

## **MONITOREO IP**

Anexando nueva tecnologías y servicios a su empresa

### **NOTA 1**

Es importante lograr una diferenciación adecuada de lo que el mercado nos ofrece , para luego si debatir cada uno de estos sistemas y equipos en forma minuciosa y detallada.

### **CONCEPTOS SOBRE LOS SISTEMAS EN LOS 90**

Durante muchos años hemos aceptado el vínculo telefónico analógico como la forma más sencilla y plural de monitorear alarmas a distancia. Hacia fines de los 90 , esta forma de comunicación de alarmas alcanzó el 95 % del mercado de monitoreo , como vínculo primario, quedando el 5 % restante conformado por el monitoreo radial VHF o UHF y el monitoreo por telefonía celular.

Estos sistemas alternativos , radio y celular , fueron utilizados en general como vínculos de respaldo (Backup) por su mayor seguridad en la comunicación pero al mismo tiempo con la contra de ser más costosos al minuto de usarlos.

La comunicación en si misma se ha desarrollado bajo la topología de la conmutación de circuitos , uniendo origen y destino de la llamada (en este caso panel de alarma y receptor de monitoreo) en una comunicación punto a punto de audio bidireccional. Sobre ese canal de audio , se trafican los pulsos (3+1, 4+2, otros) , los tonos multifrecuentes (DTMF) típicos del Contact Id o las tramas de módem FSK típicas de los formatos SIA , MODEM IIe y otros

### **LA CONMUTACION DE PAQUETES**

A partir del 2004 , la inserción de la red Internet como un nuevo paradigma de comunicación nos lleva a cambiar la forma de interpretar estos enlaces , olvidando la conexión virtual de audio entre origen y destino y pasando a utilizar paquetes digitales de información que se rutean a través de una red global compartida, como puede ser la Internet. Surge así la modalidad de monitoreo por TCP-IP , como homónimo genérico para la comunicación de alarmas por redes digitales de paquetes. TCP-IP es un protocolo multicapa de comunicación , que se ha masificado en la internet actual aunque no es el único puesto que muchos otros protocolos conviven en la red ( UDP , Token Ring , HLDC) sin nosotros preocuparnos al respecto.

### **ESPECIFICANDO UN POCO MAS**

Ahora bien, ya sabemos que vamos a transmitir paquetes de alarma por una red y estos paquetes llegarán al destino (Estación central de Monitoreo) sin que debamos preocuparnos como. Pero si nos preocupan cosas como la demora , el costo por uso y el costo por equipos.

Analizemos este caso :

El sitio protegido tiene un panel de alarma comunicado por vía telefónica. Con este sistema se estilaban usar chequeos periódicos en frecuencias de 1 a 4 por día , para mantener bajo consumo de pulsos telefónicos y de ocupación de la línea. El cliente requiere un control más frecuente para lograr mayor seguridad antisabotaje. Si ese cliente dispone de conexión a Internet de 24 horas (ver luego aclaración BANDA ANCHA \*) , podemos interfasear su panel de

alarma con Internet y lograr chequeos a nivel de minutos , dandole mas seguridad y reabsorviendo el costo de pulsos por llamadas telefonicas ahora dentro del abono de internet 24 hs. Ademas en este esquema se abandonan los costos de llamadas telefonicas de larga distancia pasando a una tarifa plana por servicio consumido.

(\*) Aclaracion : Banda Ancha : Es importante discernir entre requerimiento de Internet banda ancha y de Internet 24 horas. El tamaño de un paquete de datos de alarma es infimo (menos de 80 bytes) por lo que no se requieren grandes anchos de banda para transmitirlos (un enlace de 64Kbps podria ser totalmente sobredimensionado). Lo que si es requerido es que el evento cuando se produce , se transmita sin demora y por ello es requerida la conexion Internet 24 hs. En Latinoamerica estos conceptos se han mezclado y se maneja el termino banda ancha como un sinonimo de ambas funcionalidades, pero sepa que el monitoreo de señales solo requiere Internet 24 hs. El ancho de banda no es critico.

Tomada la decision de comunicar al cliente via Internet por red , los caminos son :

- 1) Cambiar panel de alarma del cliente por uno con salida a Internet o colocar una interfase Internet al panel actual
- 2) Verificar que el cliente disponga de un acceso a su Router (MODEM ruteador de internet) mediante el cual el servicio de internet del sitio se comparte entre PCs , DVRs , alarma y otros
- 3) Verificar que ese Router si contiene un Firewall disponga que los ports de Internet que la alarma usa esten abiertos para el modo requerido (TCP , UDP o ambos)
- 4) Verificar la alimentacion ININTERRUMPIDA del router y de todo equipo relativo a que el servicio de internet interno al sitio no caiga por fallas de suministro electrico
- 5) Setear el software en la estacion central y activar la cuenta de recepcion

## **ESCENARIOS FAVORABLES Y DESFAVORABLES PARA ESTA MODALIDAD**

### **FAVORABLES**

- a) El monitoreo TCP-IP por red es sin duda en el que mejor se aprovechan los costos porque el costo de internet ya se pagaba habitualmente en el sitio protegido y el uso del mismo por la alarma , no devenga nuevos consumos.
- b) No hay costos de larga distancia sino tarifas planas
- c) La integracion de imagen y audio es sencilla y se puede mejorar el servicio prestado muy simplemente
- d) Se chequea periodicamente el sistema a nivel de minutos
- e) Si se utilizo un panel de alarma con interase IP integrada , se podra hacer up y downloading al panel por la red internet obviando el acceso telefonico ( no mas rings de telefono en el sitio protegido)

### **DESFAVORABLES**



- a) Muchos sitios protegidos reciben Internet por las lineas telefonicas , en modalidad ADSL El corte de la linea telefonica por tentativa de robo , dejare inactivo igualmente el enlace internet. Esto , si bien ocurrira tal cual descrito , generara una aviso de falla de supervision de enlace en la estacion central al minuto de producirse , permitiendo la reaccion preventiva.
- b) Internet de banda ancha no esta aun disponible en muchos lugares
- c) Las interfases de monitoreo IP son exageradamente costosas por ahora (paciencia , todo cambia !!)

Por la compatibilizacion de monitoreo IP con su estacion central de alarmas , DESPREOCUPESE !

**Usted dispone de SoftGuard para que se encargue del asunto**

## **NOTA 2**

En la nota anterior iniciamos la recorrida por los sistemas de monitoreo IP , especificando inicialmente los de monitoreo IP por red fija.  
Es momento entonces de ahondar en el conocimiento de como funcionan y en base a ello perfilar el futuro inmediato de aplicacion de estos sistemas en nuestro negocio.

## **DIRECCION IP Y DIRECCIONAMIENTO**

*Necesito una IP Fija ? (La pregunta del millon de dolares)*

Para responderla , vamos a trabajar juntos el concepto y sus implicancias asi como trazar analogias directas al sistema telefonico para su facil comprension

En una red digital de paquetes los datos viajan de un origen a un destino dentro de un formato encapsulado llamado DATA PACKET , para nosotros : "paquete"  
Estos suelen tener basicamente 3 bloques , encabezado , datos y cierre.  
El encabezado define quien recibe y quien envia ese paquete. Con solo ese dato , la red internet aporta la inteligencia de ruteo para que esos paquetes arriben a destino y solo en milisegundos.

Asi como en la red telefonica mundial cada persona o empresa tiene un numero telefonico fijo , al que siempre sabemos que podemos llamarle , en la red Internet cada sitio debe tener una direccion IP fija a la cual contactar para comunicarse.

Hoy dia se utiliza el direccionamiento IP version 4, que define a una IP como 4 numeros (segmentos) separados por puntos : nnn.nnn.nnn.nnn , donde cada segmento puede valer entre 1 y 255

Nos conectamos a internet a traves de prestadores del servicio (Internet Service Provider ISP en ingles), los cuales son habitualmente las mismas empresas telefonicas. Ellos se conectan a Internet por enlaces troncales y por ser proveedores del servicio disponen de tramas de segmentos IP.

Al conectarnos a Internet por estos prestadores , ellos nos asignan una direccion IP o mas para ingresar a la red y comunicarnos.  
Esa direccion IP puede ser fija(estatica) o variable(dinamica) dependiendo del servicio contratado a

ese prestador.

**IMPORTANTE :** Para usos de seguridad a distancia , la IP de recepcion de alarma o eventos **DEBE SER del tipo fija(estatica).**

*Imagine por un minuto como podria funcionar vuestro sistema de monitoreo telefonico si a diario la empresa de telefonía que les da el servicio , les cambiara el numero .....*

### **IP FIJA e IP DINAMICA**

Ejemplo : El prestador de internet xxxxxx de Mexico dispone del segmento 205.57.128.xxx para sus clientes. Eso significa que al conectarnos a internet a traves de el , nuestro sistema recibira una IP entre 200.57.128.001 y 200.57.128.255.

Si contratamos a este prestador que nos de una IP fija , la misma no cambiara nunca y podremos con total tranquilidad direccionar los paneles de alarma hacia esa IP destino.

Si en cambio , la IP es dinamica y cambia no existira tal posibilidad

El porque de las IP dinamicas encuentra su explicacion en que en el caso del ejemplo , el prestador puede tener mas de 255 usuario para ese rango de 255 IP siempre y cuando los 255 no intenten conectarse al mismo tiempo. Los criterios estadisticos asi lo confirman y por ende este prestador vende servicio a mas clientes que lo que su capacidad tecnica directa simultanea le permite.

### **APUNTAMIENTO**

El direccionamiento ( la capacidad de internet de dirigir paquetes a su destino ) puede ser expresado de 2 formas :

- 1) Por IP a una direccion nnn.nnn.nnn.nnn
- 2) Por URL a destinos xxxxxxxxxxxx.xxx

En este ultimo caso , las direcciones URL siempre apunta a una direccion IP.

Si Uds disponen de una IP Fija , pueden contratar un nombre de dominio URL con empresas u organismos de gestion de dominios y apuntarlos a esa IP

Ej : cnn.com apunta a 64.236.24.12

### **DNS DINAMICO**

**No dispone de IP Fija en su estacion central de alarmas ?**

**El consejo es : Olvide brindar servicios de seguridad por Internet sin ella.**

Si aun asi decide , brindarlos :

Existen empresas de internet que brindan servicio de DNS Dinamico como por ejemplo dyndns (<http://www.dyndns.com>).

En estos sitios usted puede registrar dominios virtuales del tipo miempresa.dyndns.org y este servicio (basico) suele ser sin costo

En su estacion central de alarmas , se conectara a internet via su proveedor actual quien le entrega una IP dinamica (cambia periodicamente).

El ruteador (router) debe disponer capacidad de DNS dinamico. Si la tiene , el mismo se encargara



---

de notificar cada n minutos a DynDNS sobre la direccion IP actualizada , de forma que todos los paquetes que lleguen a DynDNS via miempresa.dyndns.org , seran ruteados a su Estacion central de Alarmas en su IP dinamica actual.

Este sistema en teoria es simple y efectivo , pero en la realidad tiene los siguientes problemas :

- 1) Los servidores DNS Dinamico pueden caerse a menudo y si los usamos gratis (Free) no hay reclamo.
- 2) Incluso pagando servicio pueden caerse y en esa ocasion no recibiremos alarmas del 100% de nuestros clientes.
- 3) Los apuntamientos por DNS Dinamico insumen mas tiempo en el envio de paquetes
- 4) Los servidores DNS Dinamico tienen delays (demoras) en actualizar las IP reales de los clientes conectados que pueden llegar a minutos (> 5) y esto nos deja incomunicados por ese plazo

**Conclusion : Vender SEGURIDAD no admite este margen de dudas**

### **NOTA 3**

En la nota anterior dilucidamos todos los temas de direccionamiento Ip.  
Ahora veremos como se procesan los eventos y como se comunican via TCP-IP

### **CAPTURA DE EVENTOS**

Las funciones de un comunicador telefonico de eventos estan integradas al 100 % en los paneles de alarma de hoy dia. El microprocesador del panel , entre sus rutinas de trabajo , verifica las entradas de sensores , comanda el teclado , opera las salidas y se comunica hacia el exterior via la linea telefonica

La programacion de estos paneles modernos incluye multiples pasos y selecciones que hacen a como el comunicador digital telefonico opera : formatos , codigos , handshake, etc.

Ningun panel actual de venta masiva y costo bajo del mercado incluye comunicador IP totalmente integrado a la programacion basica del panel.

Entonces , estamos necesariamente ante el escenario de generar una INTERFAZ.

De que formas podria un comunicador IP notificarse de los eventos que ocurren al panel de alarma y asi enviarlos por la red Internet al centro de monitoreo ?

- 1) Por conexiones fisicas a entradas de la interfaz
- 2) Por emulacion de la linea telefonica y captura
- 3) Por "pishing" del bus de comunicacion entre panel y teclado

Analizemos cada uno de estos casos y sus ventajas y desventajas

#### 1) **Por conexiones fisicas a entradas de la interfaz**

Este metodo utiliza la tecnica de conexion directa por cables entre el panel de alarma y la interfaz TCP-IP.

Esta ultima dispone de entradas (normalmente bornes a tornillo) que se programan para dispararse por estados alto o bajo de señal.

Suelen conectarse a puntos estrategicos del panel de alarma como el positivo de salida a sirena , los PGM o salidas programables de los paneles u otros.

Ventajas y desventajas

Garantizan universalidad de uso con cualquier panel aunque cada caso puntual sera diferente al anterior segun el panel y esto conlleva a adaptaciones permanentes y a la complejidad de uso.

Utilizandolo se monitorearan estados puntuales como ser ROBO (sin detalle de zonas), ACTIVACION o DESACTIVACION (sin detalle de que usuario) , FALLA ( sin indicar cual ) , etc.

#### 2) **Por emulacion de la linea telefonica y captura**

Este metodo utiliza la tecnica de conexion de la interfaz a la salida del panel hacia la linea telefonica.

El panel procesa una alarma que debe comunicar a la central y toma la linea telefonica tal cual fue programado para hacerlo. En lugar de recibir tono de discado real de la linea, recibe tono generado localmente por la interfaz TCP-IP. Sin reconocer la diferencia , disca el numero telefonico de la estacion central al que la interfaz IP hace caso omiso (serie de tonos DTMF o pulsos segun pais y ciudad).

Luego envia un evento de alarma en formato CONTACT ID por ejemplo (tonos DTMF) que son reconocidos y procesados por la interfaz IP , enviado via Internet a la central y recibidos los mismos correctamente , la misma interfaz genera saludo de despedida conocido como Kiss Off y el panel corta la llamada.

En este caso el panel nunca se dio por enterado que su evento se comunico por via distinta a la linea telefonica , pese a que el interfaz logro hacerlo.

Ventajas y desventajas

Suelen ser genericas y universales porque al aceptar formatos como CONTACT ID la mayoría de los paneles de alarma pueden dialogar con ellas.

Gracias a que procesan CONTACT ID , permiten reportar lo llamado FULL DATA TRANSFER (FDX) o sea eventos con informacion de zonas , usuarios y demas data

### 3) Por "pishing" del bus de comunicacion entre panel y teclado

La comunicacion digital entre el panel de alarma y sus teclados se realiza a traves del llamado Key BUS (KB). En los diferentes modelos y marcas se presenta en versiones de 1 o 2 hilos.

Esta comunicacion es del tipo PROPIETARIA es decir interna a la empresa fabricante y normalmente no es informada publicamente.

Lo bueno de "comprenderla" es que en ella se comunican el 100 % de los estados del sistema y toda la info esta alli disponible.

Obviamente el fabricante de cada panel tiene esa informacion por lo cual las interfaces IP que fabrican seran capaces de trabajar sobre sus KB sin problemas pero estas mismas interfases no serviran para otros paneles de otros fabricantes o a veces para otros modelos de la misma fabrica.

Algunas empresas que manufacturan interfases de radio o backup celulares en el mundo han estudiado y lanzado productos capaces de leer el KB de ciertas marcas pero es un trabajo muy tedioso y complejo que luego solo reditua para conectarse a esas marcas y modelos de paneles.

#### Ventajas y desventajas

Esta tecnica permite procesar Full Data Transfer de forma nativa. Es muy veloz y simple. Incluso permite que se puedan en forma inversa de comunicacion programar los paneles o controlarlos remotamente via Internet (up-downloading)

En contrasentido no son genericas ni universales y no fortalecen la idea de la universalizacion

Luego de este analisis , es probable que encuentren ustedes mas preguntas que respuestas en el haber.

Es cierto , pero al mismo tiempo no podemos permitirnos que nuestras empresas avancen hacia un futuro dictado por el destino , sin intervenir activamente en el mismo.

#### **Monitoreo IP no tiene estandares hoy dia.**

El paso del tiempo ira generandolos y nos iremos dando cuenta de ello.

Por el momento , sentido comun , evaluacion de costo-beneficio y CUIDADO !!!

Algunos consejos :

1) Si su empresa tiene un indice de diversificacion de paneles bajo , es decir que mas del 80 % de sus abonados han sido provistos como paneles de una marca o mejor una marca y un modelo x , puede ser util alinearse a comunicadores propietarios IP del tipo 3.

Si en cambio , usted recibe variedades amplias de paneles , busque un modelo de universalidad

2) Precios : Los costos actuales de las interfases IP limitan la aplicacion al 10 % superior de la cartera de abonados de cada empresa en terminos de poder adquisitivo.

Estos costos bajan a diario y son insostenibles.

La inmensa mayoria de empresas fabricantes electronicas tienen su alcance la fabricacion de interfases del tipo 1 y del tipo 2.

Esperen rebajas IMPORTANTES !!!!

#### **NOTA 4**

En la nota anterior revisamos las formas de captura de eventos.

Para terminar de abarcar el tema planteado de Monitoreo Ip , nos queda revisar las diferencias entre la comunicacion por red fija y por red celular (GPRS o CDMA)

#### **LOS VINCULOS DE COMUNICACION**

Mas alla de que como factor comun , todos los equipos estudiados operen en protocolo TCP-IP , modalidades TCP o UDP , existen diferentes tipos de redes y vinculos para lograr la comunicacion entre base y suscriptores :

1) Red Internet , acceso cableado o inalambrico

- Acceso por DSL o ADSL via linea telefonica
- Acceso por cable de video o cablemodem
- Acceso inalambrico por redes privadas
- Acceso Internet Wi-Fi o Wi-Max
- Otros accesos

2) Red Celular digital , modo GPRS

3) Red Celular digital , modo CDMA-1X

4) Redes satelitales

- BGan de Inmarsat
- Vsat
- Globalstar
- Otras

Del menu anterior , se desprende que hay opciones para todos los casos y siempre deberan evaluarse los siguientes factores :

- a) Disponibilidad del servicio en tiempo (caidas, up-time, inmunidad al clima)
- b) Conveniencia del servicio en costos (acorde a consumos medidos y usos)

En general de todos los mencionados , ha logrado un importante despegue el servicio por GPRS por lo cual vamos a comentar algunos detalles del mismo :

#### **QUE ES GPRS ?**

GPRS ( por General Packet Radio System ) es un protocolo de transmision de datos empaquetados entre equipos de telefonía celular y la red internet

La modalidad GSM de telefonía celular movil , la mas extendida del planeta , permite la operacion del sistema GPRS para transmision de datos entre moviles y puestos fijos



Para describirla rapidamente , todos los moviles tienen la habilidad de comunicarse en una intranet TCP-IP , a traves de las antenas celulares (nodos).

A traves de los Gateways que la compania prestadora celular dispone , los moviles pueden llegar con sus paquetes a la red internet publica y viceversa Estos gateways se denominan APN (Access Point Name) y a traves de ellos los paquetes de datos ingresan y egresan al sistema , desde la internet.

### **VENTAJAS DEL USO DEL GPRS EN RELACION A LA INTERNET POR RED FIJA**

- 1) La conexion a la red es inalambrica (celular) por lo cual no puede ser interrumpida por cortes de cables como el caso de la internet de banda ancha por linea telefonica o por cable de video
- 2) El costo de uso del GPRS , si bien medido , es muy economico y no representa un gran gasto desde el punto de vista que los paquetes de alarma son pequenos (poca cantidad de informacion)
- 3) El hecho de ser celular , permite que los puntos a monitorear esten en movimiento dentro de la red en el area de cobertura. Esto hace que el uso en localizacion y seguimiento de vehiculos o alarmas en ellos sea una aplicacion ideal del GPRS

### **DESVENTAJAS DEL USO DEL GPRS EN RELACION A LA RED FIJA**

- 1) El costo de los equipos para GPRS involucra transceptores celulares hibridos que elevan en U\$ 100 aproximadamente el costo de estos terminales sobre las soluciones que operan con red fija.
- 2) Las redes GPRS no son redes de banda ancha aunque sean vendidas como tales. Las velocidades netas de transferencia suelen ser muy bajas ( 40 Kbps) en relacion a la red internet fija.
- 3) Cuando se equipa un objetivo protegido con una interfaz de alarma para red internet fija , se suele aprovechar la conexion de banda ancha preexistente , licuando el costo de servicio involucrado, no asi en el caso del GPRS donde se incorpora una nueva factura de servicio , periodica y medida en consumo.

***Amigos , como en las 3 notas anteriores , la intencion ha sido esclarecer un poco mas dentro de lo posible una realidad que no es fija sino por el contrario , de un dinamismo tal que para cuando esta nota sea revisada en un par de meses , muchos de los conceptos vertidos resultaran obsoletos , por lo que el compromiso de nuestra parte y la peticion a ustedes los usuarios de soluciones SoftGuard , es la de enriquecer el debate y volcar su propio feedback para que toda la comunidad de usuarios , sea finalmente la favorecida.***

Cordiales saludos

**SOFTGUARD TECH CORP.**