Adax FastPlane

adax
Legacy to LTE

Data Plane acceleration for high capacity and performance in 3G, 4G, 5G, IoT and M2M networks

Introduction

Adax FastPlane is a high performance data plane solution supporting GTP-U and GRE tunneling that allows users to quickly implement complex data plane solutions for 3G, 4G and 5G mobile networks supporting automatic relaying between GTP tunnels, between GRE tunnels, and between GTP and GRE tunnels.

As network capacity increases so does the need for performance, security and reliability. Adax FastPlane software, and its sister product, SCTP/T (see separate datasheet), are designed to meet the exploding capacity demands of cellular networks, especially from IoT and M2M. This particularly impacts GTP-U and the encapsulation and de-encapsulation of packets, PDP context requests and responses, and packet header insertion and enhancement.

Accelerating GTP and GRE tunnels and offloading GTP data traffic is a critical requirement in the performance of cellular networks, especially for traffic management, policing and load balancing in the core network. Removing bottlenecks in the network increases performance and traffic policing improves Quality of Service.

Adax FastPlane supports the GTPv1-U (GPRS Tunneling Protocol User Plane Version 1) as specified in 3GPP TS 29.060 and TS 29.281 and GRE (Generic Routing Encapsulation) as specified in RFC 2890 and RFC 2784.

4G User Plane

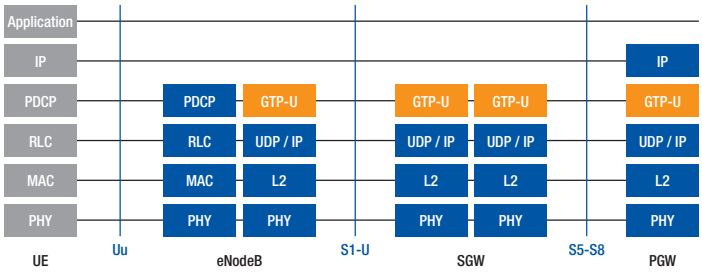

Figure 1 – Control Plane for S1-U and S5-S8

4G Control Plane

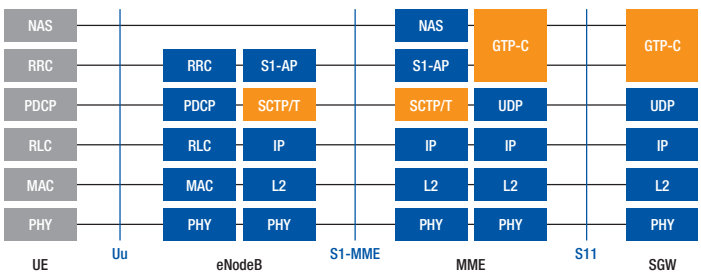

Figure 2 – Control Plane for S1-MME and S11

Adax FastPlane Software Features

- Can be deployed as a virtual network element on a variety of different commercial cloud computing providers, e.g. Amazon AWS, VMware, OpenStack, MS Azure
- Support for Multiple APNs and for Overlapping Addresses for MS devices
- Interworking between IP and GTP-U (GTP Tunnel termination)
- Termination and Relay per PDP context for Mobile Data Offload (GTP Bypass)
- Interworking between two separate GTP tunnels (GTP Relay)
- GTP-U Echo Requests/Responses can be terminated to the host, relayed to another GTP tunnel, processed automatically, or discarded
- Can be used to implement Keyed or unkeyed GRE tunnels
- GRE tunnels can also be configured to relay packets decapsulated from the tunnel to other GRE tunnel(s) or GTP PDP context(s)
- Remote API Library provides loosely coupled application interface enabling user applications and GTP-C stacks to be implemented on the same machine or on different virtual machines in the cloud
- Traffic Policing support for ingress and egress packets. Including DSCP copying and/or remarking and six different Token Bucket Traffic Policing algorithms
- Support for millions of PDP contexts subject to system configuration
- Support for PDP context statistics indications
- Support for PDP context lifetime indications
- IPsec to GTP interworking
- Supports GTPv1-U (GPRS Tunneling Protocol User Plane Version 1) as specified in 3GPP TS 29.060 and TS 29.281 and GRE (Generic Routing Encapsulation) as specified in RFC 2890 and RFC 2784

FastPlane Application Areas

- **Core Network Performance Acceleration**
  - 4G PGW, SGW and MME enhancement
  - 3G SGSN and GGSN enhancement
  - ePDG for secure access to 4G core network
  - Load Balancing, Backhaul & Aggregation
  - QoS Traffic Management and Policing
- **IoT and M2M for Cellular networks**
  - Vehicle telematics ‘connected car’ - Industrial automation, monitoring and control
  - Intelligent transport systems
  - Smart homes and buildings
  - Healthcare

GTP

GTP (GPRS Tunneling Protocol) is a UDP/IP based tunneling protocol used within the core radio control network of 2.5G (UMTS), 3G (GPRS) and 4G (LTE) and 5G cellular networks. GTP is used at various places within the network core, typically between the BSS and SGSN and in the GGSN in 3G networks, and between the eNodeB and SGW and in the PGW in 4G networks. See Figs 1-2 on Pg 1.

GTP consists of two separate protocols: GTP-U is the data plane protocol which tunnels data packets within the core network and GTP-C is the control plane protocol, responsible for setup and teardown of GTP-U tunnels.

GRE

GRE (Generic Routing Encapsulation) is used in various network configurations to provide a generic tunnel capable of transporting various network layer protocols across an IPv4 or IPv6 network. For example, a PGW PDN gateway may use GRE tunnels to provide access to two separate APNs via an Address Family Transition Router as described in RFC 6674. This may be used to provide access to different APNs in the GGSN or PGW where MS Users are assigned overlapping IP addresses for each APN.

Adax FastPlane Remote API Library

Users configure and control Adax FastPlane via the API Library which is linked with the user's application and provides the C-language functions for the application to construct and decode Remote API library packets. It supports all the functions necessary for an external GTP-C or PMIPv6 implementation to set up and tear down GTP Tunnel Endpoints and GTP PDP contexts GRE Tunnel Endpoints, and GRE tunnels.

The FastPlane Library is a loosely coupled application interface. This means that instead of communicating with the Policy Manager via C-language function calls, the user's application or GTP-C protocol stack communicates with it via TCP or UDP packets which contain data structures to control the GTP/GRE data plane. This provides a convenient RPC method which allows user applications and GTP-C stacks to be implemented on the same machine as the GTP/GRE data plane or on a different virtual machine "in the cloud".

DPDK Support

Data Plane Development Kit (DPDK) greatly boosts packet processing performance (up to 10x) and throughput, allowing more time for data plane applications.

Adax FastPlane for Linux/DPDK replaces the kernel components of Adax FastPlane with a DPDK based implementation in Linux user space. The Adax FastPlane for Linux/DPDK has significantly higher performance than the in-kernel version of Adax FastPlane.

Capacity and Reliability for Massive M2M and IoT Connections

IoT and M2M communications represent a significant growth opportunity for the 3GPP ecosystem. Millions of low-speed, low data volume, M2M and IoT devices will be deployed on a massive scale and they will all need to be connected to the core mobile network. This huge increase in the number of devices connecting to the core network over the S1 and Gb interfaces will require highly efficient, high capacity data and control plane protocol implementations such as Adax FastPlane and SCTP/T.

These Adax protocol products deliver the capabilities and performance to handle this massive number of connected devices securely and reliably without impacting overall network performance and Quality of Service, thus improving the user experience.

3GPP and NarrowBand IoT

3GPP is moving ahead with the standardization of NB-IOT. 3GPP TR 45.820, 'Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)', defines a new narrowband radio technology to address the requirements of the IoT. The new technology will provide improved indoor coverage, support a massive number of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption and optimized network architecture. As well as enhancements to the S1 interface to the core network the NB-IOT standard includes the option for the large number of connected devices to use the Gb interface to the base station on a new Cooperative Ultra NarrowBand (C-UNB) and then be interworked in an SGSN to GTP.

IPsec Interworking

Adax FastPlane is integrated with the Adax IPsec package allowing interworking between IPsec and GTP-U/GRE tunnels in applications such as ePDGs which provide secure access to the mobile network core for untrusted WiFi gateways. GTP-C traffic can also be encapsulated into IPsec tunnels to secure the control plane signaling, allowing untrusted networks to be used for networking signaling traffic. As the Adax FastPlane software terminates the IPsec and then encapsulates the GTP-U in one operation it can remove the need for a separate IPsec Gateway.

AFP 0718/01

adax inc
2900 Lakeshore Ave,
Oakland, CA 94610, USA
Tel: (510) 548 7047
Fax: (510) 548 5526
Email: sales@adax.com

adax europe ltd
40 Caversham Road
Reading, Berkshire,
RG1 7EB, UK
Tel: +44 (0) 118 952 2800
Fax: +44 (0) 118 957 1530
Email: sales@adax.co.uk

adax china
Unit B-4 27 floor,
No. 888 Wan Hang Du Road
Shanghai 200042, China
Tel / Fax: +86 21 6386 8802
Email: sales@adax.com