User Guide
IP Connect

Revision: 1.0

maingate

ADDRESS: BOX 244, SE-371 24 KARLSKRONA, SWEDEN
VISITORS: DROTTNINGGATAN 16
PHONE. +46 455 36 37 00 FAX: +46 456 36 37 37
WEB: WWW.MAINGATE.SE

Table of Contents

1 Introduction

This document is intended to be used by the customer during configuration and use of the Maingate IP Connect service.

2 Service overview

Maingate IP Connect provides transparent IP communication between a customer application and terminals equipped with GSM/UMTS GPRS modems using fixed IP addressing. An overview of the functionality is shown in Figure 1 - Service overview.

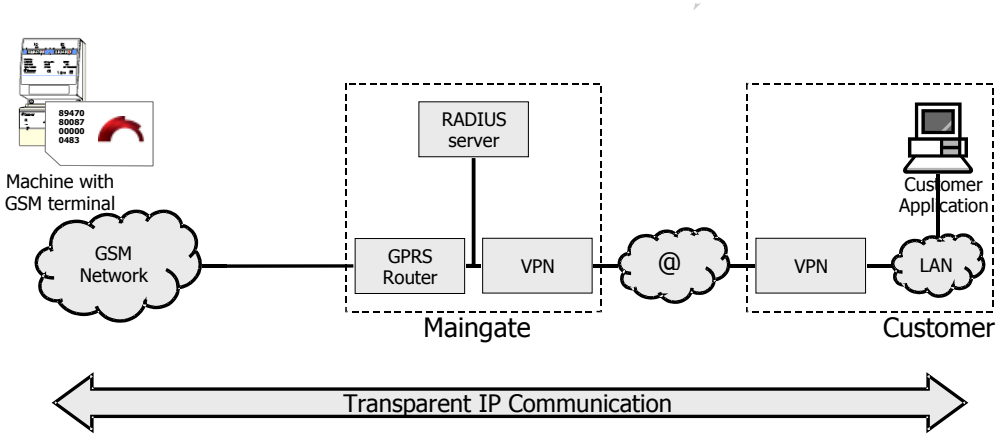

Figure 1 - Service overview

The customer application is connected to Maingate over Internet using a VPN tunnel. When using fixed IP addressing, each terminal is configured once in Maingate's RADIUS with desired parameters that control the communication settings (MSISDN and IP address). Once the configuration has been done, communication is initiated by activating a GPRS PDP Context and thereafter sending IP packets from application or from a terminal.

When your Maingate SIM-cards are delivered, the mapping between MSISDN and IP address is already done. The mapping is showed in Maingate Manager.

The VPN tunnel could either be set up "site-to-site" as in figure above, directly from a host with VPN client software provided by Maingate or with Maingate Managed VPN Router solution using redundant routers for high availability.

2.1 Service specifications

The Maingate IP Connect service supports the following functionality:

- Support for IP addressing according to IPv4
- Customer unique APN with separated IP transport to customer site
- Radius servers at customer site (requires Customer unique APN)

2.2 Terminal requirements

In order for the IP Connect service to be successfully used with a terminal, the terminal must satisfy the following requirements:

- The terminal must be equipped with a GSM or UMTS modem that supports GPRS
- The terminal must be equipped with a Maingate M2M subscription
- The terminal must support PPP according to RFC 1661 of the IETF
- The terminal must support dynamic IP address allocation over PPP

3 Set up of IP Connect

Once the customer has ordered the IP Connect service, Maingate will contact the person stated as Technical Contact Person to agree IP addresses and VPN configuration procedures.

When the account has been configured, a confirmation mail will be sent to the Main Contact Person and Technical Contact Person. Attached to the confirmation mail are two or three documents:

- IP Connect User Guide (this document)
- VPN / MVR / VPN Client Configuration Form, confirming the allocated IP address range and configuration parameters for the VPN tunnel.
- *APN Configuration Form, confirming configuration parameters for the APN, in case of customer unique APN.*

The VPN pre-shared key or user credentials are sent to the customer in separate emails or by SMS.

4 Device IP Ranges

When a terminal is identified and addressed using its IP address, it is vital to secure that each terminal always is allocated a unique IP address. IP Connect performs a check each time a terminal is registered to verify that the IP address is unique when static addressing applies.

In order to avoid that different IP Connect accounts attempt to associate the same IP address to different terminals, each account is only permitted to register IP addresses from a predefined number of IP address ranges. These IP address ranges are compared and verified during service ordering.

NOTE! If one IP Connect account has been allocated a certain range of IP addresses, this range cannot be used by another account. This is the reason why Maingate reserves the right to refuse the use of certain IP addresses.

It is possible to allocate several IP address ranges to one IP Connect account.

When using a customer unique APN, the IP addresses assigned to terminals could be chosen by customer as the traffic will be fully separated from Maingate routing domain. The range must however be specified to Maingate for configuration purposes.

5 IP Configuration

In order for IP Connect to function correctly, the transmission of IP packets between Maingate and the customer must be carefully configured. A VPN tunnel is used to carry the traffic between terminals and application. The VPN tunnel ensures that private IP addresses can be used but also protects data across the Internet and ensures that one customer's traffic is separated from other traffic.

5.1 APN

Maingate offers two types of APN, a common APN and a customer unique APN. The common APN is shared with other Maingate customers, but as no intra APN traffic is allowed and IP traffic is later separated with VPN, one customer cannot access another customer terminals.

The customer unique APN enables traffic separation and APN configuration which only apply for this customer. The IP addresses can be chosen with no restrictions and intra APN traffic could be enabled or disabled for the customer GPRS network or a subnet of the same. Other parameters that can be set are for example DNS servers, DHCP and Radius.

When a customer unique APN is ordered, the "APN Configuration Form" needs to be filled in to setup the APN to fit customer requests. A customer APN also includes the Managed VPN Router service.

5.2 VPN Configuration

IPSec encryption is used for the VPN tunnel between Maingate and the host or LAN connecting the customer application. IPSec is a set of standard protocols for implementing secure communications and encryption key exchange between computers.

An IPSec VPN generally consists of two communications channels between the endpoint hosts: a key-exchange channel over which authentication and encryption key information is passed, and one or more data channels over which private network traffic is carried.

The key-exchange channel is a standard UDP connection to and from port 500. The data channels carrying the traffic between the client and server use IP protocol number 50 (ESP).

More information is available in RFC 2402 (the AH protocol, IP protocol number 51), RFC 2406 (the ESP protocol, IP protocol number 50), and RFC 2408 (the ISAKMP key-exchange protocol).

Configuration details are provided by mail from Maingate after service ordering. The VPN tunnel must be configured according to these methods in order to function.

The IPSec VPN to customer could be set up in two ways. Either with a standard “Site-to-Site” configuration or with a VPN Client software on customer host. Customer will choose which method that is best suitable.

5.3 IP Routing

5.3.1 IP routing when using Maingate common APN

Once the VPN tunnel has been established, the customer network or host must be configured to route applicable packets through the VPN and allow packets from the VPN to reach the customer application. When using VPN Client, this would normally be taken care of automatically by the software itself.

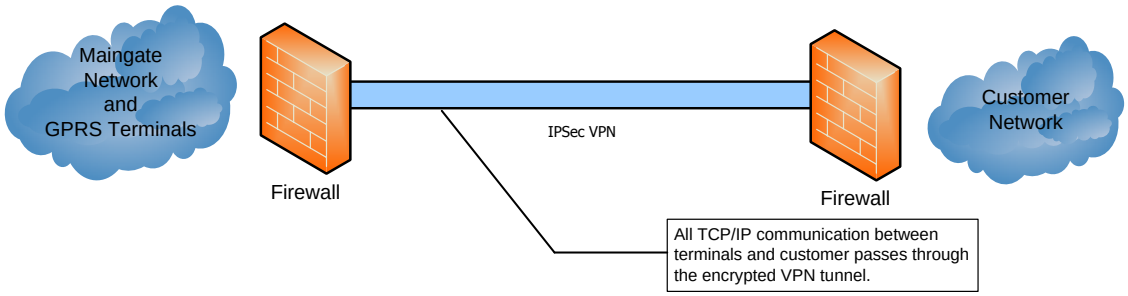

Figure 2 - Terminal communication through the VPN tunnel.

5.3.2 IP routing using customer unique APN

The APN resides on a routing domain separated from Maingate, which lets the customer choose IP addresses for both GPRS terminals and applications on server side. The separation of routing domain is accomplished with a Maingate Managed VPN Router setup, which makes the interface between customer and Maingate in customer premises. This setup is described with Figure below.

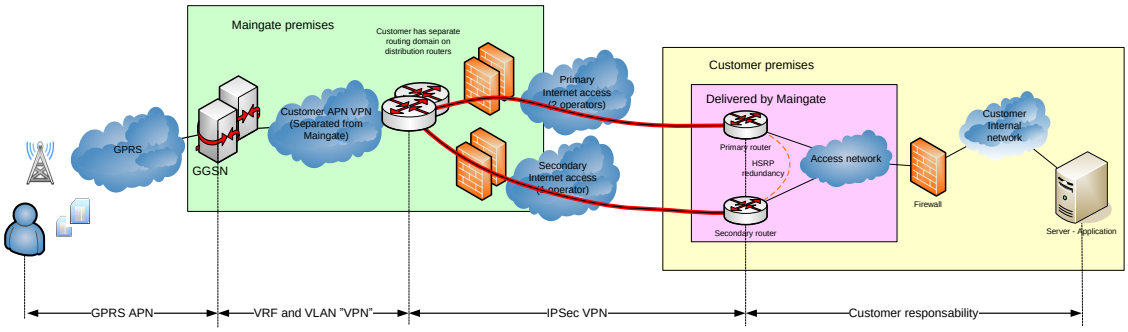

Figure 3 - Terminal communication through the VPN tunnel.

5.4 Firewall Configuration

The customer must secure that the customer's firewall is open to allow the types of IP sessions to pass that are used by terminal and application. If not, the IP packets will be blocked by the customer's firewall and communication will not function correctly. Maingate's firewall towards the VPN tunnel is open to allow for all types of IP sessions to pass.

When using Managed VPN Router with routers placed behind customer firewall, there will also be rules set up to enable traffic to Maingate. These are defined in User Guide for the Managed VPN Router service.

5.5 Terminal Client Configuration

IP communication through IP Connect will not function correctly, if the terminal's IP client is not configured with the correct settings. The terminal must be configured as follows:

- Allow dynamic IP address allocation over PPP
- Default Route or alternatively static routing must be defined for IP Connect

NOTE! If the Default Route or static routing is not configured, the terminal will be able to connect correctly to IP Connect, but not be able to communicate with the application.

6 Communication

After a terminal has been registered in RADIUS and HLR, it is possible to initiate connection to IP Connect and thereafter communicate to and from that terminal.

6.1 PDP Context activation

Before IP packets can be exchanged between terminal and application, the terminal must connect to GPRS. This is accomplished by performing "PDP Context activation" to the APN provided for GPRS from the terminal. (The APN is found in the IP Connect Configuration Form, see section 3.) The supplier of the GSM modem in the terminal should be consulted regarding how to perform PDP Context activation.

After PDP Context activation has been completed successfully, IP communications can be initiated. Should the PDP Context be lost for any reason, it must be re-activated by the terminal before communication can take place again.

Avoid connecting a large number of devices to GPRS at the same time to prevent congestion. If scheduled PDP Context activations are needed, take both time and geographical area into consideration.

6.2 Addressing terminals

During PDP Context activation, the terminal's IP client will be assigned the IP address that this terminal was assigned during registration (see section 6).

The MSISDN parameter uniquely identifies the terminal and provides the mapping to the correct IP address, which identifies the terminal to the customer application. The mapping of parameters for is shown in *Figure 4– Parameter mapping during PDP Context activation*.

Note!	Even though the terminals use dynamic IP address allocation over PPP, the terminal will <u>always</u> be assigned the same IP address from RADIUS or HLR for each PDP Context Activation.

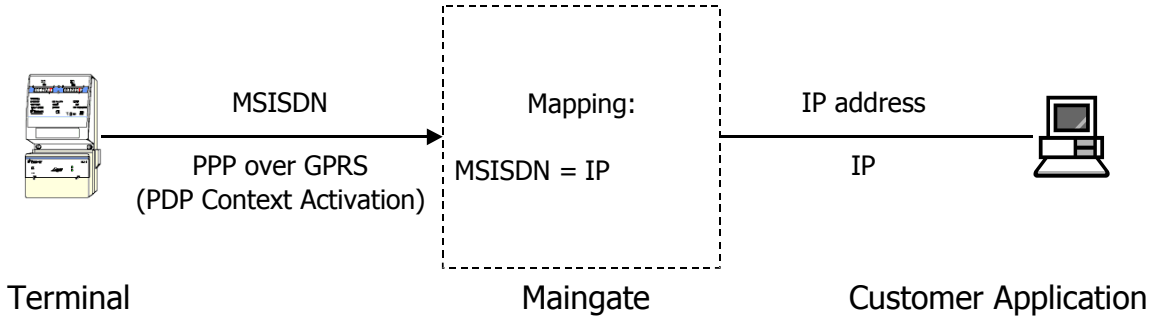

Figure 4– Parameter mapping during PDP Context activation

6.3 PDP Context Disconnection

Normally, an activated PDP Context does not need to be terminated. The PDP Context can be kept open constantly, to assure that the application can communicate to the terminal. IP Connect will not initiate a disconnection.

In some cases, the terminal may lose its PDP Context due to network-related issues. Thus, if a constant IP connection to the terminal is required, the terminal
must contain functionality to identify a disconnection and automatically reconnect to GPRS.

6.4 Maingate Network Services

6.4.1 DNS (Domain Name System)

Terminals will be automatically assigned two of Maingate's DNS-servers when connecting to GPRS. Recursion is on, enabling you to resolve public records.

6.4.2 NTP (Network Time Protocol)

Terminals using IP Connect have access to a local NTP server within Maingate's LAN. This NTP server can be used to perform time synchronisation of terminals using NTP.
The address to use is: ntp.maingate.se

6.4.3 PING (ICMP)

If you want to test the communication from your terminals you can ping the address of ping.maingate.se. This enables you to test the traffic without the need of a fully functional VPN-tunnel. Note that this is only for troubleshooting purposes.

7 Security Aspects

When using IP-based communication, special attention must always be paid to providing adequate security to protect systems and information. Since use of IP Connect effectively expands the customer's LAN to a multitude of connection points that potentially can be used by unauthorised persons, special attention to security in this case.

7.1 Accessible Network Destinations

When a terminal is connected via IP Connect, this terminal can address and communicate with the following network destinations:

1. Customer LAN
2. Maingate Network Services

Figure 5 illustrates the accessible network destinations.

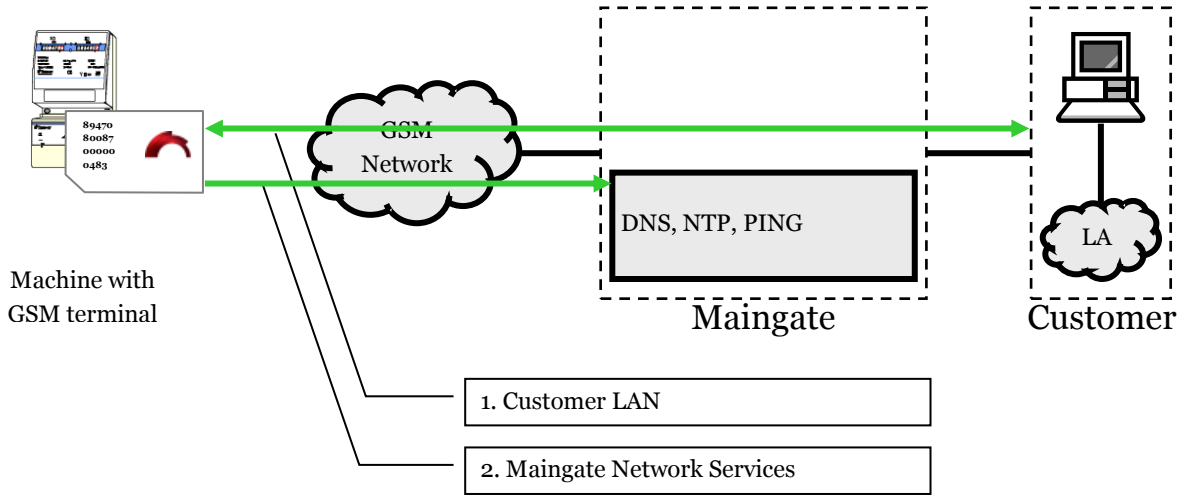

Figure 5 – Accessible network destinations (direction of arrow illustrates what party may initiate communications)

7.2 Terminal and Application Security

Control of a SIM card that is used together with IP Connect and knowledge of the correct APN, gives a malicious attacker the possibility to address the customer's LAN.

To prevent attacks on the customer's network from a terminal, the customer must use a firewall that blocks malicious IP traffic from reaching his systems.

8 Appendix

8.1 Terminology

Account	An IP Connect account containing a group of terminals and a customer application between which communication can take place
API	Application Programming Interface
APN	Access Point Name
GPRS	General Packet Radio Service
HLR	Home Location Register
IETF	Internet Engineering Task Force
IP Default Route	Default destination of unspecified IP packets
LAN	Local Area Network
MVR	Managed VPN Router
NTP	Network Time Protocol
PDP	Packet Data Protocol
PPP	Point-to-Point Protocol
RADIUS	Remote Access Dial-in User Service
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
XML	Extensible Mark-up Language