TELEMEDIDA PARA CLIENTES CON CONSUMOS >5GWH/AÑO< 100GWH/AÑO

INTRODUCCIÓN.-

El presente documento pretende definir el protocolo de comunicaciones de los Terminales Remotos de Telemedida (TRT), de los consumidores conectados a las redes de NORTEGAS, con objeto de facilitar la interconexión, basada en estándares, que según la ORDEN ITC/104/2005 de 28 de Enero, artículo 18, disponía que "En el plazo máximo de nueve meses a partir de la entrada en vigor de la presente Orden, los consumidores con consumos superiores a 5gwh/año, deberán disponer de equipos de telemedida capaces de realizar, al menos, la medición de los caudales diarios".

FUNCIONALIDAD DEL TERMINAL REMOTO DE TELEMEDIDA.-

Con objeto de ofrecer la máxima flexibilidad a los Clientes para decidir el tipo de equipo a instalar, el TRT deberá enviar como ejemplo la trama siguiente:

Va:12345678<return> (8 caracteres con el totalizador de volumen bruto, m3)
Vr:12345678<return> (8 caracteres con el totalizador de volumen corregido, Nm3)
P1.008<return> (Valor de la presión en bares, con tres decimales)
T-13.78<return> (Valor de temperatura, en ºC , con dos cifras y 2 decimales)
@<return> (Indica la existencia de un error en el corrector

- El TRT deberá adquirir del corrector con una periodicidad inferior a 5 minutos, las lecturas de volumen bruto, volumen corregido, presión , temperatura y fallo de corrector.

Las lecturas se enviarán de manera espontánea por el Terminal, mediante mensaje SMS o vía TCP/IP sobre GPRS.

1. SEGURIDAD DE LAS COMUNICACIONES

1.1. CARACTERISTICAS DEL SISTEMA INTRANET IPSec

En el diseño de la interconexión de la Red de NORTEGAS con la red GSM/GPRS del operador se han considerado las necesidades actuales de NORTEGAS, así como posibles futuras evoluciones, con la finalidad de ofrecer una solución de carácter abierto, flexible y adaptable a un entorno de telecomunicaciones cambiante.
El acceso a la red corporativa (Intranet) de NORTEGAS requiere de unas condiciones de seguridad, velocidad y disponibilidad mínimas para ser adoptado. Dicha solución está basada en una arquitectura de conexión indirecta entre la red GSM/GPRS

del operador y NORTEGAS, y cuya seguridad es contemplada mediante la utilización de protocolo IPSec.

1.2. DESCRIPCION DEL SISTEMA DE COMUNICACIONES

El sistema de comunicación está basado en el servicio Intranet IPSec, que permite obtener un entorno de comunicaciones cómodo, muy potente y altamente fiable.

Las principales ventajas que se obtienen con esta solución son:

- Racionalizar las inversiones y costes de mantenimiento en comparación con las alternativas disponibles hasta la fecha.
- Infraestructura muy sencilla
- Direccionamiento IP del servicio adaptado al plan actual del que dispone NORTEGAS.
- Seguridad en la comunicación como consecuencia de:
  a) Autenticación a nivel de usuario.
  b) Autenticación a nivel de tarjeta SIM.
  c) Utilización del protocolo IPSec

Para que el acceso seguro sea posible, NORTEGAS dispone de un equipo terminador de túneles IPSec con salida a Internet. Contra este equipo se establecerá el túnel que comunicará a NORTEGAS con la infraestructura del operador GSM/GPRS.

El servicio Intranet IPSec está diseñado para adaptarse a todo tipo de servicios o aplicaciones basadas en el protocolo IP a las que se quiera dar acceso. NORTEGAS podrá elegir cuantos perfiles diferentes necesite. Estos perfiles podrán tener pooles de direcciones IP distintos, posibilitando un tratamiento diferenciado a nivel de Terminal/servicio.

1.3. ACCESO GPRS

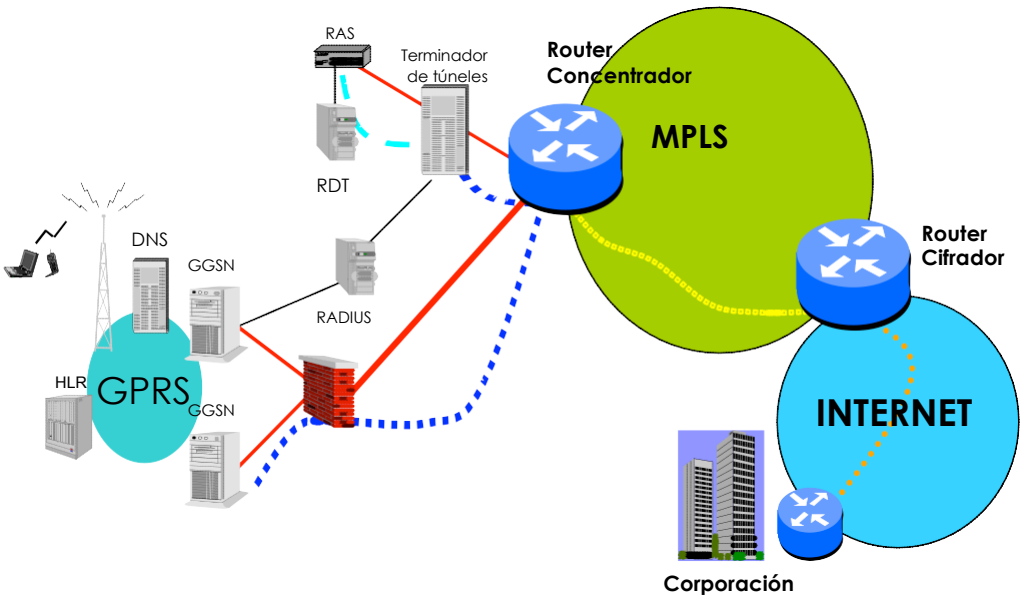
El servicio ofrece la posibilidad de que un Terminal previamente dado de alta pueda acceder a la Intranet de NORTEGAS utilizando como medio de acceso la tecnología GPRS.

La elección de direcciones IP que les serán asignados a los Terminales corresponderá a NORTEGAS.

Las principales características del acceso GPRS son las siguientes:

- El acceso GPRS es mediante conmutación de paquetes y el acceso a la corporación se hace a través del GGSN que es el nodo de la red GPRS que hace de router.
- En GPRS no se hace una llamada de datos sino que se establece una sesión “contexto PDP”

La arquitectura posible de red, para el acceso GPRS, sería la siguiente:



Sobre la arquitectura considerada mas arriba podemos identificar como se lleva acabo una conexión extremo a extremo. Cuando el terminal móvil inicia el contexto GPRS, la red consulta al HLR sí el teléfono llamante tiene permiso para activar un contexto con el APN de NORTEGAS. Si el número no está suscrito en dicho APN, la red no progresa la petición.

Una vez comprobada la subscripción en el HLR la petición le llega al GGSN que da servicio a NORTEGAS el cual lanza una petición de autenticación al servidor RADIUS de red. El servidor RADIUS comprobará que la terna (número llamante, usuario@nemonico, password) es correcta. En caso afirmativo asignará al Terminal la dirección IP estática asociada con dicha terna(número llamante,usuario@nemonico,password) dentro del rango de IPs asignadas a la intranet de NORTEGAS.

Una vez que el Terminal dispone de la dirección IP, el GGSN encapsulará todo el tráfico de dicho usuario por el túnel GRE asociado (túnel exclusivo para evitar cualquier intrusión no deseada). El túnel finaliza en el router de entrada a la red MPLS, el cual es el encargado de enrutar el tráfico hacia el router cifrador quien encamina el tráfico de usuario hacia el túnel IPSec correspondiente a NORTEGAS.
De esta manera y a todos los efectos, el tráfico generado por el Terminal llega a la corporación sin ninguna alteración, permitiendo así el uso de cualquier servicio, protocolo o aplicación que funcione sobre una conexión IP.

1.4. AUTENTICACION DE TERMINALES

La autentificación de usuarios/terminales se realiza con el sistema –nombre de usuario y clave- además de hacerlo a nivel de número llamante, es decir, para que un usuario/terminal sea autenticado correctamente debe conocer sus parámetros de conexión y, además, estos deben estar asociados de manera unívoca a la línea que está utilizando para la conexión(tarjeta SIM). Cualquier intento de conexión desde otra línea con esos mismos parámetros de conexión no será procesado con éxito y la llamada no podrá progresar.

Con este nuevo nivel de seguridad, para apropiarse indebidamente de una conexión no bastará sólo con conocer un nombre de usuario y la clave asociada al mismo, sino que además sería necesario hacerse con la tarjeta SIM a la que está asociado el número de teléfono móvil casado con dichos valores.

Para efectuar la autenticación de usuarios se dispone de un Radius que se configurará como servidor y que se encargará de analizar las peticiones de acceso por parte de los distintos usuarios.

Una vez autenticado el usuario/terminal, la conexión será efectiva entre éstos y la máquina remota pudiendo cursarse tráfico bidireccional entre ambos.

2. COMUNICACIÓN SMS

El Terminal puede comunicar con el servidor de telecontrol mediante intercambio de mensajes SMS.
El texto SMS del mensaje enviado por el TRT deberá tener el formato siguiente:

Va:12345678<return>	(8 caracteres con el totalizador de volumen bruto, m3)
Vr:12345678<return>	(8 caracteres con el totalizador de volumen corregido, Nm3)
P1.008<return>	(Valor de la presión en bares, con tres decimales)
T-13.78<return>	(Valor de temperatura, en ºC , con dos cifras y 2 decimales)
@<return>	(Indica la existencia de un error en el corrector)

El mensaje se enviará como mínimo una vez al día, con los valores de los totalizadores a las 24:00 h. del día anterior.

3. COMUNICACIÓN GPRS

Es posible realizar la comunicación vía GPRS. Para ello el Terminal realiza una conexión TCP/IP al FRONTEND. Para ello el Terminal se debe haber autenticado como se explica en el apartado1.4, por lo que el FRONTEND identificará al Terminal remoto por su dirección IP y si es válida aceptará la conexión.
La trama utilizada sobre dicha conexión TCP/IP será la misma utilizada sobre SMS.