which must be from 1 to 63 alpha and/or numeric characters. The PDG service name can be the same across all PDG services within the same context and across all contexts.
IP address of the WLAN interface	The IP address of the WLAN interface configured in the PDG context is needed to start the PDG service.
SGTP service name	A unique alpha and /or numeric name for the SGTP service configuration.
SGTP context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the SGTP context is recognized by the system.
Crypto template name	The name of the IKEv2 crypto template to be used.
PLMN ID (Public Land Mobile Network Identifier)	The MCC (Mobile Country Code) and MNC (Mobile Network Code) for the PDG/TTG.
PDG/TTG Mode	The mode in which the PDG/TTG functions: • In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN. • In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service. **IMPORTANT:** PDG mode is not supported in this software release.

Required SGTP Context Configuration Information

The following table lists the information that is required to configure the SGTP context.

Table 7. Required Information for SGTP Context Configuration

Required Information	Description
SGTP context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the SGTP context is recognized by the system.
DNS interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the interface between the DNS and the PDG/TTG.
SGTP interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. This is the Gn' interface between the TTG and the GGSN.
Logical interface address(es)	IP address(es) and subnet(s) are assigned to the logical interface(s) which are then associated with physical ports.
Gateway IP address	The gateway IP address for configuring the IP route from the SGTP interface to the GGSN.

Required SGTP Service Configuration Information

The following table lists the information that is required to configure the SGTP service.

Table 8. Required Information for SGTP Service Configuration

Required Information	Description
SGTP service name	A unique alpha and /or numeric name for the SGTP service configuration.
GTP-U address	An IP address that is associated with an interface in the current context. This is used for GTP-U over the Gn' interface.
GTP-C address	An IP address that is associated with an interface in the current context. This is used for GTP-C over the Gn' interface.

Required DNS Client Configuration Information

The following table lists the information that is required to configure a DNS client in the SGTP context. This DNS client is used during DNS resolution to resolve the received APN to the IP address of the GGSN.

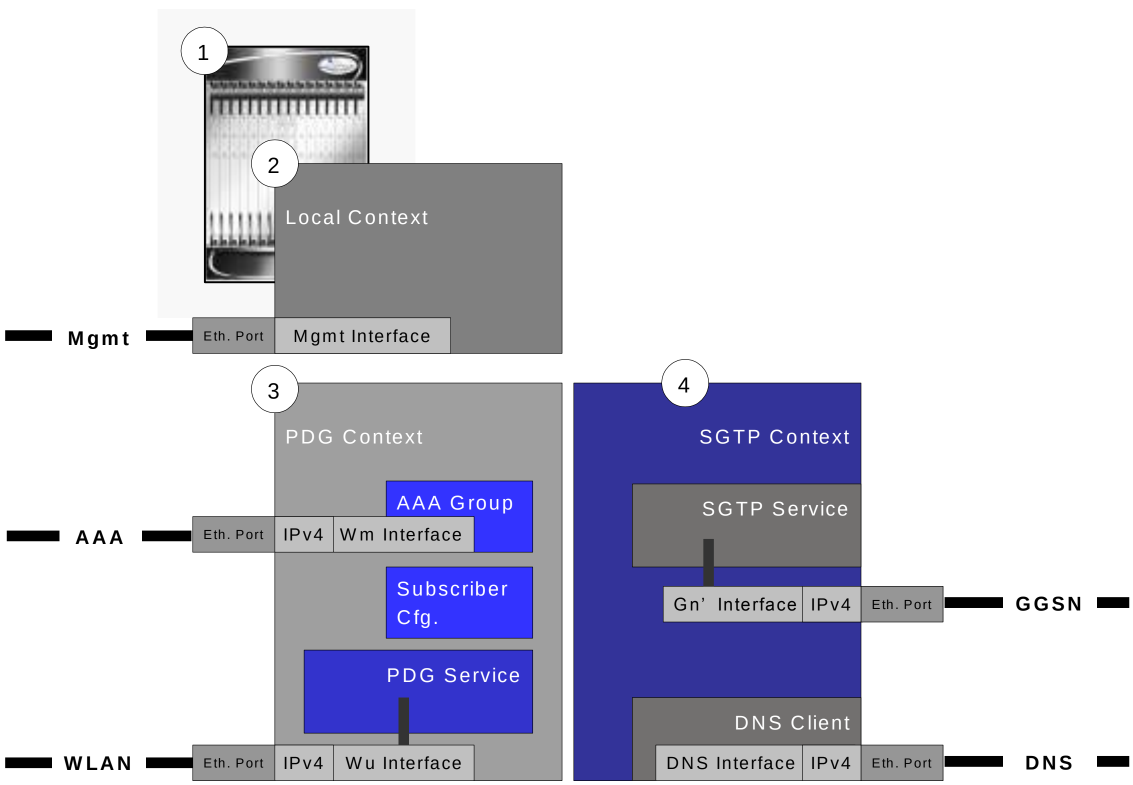
Table 9. Required Information for DNS Client Configuration

Required Information	Description

Required Information	Description
Primary DNS IP address	IPv4 address of the primary domain name server.
Secondary DNS IP address	IPv4 address of the secondary domain name server.
DNS Information	The IP addresses of the primary and secondary DNSs and the local DNS client address.

TTG Configuration

The figure below shows the contexts in which TTG configuration occurs.



To configure the system to perform as an TTG:

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide.*

Step 2 Set initial configuration parameters by modifying the local context found in the section Initial Configuration.

Step 3 Create the PDG context, PDG service, AAA (Authentication, Authorization, and Accounting) group configuration, EAP profile configuration, IKEv2 and IPSec transform set configuration, and crypto template configuration by applying the example configuration found in the section PDG Context Configuration.

Step 4 Create the SGTP context and SGTP service by applying the example configuration found in the section SGTP Context Configuration.

Step 5 Log system activity by applying the example configuration found in the section Logging Configuration.

Step 6 Save the configuration by following the steps found in the chapter *Verifying and Saving Your Configuration* in this guide.

Initial Configuration

Set local system management parameters by applying the example configuration in the section Modifying the Local Context.

Modifying the Local Context

Use the following example to create a management interface, configure remote access capability, and set the default subscriber in the local context:

```
configure
    context local
        interface <mgmt_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        server sshd
            subsystem sftpd
            exit
        server telnetd
            exit
        subscriber default
            exit
        administrator <name> encrypted password <password> ftp
        aaa group default
```

```
         exit
       gttp group default
          exit
       ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <mgmt_interface_name> local
       exit
    end
```

The system automatically creates a default subscriber, default AAA group, and default GTTP group whenever a context is created. The **ip route** command in this example creates a default route for the management interface.

PDG Context Configuration

Step 1 Create the context in which the PDG service will reside by applying the configuration in the section Creating the PDG Context.

Step 2 Create the AAA group by applying the configuration in the section Creating the AAA Group.

Step 3 Create the EAP (Extensible Authentication Protocol) profile by applying the configuration in the section Creating the EAP Profile.

Step 4 Create from one to six IKEv2 transform sets by applying the configuration in the section Creating IKEv2 Transform Sets.

Step 5 Create from one to four IPSec transform sets by applying the configuration in the section Creating IPSec Transform Sets.

Step 6 Create the crypto template for IKEv2 SA negotiation and specify the associated EAP profile by applying the configuration in the section Creating the Crypto Template.

Step 7 Create the PDG service by applying the example configuration in the section Creating the PDG Service.

Creating the PDG Context

Use the following example to create the PDG context and the Wu interface between the UEs in the WLAN and the PDG/TTG, and to bind the interface to an Ethernet port:

```
configure
    context <pdg_context_name>
        interface <wlan_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        interface <pdg_loopback_interface_name> loopback
            ip address <ip_address> <subnet_mask>
            exit
        ip route 0.0.0.0 0.0.0.0 <gateway_ip_address> <wlan_interface_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        bind interface <wlan_interface_name> <pdg_context_name>
        end
```

The **ip route** command in this example creates a default route for the Wu interface between the UEs in the WLAN and the PDG/TTG. The Wu interface carries the IPSec tunnels between the UEs and the PDG/TTG.

Creating the AAA Group

Use the following configuration example to create the AAA group configuration for UE authentication and to bind the interface to an Ethernet port:

```
configure
    context <pdg_context_name>
        interface <pdg_aaa_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        radius attribute nas-ip-address address <ip_address>
        radius dictionary <aaa_custom-dictionary>
        radius server <ip_address> encrypted key <key> port <port_num>
```

```
      radius accounting server <ip_address> encrypted key <key> port <port_num>
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <aaa_pdg_interface_name> <pdg_context_name>
      end
```

This example places the AAA group in the PDG context.

Creating the EAP Profile

Use the following commands to configure an EAP profile for UE authentication:

```
configure
   context <pdg_context_name>
      eap-profile <eap_profile_name>
         mode authenticator-pass-through
         end
```

In this example, the EAP method is used for UE authentication. The **eap-profile** command creates the EAP profile to be used in the crypto template (configured below) for the PDG service.

The **mode authenticator-pass-through** command specifies that the PDG/TTG functions as an authenticator pass-through device, enabling an external EAP server to perform UE authentication.

Creating IKEv2 Transform Sets

Use the following example to create the required number of IKEv2 transform sets:

```
configure
   context <pdg_context_name>
      ikev2-ikesa transform-set <ikev2_ikesa_tset1>
         encryption aes-cbc-128
         group 2
         hmac sha1-96
```

```
prf sha1
exit
```

This example shows default values.

Creating IPSec Transform Sets

Use the following example to create the required number of IPSec transform sets:

```
configure
    context <pdg_context_name>
       ipsec transform-set <ipsec_tset1>
       encryption aes-cbc-128
       group 2
       hmac sha1-96
       mode tunnel
          exit
```

This example shows default values.

Creating the Crypto Template

Use the following configuration example to create the crypto template used to define a cryptographic policy for the PDG service:

```
configure
    context <pdg_context_name>
       crypto template <crypto_template_name> ikev2-subscriber
          certificate <name>
          natt
          authentication eap profile <eap_profile_name>
          ikev2-ikesa transform-set list <ikev2_ikesa_tset1>
          payload <payload_name_1> match childsa
```

```
      ip-address-allocation dynamic
      ipsec transform-set list <ipsec_tset1>
      exit
   payload <payload_name_2> match childsa
      ipsec transform-set list <ipsec_tset1>
      exit
   ikev2-ikesa keepalive-user-activity
   ikev2-ikesa policy error-notification
      end
```

You must create one crypto template per PDG service. The **ikev2-subscriber** keyword in the **crypto template** command specifies that IKEv2 protocol is used. The **certificate** command binds the specified X.509 trusted certificate to the crypto template. The **natt** command enables NAT traversal initiation for all security associations derived from the crypto template.

The **ikev2-ikesa keepalive-user-activity** command resets the user inactivity timer when keepalive messages are received from the peer. The **ikev2-ikesa policy error-notification** command enables the PDG/TTG to generate Error Notify messages for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

Creating the PDG Service

Use the following example to do the following:

- Create the PDG service.
- Configure the Public Land Mobile Network (PLMN) identifiers on the PDG/TTG.
- Identify the SGTP service to be associated with the PDG service. This is needed to support TTG functionality on the PDG/TTG by enabling the Gn' interface between the TTG and the GGSN.
- Bind the PDG service to the IP address of the PDG loopback interface.
- Bind a crypto template to the PDG service.
- Specify the mode in which the PDG/TTG functions:
  - In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
  - In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

IMPORTANT: PDG mode is not supported in this software release.

```
configure
```

```
    context <pdg_context_name>
       pdg-service <pdg_service_name>
          plmn id mcc <mcc_number> mnc <mnc_number>
          associate sgtp-service <sgtp_service_name>  context
<sgtp_context_name>
          bind <ip_address> crypto-template <crypto_template_name> mode ttg
          end
```

The IP address that you bind to the PDG service above is used as the connection point for establishing the IKEv2 sessions between the UEs in the WLAN and the PDG/TTG.

SGTP Context Configuration

You need to create an SGTP context and service to enable GPRS Tunneling Protocol (GTP) on the PDG/TTG to use for sending packet data between the TTG and the GGSN. At a bare minimum, you must configure an IP address to use for GTP-C (Control signaling) and an IP address for GTP-U (User data). You also need to configure a DNS client in the SGTP context.

Step 1 Create the SGTP context by applying the configuration in the section Creating the SGTP Context.

Step 2 Create the SGTP service by applying the configuration in the section Creating the SGTP Service.

Step 3 Configure DNS settings for the DNS servers by applying the configuration in the section Configuring the DNS Client.

Creating the SGTP Context

Use the following example to create the SGTP context and interface (the Gn' interface) to the GGSN, create a DNS interface, and bind these interfaces to Ethernet ports:

```
configure
    context <sgtp_context_name>
       interface <dns_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       interface <sgtp_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
```

```
interface <sgtp_loopback_interface_name> loopback
   ip address <ip_address> <subnet_mask>
   exit
ip route 0.0.0.0 0.0.0.0  <gateway_ip_address> <sgtp_interface_name>
exit
port ethernet <slot_number/port_number>
   no shutdown
   bind interface <dns_interface_name> <sgtp_context_name>
   exit
port ethernet <slot_number/port_number>
   no shutdown
   bind interface <sgtp_interface_name> <sgtp_context_name>
   end
```

Creating the SGTP Service

To create the SGTP service:

- Create the SGTP service.
- Specify the IP address of an interface in the current context to use for GTP-C.
- Specify the IP address of an interface in the current context to use for GTP-U.

Use the following example to create the SGTP service:

```
configure
    context <sgtp_context_name>
       sgtp-service <sgtp_service_name>
          gtpc bind <ip_address>
          gtpu bind <ip_address>
          end
```

Configuring the DNS Client

Use the following example to configure the DNS client:

```
configure
    context <sgtp_context_name>
       ip domain-lookup
       ip name-servers <ip_address_primary_dns>
<ip_address_secondary_dns>
       dns client <dns_client_name>
          bind address <dns_client_ip_address> port <number>
          cache ttl positive
          cache ttl negative
          round-robin-answers
          exit
       ip route <dns_server_subnet> <subnet_mask> <gateway_ip_address>
<dns_interface_name>
       end
```

This DNS client is used during DNS resolution to resolve the received APN to the IP address of the GGSN.

Logging Configuration

Use the following example to enable logging:

```
configure
    logging filter active facility sessmgr level <critical/error>
    logging filter active facility ipsec level <critical/error>
    logging filter active facility ttg level <critical/error>
    logging filter active facility pdg level <critical/error>
    logging active
```

Verifying and Saving the Configuration

To verify and save the TTG configuration, follow the instructions in the *Verifying and Saving Your Configuration* chapter in this guide.

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

`show apn all`

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi

 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

IMPORTANT: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type>* *<service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1

Context : test1
```

```
Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
#################################################################################

Displaying Global
AAA-configuration errors
#################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

`[local]host_name#`

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress* | *host_name* [*:port#*] } [*/directory*] */file_name* • **ftp://**[*username* [*:pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* • **sftp://**[*username* [*:pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

IMPORTANT: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices .This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

```
save configuration tftp://config_server/init_config.cfg
```

Chapter 4
Monitoring the PDG Service

This chapter provides information for monitoring the status and performance of the PDG service using the **`show`** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **`show`** command keywords, refer to the *Command Line Interface Reference.*

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system.

Table 10. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View PDG Service Information and Statistics	
View PDG service information	**show pdg-service { all | name** *service_name* **}**
View PDG service statistics	**show pdg-service statistics**
View PDG service bulk statistics	**show bulkstats variables pdg**
View IPSec and IKEv2 Information	
View IPSec security associations	**show crypto ipsec security-associations**
View IPSec transform sets	**show crypto ipsec transform-set**
View IKEv2 security associations	**show crypto ikev2 security-associations**
View IKEv2 transform sets	**show crypto ikev2 transform-set**
View crypto map configuration information	**show crypto map map-type ipsec-ikev2-subscriber**
View IPSec session recovery status	**show ipsec session recovery status**
View IPSec IKEv2 statistics	**show crypto statistics ikev2**
View Congestion Control Information	
View Congestion Control Statistics for PDG	**show congestion-control statistics ipsecmgr**
View Subscriber Information	
Display Session Resource Status	
View session resource status	**show resources session**
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*
View Subscribers Currently Accessing the System	
View a list of subscribers currently accessing the system	**show subscribers all**
View PDG-specific context information for subscriber sessions.	**show subscribers pdg-only**

To do this:	Enter this command:
View PDG-specific context information per PDG service.	**show subscribers pdg-service** *service_name*
View Session Subsystem and Task Information	
Display Session Subsystem and Task Statistics ***IMPORTANT:*** Refer to the *System Software Task and Subsystem Descriptions* appendix in the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View Session Manager statistics	**show session subsystem facility sessmgr all**
View Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping.

Statistics and counters can be cleared using the CLI **`clear`** command. Refer to the *Command Line Interface Reference* for detailed information on using this command.

Appendix A
TTG Sample Configuration File

This appendix contains a sample configuration file for the PDG/TTG. The following configuration is supported:

Sample TTG Configuration

In the following configuration example, commented lines are labeled with the number symbol (#) and variables are identified using italics within brackets (<*variable*>).

Sample TTG Configuration

This section contains the following sample configuration file for a PDG/TTG functioning as a TTG:

```
# Modify the local context for local system management
configure
    context local
        interface <mgmt_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        server sshd
            subsystem sftpd
            exit
        server telnetd
            exit
        subscriber default
            exit
        administrator <name> encrypted password <password> ftp
        aaa group default
            exit
        gttp group default
            exit
        ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        bind interface <mgmt_interface_name> local
        exit
```

```
    end
# Configure the PDG context
configure
    context <pdg_context_name>
        interface <wlan_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        interface <pdg_loopback_interface_name> loopback
            ip address <ip_address> <subnet_mask>
            exit
        ip route 0.0.0.0 0.0.0.0 <gateway_ip_address>
<wlan_interface_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        bind interface <wlan_interface_name> <pdg_context_name>
        end
# Configure the AAA group
configure
    context <pdg_context_name>
        interface <pdg_aaa_interface_name>
            ip address <ip_address> <subnet_mask>
            exit
        radius attribute nas-ip-address address <ip_address>
        radius dictionary <aaa_custom-dictionary>
        radius server <ip_address> encrypted key <key> port <port_num>
        radius accounting server <ip_address> encrypted key <key> port
<port_num>
        exit
    port ethernet <slot_number/port_number>
```

```
        no shutdown
        bind interface <pdg_aaa_interface_name> <pdg_context_name>
        end
#Create the EAP profile
configure
    context <pdg_context_name>
        eap-profile <eap_profile_name>
           mode authenticator-pass-through
           end
#Create the IKEv2 transform sets
configure
    context <pdg_context_name>
        ikev2-ikesa transform-set <ikev2_ikesa_tset1>
           encryption aes-cbc-128
           group 2
           hmac sha1-96
           prf sha1
           exit
#Create the IPSec transform sets
configure
    context <pdg_context_name>
        ipsec transform-set <ipsec_tset1>
        encryption aes-cbc-128
        group 2
        hmac sha1-96
        mode tunnel
           exit
#Create the crypto template
configure
```

```
    context <pdg_context_name>
       crypto template <crypto_template_name> ikev2-subscriber
          certificate <name>
          natt
          authentication eap profile <eap_profile_name>
          ikev2-ikesa transform-set list <ikev2_ikesa_tset1>
          payload <payload_name_1> match childsa
             ip-address-allocation dynamic
             ipsec transform-set list <ipsec_tset1>
             exit
          payload <payload_name_2> match childsa
             ipsec transform-set list <ipsec_tset1>
             exit
          ikev2-ikesa keepalive-user-activity
          ikev2-ikesa policy error-notification
             end
#Create the PDG service
configure
    context <pdg_context_name>
       pdg-service <pdg_service_name>
          plmn id mcc <mcc_number> mnc <mnc_number>
          associate sgtp-service <sgtp_service_name> context
<sgtp_context_name>
          bind <ip_address> crypto-template <crypto_template_name> mode
ttg
          end
# Configure the SGTP context
configure
    context <sgtp_context_name>
       interface <dns_interface_name>
```

```
          ip address <ip_address> <subnet_mask>
          exit
       interface <sgtp_interface_name>
          ip address <ip_address> <subnet_mask>
          exit
       interface <sgtp_loopback_interface_name> loopback
          ip address <ip_address> <subnet_mask>
          exit
       ip route 0.0.0.0 0.0.0.0 <gateway_ip_address>
<sgtp_interface_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <dns_interface_name> <sgtp_context_name>
       exit
    port ethernet <slot_number/port_number>
       no shutdown
       bind interface <sgtp_interface_name> <sgtp_context_name>
       end
#Create the SGTP service
configure
    context <sgtp_context_name>
       sgtp-service <sgtp_service_name>
          gtpc bind <ip_address>
          gtpu bind <ip_address>
          end
#Configure the DNS client
configure
    context <sgtp_context_name>
```

```
        ip domain-lookup

           ip name-servers <ip_address_primary_dns>
<ip_address_secondary_dns>

           dns client <dns_client_name>

              bind address <dns_client_ip_address> port <number>

              cache ttl positive

              cache ttl negative

              round-robin-answers

              exit

        ip route <dns_server_subnet> <subnet_mask> <gateway_ip_address>
<dns_interface_name>

        end

#Enable logging

configure

    logging filter active facility sessmgr level <critical/error>

    logging filter active facility dhost level <critical/error>

    logging filter active facility ipsec level <critical/error>

    logging filter active facility ttg level <critical/error>

    logging filter active facility pdg level <critical/error>

    logging active

    end
```

Appendix B
PDG/TTG Engineering Rules

This appendix provides PDG/TTG (Packet Data Gateway/Tunnel Termination Gateway) engineering rules or guidelines that must be considered prior to configuring the ASR 5000 for your network deployment. These rules apply to installations in which the PDG/TTG is functioning as either a PDG or a TTG network element.

General and network-specific rules are located in Appendix A of the *System Administration Guide.*

The following rules are covered in this appendix:

- IKEv2/IPSec Restrictions
- X.509 Certificate (CERT) Restrictions
- IPv6 Restrictions
- ICMPv6 Restrictions

IKEv2/IPSec Restrictions

The following is a list of known restrictions for IKEv2 and IPSec:

- Each PDG service must specify one crypto template.
- The PDG/TTG supports traffic selectors with just IPv4 address values. IPv6 address values are not supported.
- The PDG/TTG supports IKEv2 only between the UE and the PDG/TTG.
- Multiple Child SAs are not supported.
- While the PFS for UE-initiated IKE SA rekeying will be implemented, the rate for rekeying (with PFS enabled) shall not exceed the rate of the IKEv2 call setup rate. This is because PFS would require performing a new D-H exchange each time a rekey is negotiated, and a performance impact is expected. Also, note that the call setup rate and the rekeying rate are mutually exclusive.
- All IKEv2 packets are sent over IPv4.
- Per RFC 4306 and RFC 4718, the following known restrictions apply with respect to the payload and its order. Violations result in INVALID_SYNTAX being returned which is being enabled or disabled through a configurable, except when the processing is noted as below.
- While RFC 4306 Section 2.19 specifies “CP payload MUST be inserted before the SA payload,” the PDG/TTG does not force strict ordering of this. The PDG/TTG processes these payloads as long as the mobile sends a CP payload anywhere inside the encryption data.
- While RFC 4306 Section 2.23 specifies “The location of the payloads (Notify payloads of type NAT_DETECTION_SOURCE_IP and NAT_DETECTION_DESTINATION_IP) in the IKE_SA_INIT packets are just after the Ni and Nr payloads (before the optional CERTREQ payload),” the PDG/TTG does not force strict ordering of this and still can process these NOTIFY payloads.
- The PDG/TTG supports transform selector payloads with only one traffic selector. The number in the TS field must be set to “1”.
- Traffic selector payloads from the UE support only traffic selectors by IP address range. In other words, the IP protocol ID must be 0. The start port must be 0 and the end port must be 65535.
- The Configuration Payload (CP) is specified in RFC 4306, Section 2.19 (Requesting an Internal Address on a Remote Network) for the situation where dynamic IP address assignment is required. Since the PDG/TTG does not support INTERNAL_IP6_ADDRESS, the CP must include at least the attribute INTERNAL_IP4_ADDRESS.
- As described above, when the PDG/TTG receives IKEv2 messages, the PDG/TTG does not enforce the payloads to be in order. However, when the PDG/TTG sends the response or generates any IKEv2 messages, the PDG/TTG will ensure that payloads are ordered according to RFC 4306.
- Only IKE and ESP protocol IDs are supported. AH is not supported since AH is deprecated in RFC 4306.
- The IKE Protocol ID specification may not use the NONE algorithm for authentication or the ENCR_NULL algorithm for encryption as specified in Section 5 (Security Considerations) of RFC 4306.
- In ESP, ENCR_NULL encryption and NONE authentication cannot be simultaneously used.

- Only one single proposal number can be used. Because RFC 4306 states that the first proposal must be numbered 1, this implies that only proposals with the proposal number value of 1 are supported. The mobile device must send a list of transforms within this single proposal number.
- No more than 16 transform types may be present in a single IKE_SA_INIT or IKE_AUTH Request message. If a deviation from this format is used in the proposal format, the PDG/TTG returns an error of INVALID_SYNTAX.

X.509 Certificate (CERT) Restrictions

The following are known restrictions for the creation and use of X.509 CERT:

- The maximum size of CERT configuration is 1K bytes.
- The PDG/TTG includes the CERT payload only in the first IKE_AUTH Response for the first authentication.
- The CERT payload will be sent in the AUTH response, if configured, irrespective of receiving CERT-REQ payload in the first IKEv2 AUTH request.
- The PDG/TTG will not process a CERT payload from the UE and will respond accordingly (with INVALID_SYNTAX) if the CRITICAL bit is set in the payload.
- If the PDG/TTG receives the CERT-REQ payload with the CRITICAL bit set in the IKE_AUTH request, the PDG/TTG will reject the exchange. If the CRITICAL bit is not set, the PDG/TTG ignores the payload and proceeds with the exchange.
- Only a single CERT payload is supported. While [RFC-4306] mandates the support of up to 4 certificates, only one X.509 certificate will be supported in the IKE_AUTH Response. This is due to the size of an X.509 certificate. Inclusion of multiple certificates in a single IKE_AUTH may result in the IKE_AUTH message not being properly transmitted.

IPv6 Restrictions

There is no support for IPv6 in this software release.

ICMPv6 Restrictions

There is no support for ICMPv6 in this software release.