

---

# **Medical Alarms and Next Generation Networks**

**September 2010**



**Phil Wait**

**Director**

**VC International Pty Ltd (VCI)**

VCI is a member of the Communications Alliance, (previously the ACIF), which is developing technical and equipment standards for the National Broadband Network

---

---

# 1 Background

Around the world, telecommunications networks are changing, from 'plain old telephone service' (POTS) networks that carry data as a secondary usage, to Internet Protocol (IP) data networks that carry voice as a secondary usage. The analogue 'public switched telephone network' (the PSTN) is undergoing fundamental change as it is modernised.

High speed broadband IP-based services employing digital subscriber line (DSL) technology are beginning to dominate the use of the copper line between customer premises and local exchanges, Asymmetric DSL (ADSL) currently being the most common. Over the past decade the advent of "voice over internet protocol" (VoIP) has added yet another dimension to telephone services and as DSL speeds improved many Internet players began offering video.

Next generation networks (NGNs) will maintain only a single network for voice, data and video, enabling carriers to maximize their service offerings and increase their revenue streams. Eventually, only a single IP data connection will be provided to private customers and all customer equipment will be IP/VoIP based.

Migration to all-IP networks has been underway for some time, with trunk (inter-exchange), corporate and government, and the public Optus HFC cable networks, already largely IP-based.

VoIP phones and "naked-DSL" services (lines without dial tone or analogue PSTN) continue to increase in popularity but up until recently, and in order to limit damage to it's existing revenue streams derived from POTS, the dominant Australian Telco with its own PSTN network has resisted the introduction of VoIP only phone services.

The National Broadband Network (the NBN) is a game-changing technology for Australian telecommunications, information and entertainment services. The NBN is to be a wholesale-only network providing a high-speed optical fibre connection to 93% of Australians, with the remaining 7% served by a lower speed wireless or satellite service.

Following the close outcome of the 2010 Federal election the NBN looks likely to be built with priority given to rural areas, and possibly with some modification along the way. If built as proposed, the NBN will effectively obsolete all other public telecommunications networks in Australia.

The move away from POTS to IP-based networks affects medical and security alarms, and both industries are introducing new hardware, data protocols, and the signaling formats to ensure a seamless migration through the various stages of network modernization.

This paper discusses the various network access technologies common in Australian homes, the introduction of the NBN (assuming it will be built largely as planned), and some of the key challenges likely to be encountered by medical and security alarm providers.

## 2 Accessing the Customer

### **What is an Access Technology?**

An 'access technology' is simply a method of connecting a customer to a network. Also called the 'last mile' connection, because it requires access into customer's premises, it is typically the most difficult and expensive part of any fixed-line network to install.

Whoever owns the 'last mile' access has a significant advantage in the marketplace, as others will need to buy wholesale access from those who own the access, typically an incumbent Telco.

Currently, the dominant access technology is the copper cable (or 'twisted pair') PSTN exchange line, which connects each customer to a local telephone exchange. Predominantly that access in Australia is owned by Telstra.

In the NBN model the fibre access technology is owned by NBN Co, who wholesale bandwidth to retail service providers (RSP's), who in turn sell their services to customers. A customer may then have multiple services from multiple RSP's, all buying customer access and bandwidth from NBN Co.

### **Local loop unbundling**

In the past there was only one network (the Telecom Australia owned Public Switched Telephone Network – the PSTN) and one access technology, (the copper cable or 'twisted pair').

The 1982 Davidson Enquiry recommended ending Telecom Australia's monopoly and by late 1999 Telstra was formed and fully privatized.

Although the Australian telecommunications market is open to competition, and many carriers and service providers compete vigorously for a customer's business, at this time Telstra still retains

ownership of critical network assets, including the 'last mile' customer access.

To pave the way for new competition in the telecommunications market, ACMA introduced a regulatory process called Local loop unbundling (LLU or LLUB). LLU allows multiple carriers to access a customers' exchange line for a 'reasonable' whole access fee paid to the owner of the line.

Although the ACCC forces Telstra to accept LLU and attempts to regulate the price Telstra charges its competitors for wholesale access to its network, naturally Telstra is not too happy about providing its assets (sometimes it is said at less than commercial rates) to a competitor who intends to take its customers.

In such an environment, it is not surprising that Telstra's competitors turned to other access technologies in order to connect the customer, and free themselves from having to rely on Telstra owned copper.

As a result, the Australian telecommunications landscape (pre NBN) currently contains several common customer access technologies. However, this is expected to radically change as the NBN is rolled out over the next 8 or so years.

## **3 Access Technologies**

### **Naked DSL**

Naked DSL services remove the PSTN exchange connection from the customer's 'local loop' telephone line, and only provide a DSL broadband internet service. A Voice-over-IP (VoIP) phone is connected to the customer's modem/router, and sometimes an Analogue Telephone Adaptor (ATA) is provided allowing connection of a standard telephone.

Telephone customers typically convert to this type of service to obtain lower call costs, but service quality can be inferior. Naked DSL services are offered by iPrimus, iinet, AAPT and others.

If an ATA is used for connection of a conventional alarm system the ATA and the end-to-end network must be configured to use the ITU-G.711 codec standard, in-band DTMF transmission. Extra battery back-up must be provided for the customer equipment modem, router and ATA etc.

However the reliability, battery back-up, and quality of service (QoS) issues are significant and for these reasons alarm communications over a naked-DSL service is problematic and potentially unreliable. VCI does not recommend connecting medical or security alarms to public naked-DSL telephone services.

Some alarm products are becoming available for connection to DSL or IP-only services, though at this time some QoS and battery back-up issues remain.

### **Hybrid Fibre Cable (HFC)**

HFC networks consist of a fibre back-bone distribution network with coaxial cable local distribution. A system of amplifiers and splitters reticulate the signal around a local area in a tree and branch structure.

The combination of fibre and a coaxial cable provides the bandwidth required for multi-channel video distribution (Foxtel etc.) and high speed broadband internet services.

The Optus HFC network also provides a high quality telephone service over the same cable which delivers its pay TV and broadband internet services. To avoid having to pay Telstra wholesale access fees for Optus telephone customers, the customer's home telephone line is disconnected from the incoming exchange line and connected instead to a "simulated PSTN" connection on the cable modem.

Recently Optus have been converting their telephone customers from an older analogue based system to a new VoIP based telephone system. During the course of this conversion some PRS and security alarms have failed to operate correctly due to an incompatibility between the alarm data and the cable modems. Problems can also occur during the installation procedure when the customer's internal telephone cable is cut from the PSTN line and connected over to the Optus cable modem.

Optus have tested a variety of PRS alarms and are advising customers when potential incompatibility exists. Optus expect to have this problem solved by mid 2011, and have also changed their installation procedures to improve the outcome when alarm equipment is present.

In fact, the Optus HFC network appears to be a very robust high quality-of-service network capable of transmitting the very short duration in-band DTMF data used by medical and security alarms without significant delay or distortion.

When correctly configured and tested, and when suitable battery back-up is installed, VCI believes the Optus network is suitable for use with medical alarms.

The Optus experience has been very interesting because, in many ways, it's a bellwether of the challenges facing medical and security alarms on the NBN.

## **FttN, FttH, and HFTP**

Generally, the longer the copper cable connecting the customer to the exchange (where the broadband signal is connected), the slower the maximum obtainable data speed to the customer. ADSL2+ is capable of very high speeds (up to 24Mbit/s downstream), but only up to about 1.5km from the exchange, after which the maximum speed falls off.

Fibre-to-the-Home (FttH), Fibre-to-the-Node (FttN), and Hybrid-Fibre-Twisted Pair (HFTP), deliver much higher broadband speeds (100Mbit/s or more) by bypassing the exchange and taking the super high speed optic-fibre cable deeper into the network, closer to the customer.

**FttH** offers the highest speed of all networks by taking the optic-fibre cable directly into customer's premises. As there is no other bridging technology which may reduce bandwidth, FttH has the highest speed potential. NBN Co. have suggested 1Gbit/s is possible to some customers.

An **FttN** network terminates the optic-fibre cable at some convenient point in the neighbourhood (the node), probably the cable pit or a cabinet in the street, or perhaps in the basement of an apartment block, and some other access technology is used to bridge the short distance from the 'node' to the customer. Because an FttN network can use the existing copper cable into the customer's premises it is often a very cost effective way to deliver very high speed services.

However, in an FttN system each service provider would probably be responsible for connecting 'their' customer to the 'node', and again to avoid paying whole access fees to the owner of the copper cable to the customer premises', a variety of alternative access technologies could be employed.

In such a scenario, alarm providers may need to have a 'basket' of different alarm technologies available depending on what was found at each customer's premises'. In cases where customers were 'converted' from one service provider to another the medical alarm equipment originally supplied may no longer work.

**HFTP**, is another name for FttN where the old 'twisted pair' copper telephone line from the customer is cut and terminated at the node, so the 'last mile' copper twisted pair connection becomes the 'last few hundred meters'. Again because the copper is a very short distance, much higher speeds are possible.

Although the NBN is to be a 93% FttH network, VCI expects that FttN or HFTP may form part where those techniques are more cost effective.

## 4 Customer Equipment

All these networks require some sort of customer equipment to be placed in the customer's premises.

In the case of the plain old telephone service (POTS) the customer equipment is simply the telephone.

Fibre, DSL, HFC cable Customer equipment consists of a modem/router which provides a number of Ethernet connections for connection to computers, entertainment systems and VoIP phones. The modem may also contain an internal Analogue Telephone Adaptor (ATA) with one or two 'simulated' PSTN connections for existing analogue telephone equipment (including alarm systems).

The NBN customer equipment will consist of an Optical Network Termination device (ONT) also called a Network Termination Unit (NTU),

but basically an optical modem, and a Routing Gateway (RG). End user devices will connect to either the ONT or the RG depending on their type.

### **Battery Back-up**

Unlike the PSTN, all customer equipment must be powered from the customers mains power supply. When critical services such as medical alarms are connected the customer equipment needs to be battery backed-up to allow operation during a power failure.

Australian Standard AS4607:1999 specifies a minimum battery back-up time of 36 hours for medical alarms during a power failure, a figure very unlikely to be achieved with customer premises modem equipment.

### **Modem Configuration**

Each type of modem (ADSL modem, cable modem, ONT/NTU etc) contains a configuration file which sets the correct operating parameters for the types of services provided, and for compatibility with the network. For typical alarm systems to work the configuration must be set to enable the highest packet priority (lowest delay), the ITU-G.711 codec standard, and in-band DTMF transmission.

A conflict may exist if a medical or security alarm is installed, or the services are changed. Configuration and re-configuration will require significant co-ordination between the alarm company and the retail service provider.

## 5 Wireless

Wireless systems provide alternative access to the customer and also provide mobility. PRS Alarm and Security providers are increasingly looking at wireless as a way to avoid the changes occurring in fixed-services.

Medical alarms are available with internal GSM wireless modem, or a Fixed Wireless Terminal can be connected external to the alarm.

However, as scarcity of available frequency spectrum limits the maximum number of wireless users, price is used as a tool for limiting spectrum usage. The supply of a wireless modem and the associated network access fees can be a very significant factor in the cost of a domestic PRS alarm system.

Additionally, the difficulty of insuring a sufficiently strong and reliable radio signal makes a wireless solution problematic in some situations. A Wireless installation must include a careful evaluation of signal strength and the equipment must not be moved from one location to another, even over very short distances, without further signal strength evaluation.

*(At 900MHz, a frequency band commonly used by mobile phones, a full wavelength is about 33cm and a half wavelength about 16cm. Reflections in the signal path can cause deep nulls and high peaks in received and transmitted signal strength over each half wavelength. In practice the situation is far more complex as multiple reflections commonly found in buildings tend to 'fill-in' the reflected peaks and nulls to some extent.*

*Diversity reception, where two antennas or receivers are placed a small distance apart is effective at overcoming the signal strength nulls caused by signal reflections. Other diversity techniques include 'polarization diversity' where one antenna is orientated vertically and the other horizontally and frequency diversity where a radio signal may be repeated on two frequencies which have a significant difference in wavelength so signal nulls do not occur in the same position. Diversity in the cell-*

*phone network is achieved to some extent by relying on multiple cell coverage and a hand-over from one cell to another when necessary.*

*Radio signal path-loss increases with frequency, and increases dramatically through buildings. The well known inverse-square-law for free-space electromagnetic attenuation becomes a much higher attenuation characteristic through buildings, depending on construction to the 3<sup>rd</sup>, 5<sup>th</sup> or even higher power, so a radio signal often falls off much faster through buildings than expected).*

### **Wireless Services and Medical Alarms**

Wireless can be highly reliable when a fixed location service is professionally installed in an area with consistently strong received signal strength, multiple cell coverage, and where the equipment is not moved.

However, in general, wireless services do not have reliability equal to the PSTN and medical alarm installers are typically not qualified or equipped to evaluate the reliability of a wireless system.

Therefore, VCI believes wireless alone is not a viable alternative to fixed line services for critical applications such as medical alarms.

### **Fixed Wireless Terminals**

When the provision or the repair of a fixed-line telephone service is not economical Telco's may use a Fixed Wireless Terminals (FWT), often mounted on the outside of a building. Fixed wireless terminals are basically a wireless module in a box with battery back-up. A 'simulated PSTN' connection on the FWT connects to the customer's telephone line in place of the normal exchange-line and a broadband internet connection, and often a FAX service is also provided.

In some cases the customer would not be aware of the change in service from fixed-line to a Fixed Wireless Terminal, as the work done is outside

the client's premises and fixed line call rates are applied to the wireless service.

Fixed Wireless Terminals are not compatible with most medical or security alarms and those alarms will stop working if the customer is converted to a Fixed Wireless Terminal.

## **6 The National Broadband Network**

In 2008, Telstra announced its intention to build a wholesale-only fibre-to-the-node (FttN/HFTP) network, providing VDSL (very high bit rate DSL) over its existing copper lines into customers' premises.

In April 2009 the Federal government announced plans to build a National Broadband Network (NBN) within 8 years (earlier in Tasmania) delivering very high speed access over an FttH network in high density areas, and by wireless and satellite in rural areas.

The NBN is currently rolling out in first-release sites in Tasmania and the mainland.

A range of service boundary points (physical interfaces) are planned throughout the network for the connection of wholesale service providers supplying content and services to customers.

Whatever its final form, because of the work done by the Communications Alliance in developing Standards and recommendations for the NBN, there will be commonality of Standards and requirements for equipment located in customer's premises', and a high quality of service (QoS) throughout the network.

## **Existing Medical Alarms over the NBN**

Following a public comment process, NBN Co. now proposes to ensure the continued operation of existing analogue equipment on the NBN, (including medical and security alarms), at least during a lengthy transitional stage.

It is proposed that an internal ATA in the ONT will provide one or two 'Simulated-PSTN' connections to existing customer premises wiring, including any analogue alarm equipment.

However several issues remain, such as the provision of a fail-safe battery backup, the monitoring of the back-up battery condition, the default configuration settings in the ONT, and the mechanics of customer migration.

## **7 IP and Alarms**

### **IP Connectivity**

The future is clearly digital and eventually all telecommunications equipment, including alarms, will be communicating over a very reliable high quality of service IP network. The NBN will eventually be an IP-only network carrying all forms of communications, information and entertainment to customers.

Although IP is currently more expensive to implement than PSTN, it does offer significant on-going cost savings on calls and very high data capacity, and new innovative services developed around IP-based solutions may ultimately lead to increased revenue streams for service providers.

The major obstacles to the early adoption of a full-IP solution for medical and security alarms are network quality of service (QoS) and network reliability:

*“The PSTN achieves five-nines [99.999%] reliability, equivalent to fewer than five minutes per year downtime, and it handles millions of simultaneous calls. A VoIP network needs to achieve similar levels of reliability and scalability”. (MULTISERVICE SWITCHING FORUM TECHNICAL REPORT, MSF-TR-ARCH-001-FINAL, “Next-Generation VoIP Network Architecture”, March 2003).*

Until the rollout of the NBN is complete and the time comes when IP connections (including all ancillary modems, routers etc) are as reliable as the current PSTN, (and suitably battery backed-up as required for PRS systems in Australian Standard AS4607), a redundant communications path over the PSTN, or at least the use of multi-path IP, will be essential for mission-critical applications.

Multi-path IP has been adopted by the security industry in an attempt to overcome the reliability issues associated with IP networks. If each IP path (network) does not share any common network infrastructure, so that an outage in one does not affect the other, reliability approaching that of a PSTN network is said to be achievable. Multi-path IP often includes a wireless path.

Some VoIP modems include a connection for a PSTN exchange line, enabling fall-back to PSTN when the IP connection is unavailable. The Belkin F1PI242ENau modem, for example, features fallback to PSTN and has two phone ports allowing for two phone services, or a phone service plus a fax service, all over a single internet account. Phone calls are automatically routed through the standard PSTN line if the IP connection is lost.

[http://catalog.belkin.com/IWCatProductPage.process?Product\\_Id=460610](http://catalog.belkin.com/IWCatProductPage.process?Product_Id=460610)

However, if a redundant path is required to overcome network reliability issues, and if data speed, capacity and call cost is not an issue, then why not just use the single most reliable path, which at this time remains PSTN?

An IP connection is currently really only an advantage if large amounts of data need to be transmitted (such as video or bio-medical data), or if call-cost is an important consideration such as if the alarm needs to be continuously monitored or generates a high call rate. In the cost sensitive medical alarm market, where the alarm is just used just to call for assistance and may be tested only once per week, an IP connection appears expensive and unnecessary if a PSTN connection exists.

In large residential aged care facilities all telecommunications and entertainment services are often supplied over an internal optic-fibre or cable distribution network, and the facility on-sells telecommunications and entertainment services to it's residents. Depending on their design, such private IP networks can provide sufficiently high QoS for a medical alarm application.

## 8 The Codec

To enable audio (voice, or analogue tones such as DTMF) to be carried over a data network, the audio must be converted to digital data at the sending end, and then converted back to analogue audio at the receiving end.

This conversion process is done by a device called a codec (**coder-decoder**) conforming to one of several International Telecommunication Union (ITU) standards. The coder takes 'samples' of the audio waveform at a high rate and converts these to a digital data stream for sending. Digital data

streams received by the decoder are reassembled in order, and then reconstructed into the original audio waveform.

Modern Codec's are increasingly implemented as software applications running on specialized microcomputers called digital signal processors, (DSP's).

The quality of the received audio depends on the speed at which the codec's at each end digitise and reconstruct the original analogue audio. Higher sampling speeds provide higher quality transmission, but generate the highest amount of data and require the greatest bandwidth and network resources (and, naturally, also the greatest network cost).

High quality telecommunications networks use ITU-G.711 codec's that digitise the audio into a 64kb/s data channel. This provides good phone quality audio and can also reproduce complex sounds, analogue modem tones, and FAX and DTMF tones.

In an attempt to save bandwidth and cost, highly voice-optimised codec standards were developed – such as ITU-G.723, ITU-G.729 and others. These codec's reduce the amount of bandwidth required by compressing (reducing sound level range) of the audio and by other techniques which highly optimise the coding-decoding process for voice. Very highly voice-optimised codec's are known as 'vocoders'.

The link between the customer premises and the exchange is called the 'last mile connection'. The amount of bandwidth available in the 'last mile' affects the choice of codec, the digitisation characteristics, and the degree of voice compression used.

Multi-standard codec's have been developed that can be reconfigured on-the-run by sending control commands to the network. These codec's can be switched to G.711 mode when a high quality codec is required for

transmitting high quality speech DTMF or data, and switched back to voice-optimised mode for speech.

The choice of codec standard is critical as it determines what, if anything other than voice, can be sent over a network. To make matters even more complex, when calls are routed between different networks, or between networks owned by different providers, often a conversion process occurs which links between different codec standards. Sometimes a first attempt is made using G.711 and if the network is busy (congested) a second attempt may be made using another lower data rate, higher compression standard.

It is therefore difficult to know the exact transmission characteristics of a particular telecommunications link. Wireless networks always use codec's with high levels of voice compression in order to make the most effective use of the limited radio frequency spectrum, and will continue to do so.

As the NBN has plenty of available bandwidth G.711 Codec standards (or equivalent) will be the standard configuration.

## **9 DTMF Data over IP**

PRS alarm diallers communicate with central receivers using a DTMF data standard developed many years ago for the security alarm industry. DTMF is transmitted as an analogue signal containing a mix of two, non-harmonically related, high and low frequency audio tones. The use of two simultaneous audio tones allows the receivers to distinguish between DTMF data and voice, avoiding false receiver activation on voice, or 'voice hits'. However, DTMF receivers are quite susceptible to distortion, background noise, and variation in level between the high and low group tones.

An IP network sends information in packets containing a few tens of bytes of data. The data packets propagate through the IP network from one end to the other in a random manner and, due to network delays (latency), are not necessarily received in the order they are sent. Depending on the path they take, transmission delay may vary between about 60 milliseconds (ms) and 300 ms, or more. The packets are reassembled at the receiving end in a device called a 'jitter filter', and output as much as possible in the order they are sent. Some packets may be received too late to be reassembled in correct order, and some may be lost altogether.

Although short delays and drop-outs are not too noticeable in voice communications, these issues become very important when transmitting time-critical data.

Additionally, in order to reduce the amount of network resource used, data is only sent when there is information to send. Voice activity is detected at the transmitting end by an 'activity detector'. However, as the activity detector takes a finite time to identify a valid signal, the leading edge of an audio signal being sent is often cut off. With voice, this is frequently noticeable as a chop to the first syllable; with DTMF, the effect is to shorten the transmitted DTMF pulse.

Alternatively and depending on the modem or network configuration, DTMF tones may not be sent as an 'in-band' digitized audio signal (in the voice channel), but rather as a series of 'out-of-band' network level commands to start and stop the play-out of DTMF digits at the receiving end.

Network level commands are sent through the network and the DTMF tones are regenerated from these commands in the receiving modem. The latency (transmission delay) in the network can vary significantly and will delay the initiation of the start and stop commands at the receiving modem. The effect of this is to significantly change the timing of the received DTMF tones at the alarm receiver.

DTMF tones sent as out-of-band commands over the 3G wireless network, as is the case when a 3G Fixed Wireless Terminal is used to replace or substitute a PSTN line, can be very significantly delayed and stretched to the point where all original data timing is lost.

Because DTMF is so entrenched in modern telecommunications systems future networks will need to handle DTMF within acceptable transmission delays. The NBN is expected to handle DTMF transmission well, but the configuration settings in the ONT may need to be changed for in-band transmission of DTMF when an alarm dialler is installed.

The “Network Working Group” is attempting to standardise the handling of signalling and DTMF tones on IP networks. The recommendations in their memos RFC2833 and RF4733 – *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, are now being adopted by network equipment suppliers. *Also see section on Quality of Service (QoS) below.*

## **10 Single Frequency Tones and FSK over IP**

Continuous single frequency tones, including FSK modem data and FAX tones, require the use of a ‘clear channel’ codec such as ITU-G.711. Voice-optimised codec’s do not transmit single tones well, causing severe level and phase distortion on the received audio.

Security and PRS alarms using the common security alarm communications standards use single frequency ‘request-to-send’ and ‘acknowledgement’ tones sent from the alarm receiver to the PRS dialler to initiate and acknowledge alarm data transmission. This technique may be incompatible with some VoIP networks and modems.

The NBN is expected to handle single-frequency tones and low-speed (<2400baud) FSK data.

## 11 Quality of Service (QoS)

*The following is largely taken from Communications Alliance Industry Guidelines G632:2007 and G634:2007*

Traditionally, the IP networks have been built to a principle that networks will operate on a “best efforts packet delivery, with no guarantees” basis.

Correcting for underlying network impairments requires extra time, and this principle suits applications that do not have particular time-sensitive requirements for packet delivery (on timescales smaller than a few seconds) such as bulk file transfer, electronic mail, and general web-browsing.

Increasingly, end-user applications that are more sensitive to network impairments and delays are being deployed, including VoIP, streaming audio and video, and distributed client/server databases. These applications work best across networks that can deliver “better than best-efforts” performance for various characteristics. To avoid client dissatisfaction with voice quality, VoIP will be allocated the highest QoS.

PRS and security alarms require a “low packet-loss” “better than best-efforts” network.

It is generally accepted that QoS enabled broadband is likely to be the dominant approach in the future. There are many applications and services that require similar network performance, so performance expectations are being developed for a small number of QoS ‘classes’, and methods are being developed to ‘mark’ packets to signal to a receiving network which IP Network QoS Class is expected to be applied to the packet as it travels through the network. That probably means switching in G.711 Codec’s end-to-end through the network and giving priority to those packets.

Security and PRS alarms that transmit short bursts of time sensitive DTMF data are very sensitive to both delay and packet-loss, however as

DTMF transmission from security and PRS alarms would be sent as a voice-band signal over the NBN, the packets would be allocated the best possible network performance.

## **12 Voice Quality over VoIP**

To extend the range of voice communications from the client to the alarm dialler, medical alarms typically use very sensitive microphones and high background noise levels are common. Highly voice-optimised codec's have difficulty processing non-voice audio sources, including constant background noise, (G.711 codec's will not suffer this problem).

In addition, as previously discussed, data is only sent when a person is actually talking and the switching delay in the VoIP activity detector may cut leading voice syllables, affecting intelligibility adversely. This shortcoming would become more noticeable at low voice levels, around the level of the background noise, and at the threshold of the activity detector.

As PRS clients needing help are often remote from the PRS dialler, and background noise in a client's home is common, voice quality over VoIP is often expected to be inferior to PSTN in a medical alarm application.

## **13 Calling Number Display**

Identification of the calling phone number, known as Caller-ID (CLI) or Calling Number Display (CND), could provide a future-proof way of identifying an alarm call from a fixed location alarm, and provide a back-up method to identify an alarm if data is lost or corrupted.

In Australia, private number CND is not available to organisations other than government-provided emergency services, (e.g. police/ fire/ ambulance). However PRS alarm diallers could be configured to send the

standard network activation code to allow CND only on calls from the medical alarm.

Although the Communications Alliance “Industry Code for Caller Number Display” (CLI/CND) ACIF C522:2007 is intended for service providers, VCI believes the principles could equally be applied to medical alarms:

*The customer must be informed about CND and the operation of the equipment in relation to CND, and*

*The customer must have the ability to override any function which enables CND either permanently or for each call.*

## 14 Conclusion

The NBN will provide a simulated PSTN connection which will support existing analogue telephones, and security and PRS alarms, at least during a long transitional period.

The Federal Government decision to build the NBN, and the work of the Communications Alliance, means there will be commonality of standards, access technologies and hardware, and high overall quality of service. Significant issues remain to do with battery back-up and battery monitoring, the configuration of customer equipment modems, and customer migration to new services.

The Optus HFC cable network also provides a ‘simulated-PSTN’ connection on the modem. The network has a high quality of service and early problems with medical and security alarms are being resolved.

Naked-DSL services are not yet suitable for the connection of a medical alarm. However the quality of service of IP networks is improving rapidly and their ability to send DTMF and single frequency tones, both required

for existing alarm equipment, is now very much better than it was just a few years ago.

Multipath-IP using wireless, as commonly used by the security industry, is not practical for cost-sensitive medical alarm applications due to cost.

Private IP networks found in some residential aged care facilities and mixed-age housing estates may be suitable for medical alarms, depending on their design and configuration.

In summary, VCI believes the PSTN interface remains the best connectivity option for medical alarms in the medium term as it's compatible with both existing PSTN lines and the proposed NBN.

However, all communications will eventually be IP based and the only connectivity option will probably be Ethernet. The medical alarm industry needs to plan for that eventuality.

## 15 Recommendations

In order to make PRS alarm communications over new networks as robust as possible, VCI recommends changing the timings and the format of the DTMF protocols, and making other changes which reduce the susceptibility of equipment to short tone drop-outs and tone artefacts generated by the network.

This changes are similar to those recently introduced in the UK to ensure alarm compatibility with the British Telecom (BT) 21CN upgrade program.

The suggested modifications are:

DTMF tones should be transmitted for 100ms and separated by a quiet period of 100ms. (The 100ms-on/100ms-off tone periods would increase call handling time by around 30%).

Alarm receivers will need to identify the format used and reconfigure receiving algorithms to suit.

Alarm receivers should ignore all tone dropouts less than 40ms duration.

Alarm receivers should ignore artifact tones, (short tones which are falsely generated within the network or the terminal equipment), less than 40ms in length.

Alarm diallers should ignore tone drop-outs less than 80ms in Ademco handshake and acknowledgement tones.

Calling Number Display could be used as a back-up for alarm unit identification.