Es innegable la penetración de las tecnologías GPRS en la transmisión de señales de alarma de sitios fijos y móviles, agregando en estos últimos años los servicios de posicionamiento. Alcanzada una masa crítica interesante llega el momento de evaluar la calidad de este sistema.

¿Hay congestión en las redes GPRS?

Lic. Néstor Gluj
Gerente de Negocios Latam
NanocommS.A.

En principio, debemos recodar que el GPRS es un servicio de la red celular GSM y su siglas en inglés significan General Packet Radio Service o, en español, Servicio General de (envío de) Paquetes vía Radio. Esta tecnología de comunicación se utiliza para la transmisión de paquetes de datos IP sobre teléfonos o módulos celulares y, en lo referente a la industria de la seguridad electrónica en Argentina, se aplica, aproximadamente, desde 2005/'06.

Su ventaja principal es el bajo costo de comunicación por evento, lo que permite un test de vínculo con frecuencias del orden de los minutos y comunicación bidireccional con los equipos, que posibilitan servicios de valor agregado, con funciones que exceden la comunicación de alarmas, ampliando las posibilidades de negocio.

Se aprovecha, además, el hecho de poder traficar sobre la red celular de los carriers que invierten millones de dólares para implementar y sostener su adecuado funcionamiento, recursos impensables en redes de radio para alarmas disponibles o implementables por otros prestadores de seguridad electrónica.

Ahora bien, ¿las redes celulares de los carriers se comportan bien a medida que el uso del canal de datos es cada vez más requerido? ¿Se puede asegurar el nivel de calidad que requieren los prestadores de monitoreo de alarmas y de Rastreadores GPS de vehículos y personas?

Ambas son muy buenas preguntas y la respuesta, en los dos casos, es: por supuesto que sí: con la implementación de APNs Privadas, la calidad y la estabilidad se mantienen perfectamente.

La clave es profundizar un poco y elegir bien la red, pues a simple vista el aumento del tráfico de los usuarios con teléfonos inteligentes (smart-phones) en las redes de celulares parecería generar un "cuello de botella" que podría hacer que las conexiones de datos se ralenticen.

Si bien lo dicho no es realmente así, el incremento en las ventas mundiales de teléfonos inteligentes y tabletas electrónicas tenía que tener su contracara: el crecimiento del volumen de datos hace que la banda ancha (APN pública) sea cada vez más "angosta".

En Argentina, el 14% de los celulares en uso son teléfonos inteligentes, categoría que registró un incremento del 225% en los últimos 12 meses. Más aún, se habla que dentro del próximo año más del 50% de los dispositivos vendidos en el mundo serán smart-phones y tablets.

Afortunadamente, las horas pico de uso de los smart-phones no coinciden con las horas de la noche y madrugada de mayor actividad delictiva.

Además, y aquí está la clave, la mayoría de estos equipos, salvo los Blackberry, trafican sobre las llamadas APNs públicas de los Carriers y es allí donde se puede generar la congestión, en especial en las horas de mayor tráfico.

En palabras sencillas, el reporte o paquete de datos recorre varios tramos en su camino de ida y vuelta entre el panel de alarmas y el Centro de Monitoreo:

- Tramo 1: de Aire desde el comunicador GPRS a la antena más cercana.
- Tramo 2: Dentro de la infraestructura del Carrier.
- Tramo 3: Puerta de Salida / Entrada del Carrier a Internet (proxies).
- Tramo 4: Internet desde el carrier hasta el Centro de Monitoreo (vínculos contratados por el Prestador de Monitoreo)
- Tramo 5: Infraestructura del Prestador de Monitoreo.
- Tramo 6: Software de Monitoreo (procesamiento de las comunicaciones y Gestión de Operadores). *(Ver gráfico 1)*

El problema

En contra de la creencia popular, los problemas de congestión no están solo en el tramo de aire, sino que también se presentan en la Salida / Entrada del Carrier a Internet, puerta por la que pasan todos los paquetes mencionados (Twitter, Facebook, MSN, etc.).

Todo este tráfico citado usa la APN pública y en una analogía, lo podemos pensar como el tráfico de vehículos de los seis carriles de la autopista Panamericana en su salida de la Cuidad de Buenos Aires un viernes a las 18 horas. La Panamericana está "muy cargada" pero "anda". Sin embargo, con cualquier roce, la autopista se atasca y se hace más lenta.

Para estos casos, los smart-phones poseen recursos tendientes a que el usuario no note las demoras o delays (retardos), pues los paquetes no se pierden. Sin embargo, estos retardos ponen a los comunicadores de alarmas realmente en problemas, pues hay tiempos que cumplir para mantener la sincronización entre el

Gráfico 1

Continúa en página 136

panel de alarmas y el sistema GPRS. Y si la red GPRS se pone lenta…

La solución

La solución es la implementación de APNs privadas con VPN, exclusivas para el tráfico de los paquetes de los comunicadores de alarma y rastreadores.

Consisten en un carril exclusivo que comienza desde el tramo de aire y sale directo al data center, donde se ubica el sistema de recepción *(Ver gráfico 2)*.

En otras palabras, es como disponer de un carril exclusivo entre la Panamericana y la colectora (APN Privada) por el que solo viajan los paquetes de los comunicadores, los que también tienen rampas de entrada y salida exclusivas, evitando los embotellamientos en esas partes.

Para implementar este tipo de APN se requieren recursos especiales, ya sea desde ciertos volúmenes comprometidos con los carriers, como routers y recursos humanos con conocimientos y certificados de tecnología informática, no siempre disponibles en relación al negocio del Monitoreo.

De allí que Nanocomm, sobre la base de entregar mejores productos, herramientas y servicios, implementó APNs privadas con los principales Carriers de nuestro mercado (nancocomm.claro.com.ar, nanocomm.movistar) proveyendo a sus clientes de una solución de extremo a extremo de calidad superior: Equipos + Comunicación (SIM Card GPRS APN Privada exclusiva) + Valor Agregado.

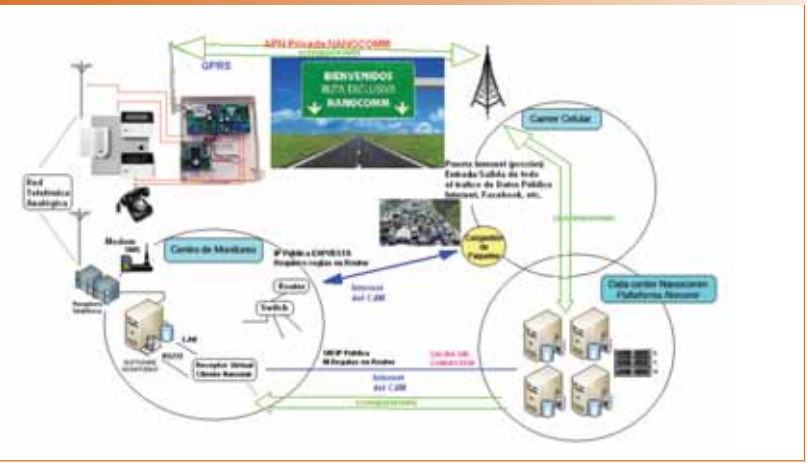
Si a lo dicho se agrega contingencia SMS/SMPP opcional, se dispondrá de un segundo vínculo inalámbrico a través de mensajes de texto inteligentes, pero con gran capacidad de tráfico, dado por el SMPP, sistema que usan los programas de entretenimientos y demás para traficar miles de mensajes por hora, algo que sería impensable en aplicaciones de módem.

Las APNs privadas con VPN y el SMPP brindan seguridad adicional, generando un túnel virtual para los paquetes, de extremo a extremo, evitando uso indebido y tráfico extra, pues las SIM Card se usan exclusivas en las APNs privadas.

Además, se pueden solicitar servicios con SIM de IP fija, que permiten la bidireccionalidad necesaria para sistemas de valor agregado, como por ejemplo la programación remota de paneles de alarma, teclado virtual y posicionamiento.

Lo expuesto en este artículo, posibilita tanto a los prestadores de monitoreo como al integrador tecnológico, comercializar los comunicadores como herramientas que brindan más seguridad y también acceso remoto, facilitando y potenciando sus negocios ■

Gráfico 2



Definición de APN y VPN

APN o *Access Point Name* es el nombre de un punto de acceso para GPRS que debe configurarse en el teléfono móvil para que pueda acceder a Internet.

Un punto de acceso es :

- Una dirección IP a la cual un móvil se puede conectar
- Un punto de configuración que es usado para esa conexión
- Una opción particular que se configura en un teléfono móvil

Los APN pueden ser variados. Son usados en redes tanto públicas como privadas.

Una red privada virtual, *RPV*, o *VPN* de las siglas en inglés de *Virtual Private Network*, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Algunas de las ventajas que ofrecen las VPN son las siguientes:

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

Existen, básicamente, tres tipos de arquietecturas para las conexiones VPN: de acceso remoto, punto a punto (que incluye la técnica de *tunneling*) y VPN over LAN.