

Emergency Call Handling in VoIP Networks



Simply Better Connected

Emergency Call Handling in VoIP Networks

Emergency Call Handling (ECH) is an essential feature of today's public telephone networks, and if Voice over IP based PSTN replacement is to become a reality, the new technology will have to deliver reliable handling of emergency calls. The needs of ECH have been extended as a result of recent national emergencies, such as floods and terrorist atrocities. These have focused Governments' attention on the need to secure the lines of communication for key workers and facilities, as well as support for emergency calls.

SIP is now the accepted technology for next generation IP based PSTN and mobile networks, underpinned by standards bodies such as ETSI TISPAN, PacketCable, 3GPP and 3GPP2.

There are two main issues relating to the implementation of ECH for VoIP:

- Locating the caller
- Managing emergency call traffic

Locating the Caller

One of the great advantages of a VoIP service is that it can be accessed from virtually anywhere; subscribers simply log on with their chosen device and their calls come to them. This potential for mobility is at the core of the problem of delivering accurate positional information to the Emergency Call Handling Centre.

Although each subscriber device may be allocated a unique IP address and port number, this, by itself, is not sufficient to physically locate a caller. IP addresses do not have the same geographic significance of fixed line telephones, nor are they supported by the purpose built network such as a mobile service provider's infrastructure.

So a new capability is required to enable emergency services to be sent to the right place. This does not just

apply to callers roaming within national boundaries, but perhaps on a global scale. Despite copious warnings that VoIP services should not be used to call 911 or 999, fatalities have occurred because the caller was actually in a different country to where the called ECH centre was located.

In the US the FCC has mandated that Interconnected VoIP providers must provide emergency operators with the call back number and location information of their customers where the emergency operator is capable of receiving it. The onus is on the customer to provide the location information, but the VoIP provider must provide the customer with a means of updating this information. This move offers the prospect of greater security for the subscriber, but for the most nomadic users, the overhead of constantly having to update location information will be an onerous task. In fact, some VoIP service providers require between 5 and 10 days notice to update the registered location of the service. Therefore, we need to supplement the manual updating of information with automatic device and network based solutions.

Due to the broad range of terminals that can support VoIP and equally broad range of technologies need to be employed to assist in providing location information. For limited types of terminals GPS may be the answer; however even this technology may only work in outdoor locations. New location technologies are being investigated such as using TV and radio station transmissions to triangulate the client device; however these techniques are currently only experimental and in any case may be of limited applicability. However, locating callers effectively with any degree of accuracy using the IP network itself will require a new level of openness on the part of service providers.

Many subscribers in a fixed network VoIP solution will use DSL technology. The best time to record the data for VoIP

users is when they get authenticated for IP services, typically with their ISP.

The subscriber uses a port on the DSL DSLAM to gain access. If the name of the DSLAM and the physical port number can be recorded, then by a series of database look-ups the location of the caller can be determined.

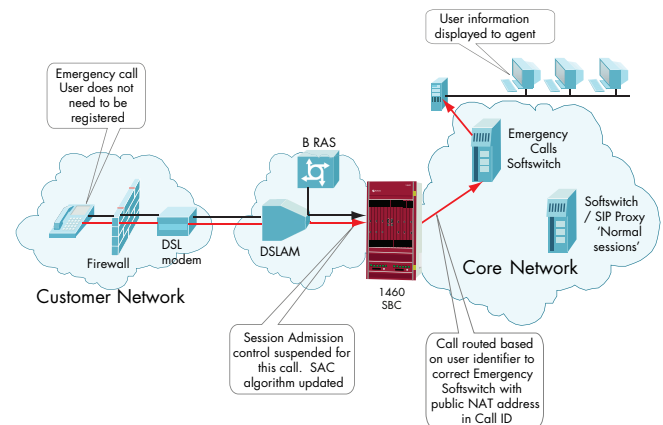
There are two potential mechanisms to allow the ISP to discover this information. When the DSLAM has IP connectivity then the "Option 82" in the DHCP exchange can be used to convey the information about DSLAM and the physical port being used to connect to the subscriber back to the ISP. The ISP would record this data in an "open" database so that the ECH service could determine caller location.

For ATM based DSLAMs, which have no real visibility of the IP world, another mechanism can be used, Extended Authentication Protocol (EAP). Here the DSLAM uses a Radius or Diameter interface to pre-authenticate the subscriber, and at this point the data can be captured.

The location information that this provides can be combined with subscriber registration records. This combination will allow the call handling centre to immediately distinguish a roaming call from one made from the registered location.

There are some developments from the IETF in the form of ECRIT - Emergency Context Resolution with Internet Technologies - which outlines various functional requirements, including identification of the emergency caller's location, the use of an emergency identifier to declare a call to be an emergency call, and the mapping function required to route the call to the appropriate Public Safety Answering Point (PSAP).

These mechanisms allow the indirect derivation of user location, but how would it be sent to the ECH centre? The call processing system would ideally append a cross reference in the SIP Invite message that establishes the call, perhaps in the *P-Network-Access-Info* field, already defined in the IMS specifications from 3GPP and ETSI.



Managing Emergency Call Traffic

The first requirement is to support emergency calls at all times, if necessary at the expense of other traffic. In the access layer this is relatively straight forward since there is a limited list of emergency call numbers, so with adequate traffic management capability, emergency calls will always get through. Access session border controllers are already used to enforce traffic policies and can identify ECH as a special case.

An additional challenge is the requirement to prioritise key worker and facility traffic below that of than emergency calls but higher than other calls.

When an emergency event occurs, people not only make emergency calls but also try to ring their friends and relations to assure them they are OK or to find out if they are affected. Of course, if the call does not get through, they repeatedly try again, amplifying the network congestion problem. Depending on the scale of the event, this traffic can be confined to localities or spread nationwide.

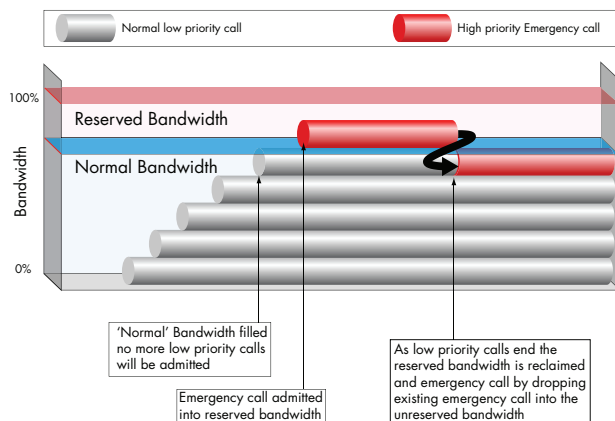
In the midst of this huge spike in traffic, key personnel will be trying to organise an effective response to the emergency. If their calls are not effectively prioritised then they will not get through. The new challenge is to allow this traffic to get through at the expense of none essential, personal calls.

The main SIP RFC 3261 does not support the required resource prioritization; however, there is a recent supplementary RFC

(RFC4412) designed to extend SIP's capability in respect to call prioritisation and the allocation of resources. This extension is intended to cover a number of service scenarios including the requirements of emergency call handling. The RFC defines new SIP header fields that allow a device to request that the call is treated by downstream elements as a high priority call. If this scheme is adopted it will allow elements such as SBC which are managing session admission to pass these calls in preference to others.

The problem is particularly acute at the network interconnect points, for example between a mobile and wireline service provider. The interconnect point will probably come under severe strain from personal callers. If the right priority marking is attached to the SIP messages, then an interconnect session border controller can readily deal with the traffic, rejecting lower priority calls and keeping essential calls flowing.

There are a number of schemes that can be used, but the key need is to allow the automatic prioritisation of traffic, and the appropriate selective rejection of new calls.



Newport Networks' 1460 SBC employs an advanced scheme where emergency calls are allocated an initial reserved capacity and the traffic management works to keep that reserved capacity clear for new emergency calls using a sliding window philosophy. For example, in

the figure above, five low priority calls are permitted and space is reserved for two new emergency calls. Once the limit of five low priority calls is reached, no further low priority calls are admitted. However, emergency calls are admitted into the reserved bandwidth. When a normal call ends, the system reclaims the reserved capacity for two new emergency calls. The system achieves this by reducing the normal call count when calls end. Thus, if the total capacity is seven and one emergency call is active, the system will limit normal calls to a maximum of four thereby preserving the new emergency call reserved bandwidth of two.

This concept can be extended to support a key personnel band, which is treated in a similar manner to emergency calls but at a lower priority. The aim of this method is to always ensure that resources exist for emergency calls and capacity is automatically allocated as the event unfolds, sometimes very rapidly and beyond the ability to control through a manual response by network operators.

Summary

Effective handling of emergency calls is vital for all VoIP networks. Identifying emergency calls, prioritising them and delivering them to the emergency operator is a key requirement. The protocols and procedures needed to enable this service exist and can be delivered today. Newport Networks 1460 session border controller supports prioritised delivery of emergency calls today and Newport is committed to supporting the emerging standards that enhance the effective delivery of emergency calls. ■