



1 Introduction

Voice over Internet Protocol (VoIP) technology enables telephone calls to be routed over data networks and this brings the following benefits:

- There are **reduced costs** associated with using a single network for data and voice communications. In addition, it is possible to bypass costly call tariffs and charges for enhanced features that are often levied by telephone operators.
- **Enhanced features** can be developed quickly and implemented immediately on a centralized server. Features such as video conferencing, mobility, file-sharing, enabled by the Session Initiation Protocol (SIP), are now accessible to all.

The Public Switched Telephony Network (PSTN) has, quite rightly, given us high expectations for availability of services and resilience of the network. In order to provide us with 'five nines' (99.999%) levels of availability, reliability of the network elements is rigorously specified; telephone exchanges are even designed to withstand earthquakes. Given these expectations, it is natural to be cautious about routing calls over a less-regulated data network.

The PSTN also offers sophisticated call handling capabilities for the emergency services. We expect to be able to pick up the phone, dial a 3-digit number and be connected, within seconds, to somebody that can help. Even callers that are unable to speak know that the operator will be able to pinpoint their location and send help on its way. Of equal importance is the ability of the operator to keep the call alive even when the caller hangs up. This can buy them vital time to locate the caller in order to send help or to deal with hoax calls. When migrating users of these networks to VoIP technology, we need to ensure that they continue to have reliable network access in the event of an emergency.

2 VoIP Gateways

One of the key obstacles to take-up of any new technology is the cost associated with taking a "rip and replace" approach – throwing out your existing equipment and replacing it. Not only is this costly, but it can also result in considerable disruption for the users of the service. Affordable gateways can ease the migration to VoIP by:

- Connecting existing telecommunications equipment to the Internet
- Converting speech into data packets
- Ensuring that quality of speech (QoS) is maintained by prioritizing voice traffic
- Interworking PSTN and VoIP protocols

At the far end, the call is either routed to an IP destination e.g., SIP phone, or is switched back to a traditional telephony network by means of another gateway.

Figure 1 shows a typical corporate network with segregated voice and data networks. In Figure 2, a gateway has been used to bridge the two networks at very little cost and with minimal network disruption. Calls to other sites are now routed across the internet, bypassing PSTN tolls. Crucially, emergency calls are able to break out locally, ensuring that they are routed to the closest emergency operator.

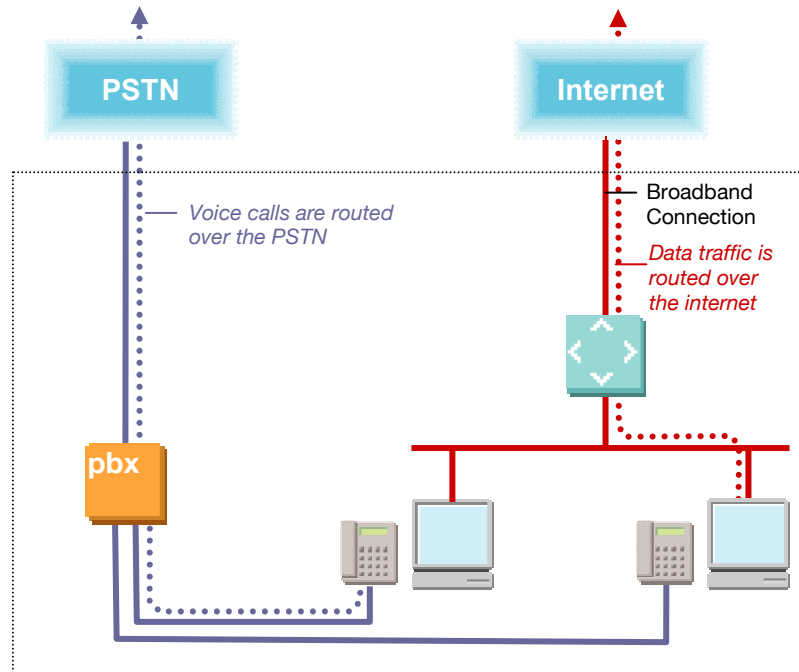


Figure 1 - Typical Corporate Network

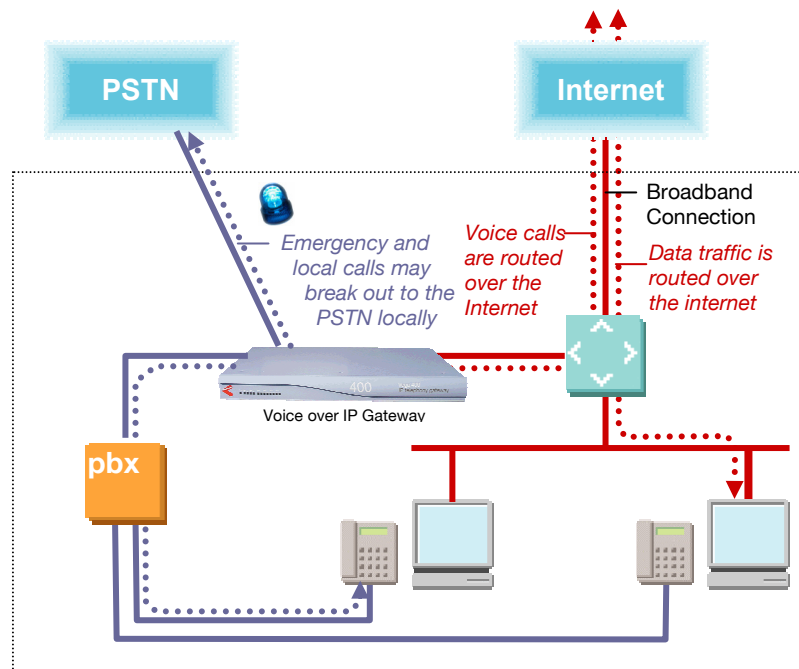


Figure 2 - VoIP-Enabled Corporate Network

3 Threats to the VoIP Network

Figure 1 shows a simple, SIP-based VoIP Network and the points at which disruption to services could occur.

The **SIP Proxy** sits at the heart of the VoIP network, registering and authenticating users, providing intermediary services for call set-up and offering enhanced features such as conferencing.

The **VoIP gateway** enables traditional telephony equipment to connect to a data network, such as the Internet, to route calls over that network. It can also provide access to the PSTN for calls that have originated on or been carried over the VoIP network.

Loss of either of these elements can cause severe disruption to voice services.

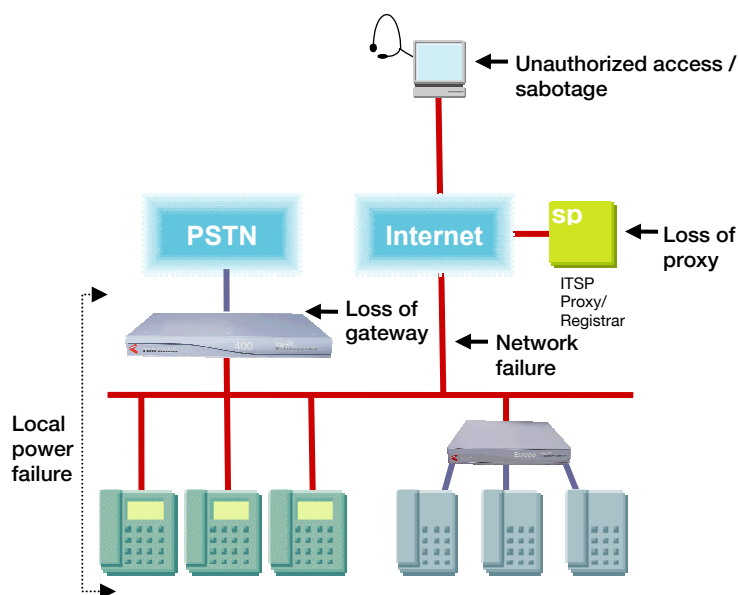


Figure 3: Threats to VoIP Telephony

Emergency Calls – VoIP to the Rescue?

Despite huge advances in VoIP quality and resiliency, there often remains one nagging doubt: whether VoIP networks can cope with life-or-death emergencies. There are two issues to be addressed here:

- the ability of VoIP users to call the emergency services:
 - the VoIP network needs to route the call (999/911/112) to the emergency operator
 - the caller should still be able to call for help when there is a power or network failure
- and that of the emergency services to respond:
 - The operator needs to be able to establish the precise location of the caller, even when that person cannot speak. Calls that break out onto the PSTN may do so at a location and with a CLI that bears no relation to the caller's physical location.
 - Organizations carrying out mission-critical activities often prefer to segregate voice and data on the basis that to lose one is an inconvenience but to lose both is a disaster.

Whilst these concerns are entirely understandable, they are not insurmountable and evidence suggests that VoIP offers callers additional options in the event of an emergency. The Internet Telephony Services Providers' Association (ITSPA) cites the London bombings of July 2005 as an example of how VoIP offered alternative access to callers when the mobile network was largely unavailable^[1].



Other factors that can affect availability include:

- **Power Failure:** Analog telephones that are connected to the PSTN are often powered from the local exchange. VoIP phones and gateways rely on local power and are, therefore, at risk when the supply fails as are any analog phones not connected directly to the PSTN.
- **Network Failure:** Data networks, with their distributed architecture are inherently resilient – if one path to your destination is unavailable, a myriad of alternative routes exists. However, no matter how resilient the data network is, if you lose your access to it, you will lose your voice services as well.
- **Human Factors:** Unfortunately, networks can be attacked by people who wish to gain some kind of financial advantage, have a grievance with the organization concerned and even those who are just looking for entertainment:
 - A **denial of service** (DoS) attack aims to render a resource unavailable to its users. It works by flooding a server with more requests than it can handle, meaning that during the attack period, the remote server will be dramatically slower or completely unavailable. Denial of service can be a particular problem for real-time services such as VoIP and it can render a telephony service completely unavailable.
 - If a network is not adequately secured, it could be vulnerable to **fraud**. By eavesdropping on the media and signaling paths, a fraudster could gain access to free calls and bank account details and could even spoof signaling messages to reroute a call to a premium rate number.
 - Even with the best of intentions, **humans** can make mistakes. A simple provisioning error could lead to disaster, if not detected and corrected.



4 The Solution

There are two key stages to protecting your VoIP network:

- Establish a **resilient network**
- **Handle failures** as they occur

Establish a Resilient Network

A key feature of VoIP telephony is that it relies on local power supplies. **Emergency power systems (EPS)** ensure that, if mains power supply is lost, essential services can still be operated. Uninterruptible power supplies (UPS) kick in the moment that power is lost and enable equipment to continue working normally. UPS systems usually utilize rechargeable batteries that are charged from the mains during normal operation. These may be backed up by an emergency generator for lengthier power outages. You may already have this technology installed for your data equipment.

Authentication of users and **encryption** of the data and media paths ensure that only authorized users gain access to VoIP services. Secure Real-time Transport Protocol (SRTP) provides encryption and authentication for the media packets, to prevent eavesdropping. To protect the signaling path, the IETF defines a secure mechanism for the delivery of SIP messages, called SIPS, which uses Transport Layer Security (TLS). Servers that are configured using Hypertext Transfer Protocol (HTTP) should support HTTPS – HTTP with security at the transport layer.

To prevent callers from placing unauthorized calls and, therefore, defrauding the bill-payer, steps should be taken to establish their identity at call setup time. These steps may include:

- Validation of the Calling Line Identity (CLI)
- Validation of the incoming gateway/physical interface
- Standard SIP authentication procedures at call setup, transfer and tear-down^[3]

To minimize the risk of human error being an issue, look for equipment manufacturers that can offer you:

- Intuitive, easy-to-configure equipment
- Comprehensive training

Failure Handling

Preserving Proxy Functionality

The distributed nature of data networks is, ordinarily, an advantage when it comes to resilience. However, if an organization's Internet connection is lost, this can lead to a complete loss of calls, if those calls are being controlled by an entity in the broadband network.

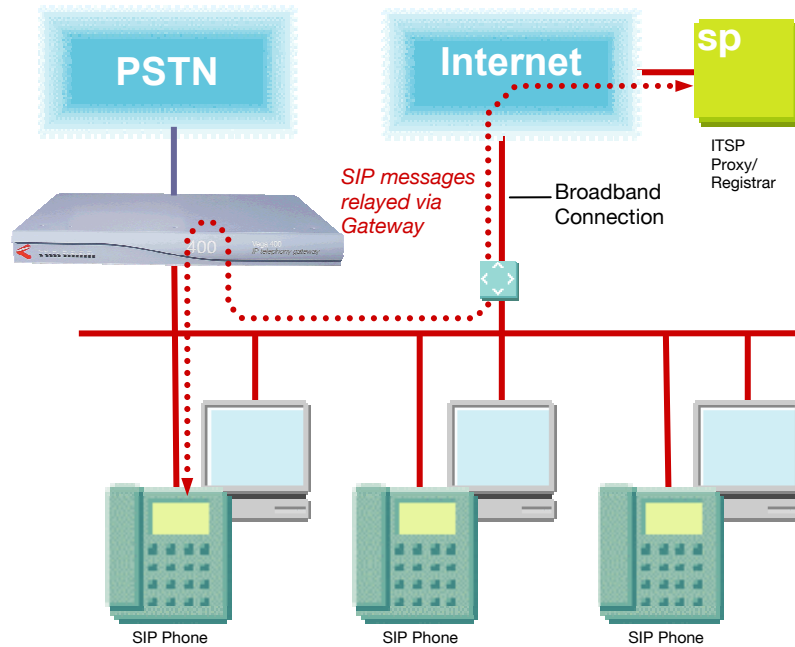


Figure 4: Resilience Proxy, Normal Operation

VegaStream gateways all support a feature called **Resilience Proxy**; the ability to relay and cache messages between an external proxy and a local data network and, if the connection to that proxy is lost, they can continue to route internal calls and calls to the PSTN, based on the cached information from the proxy.

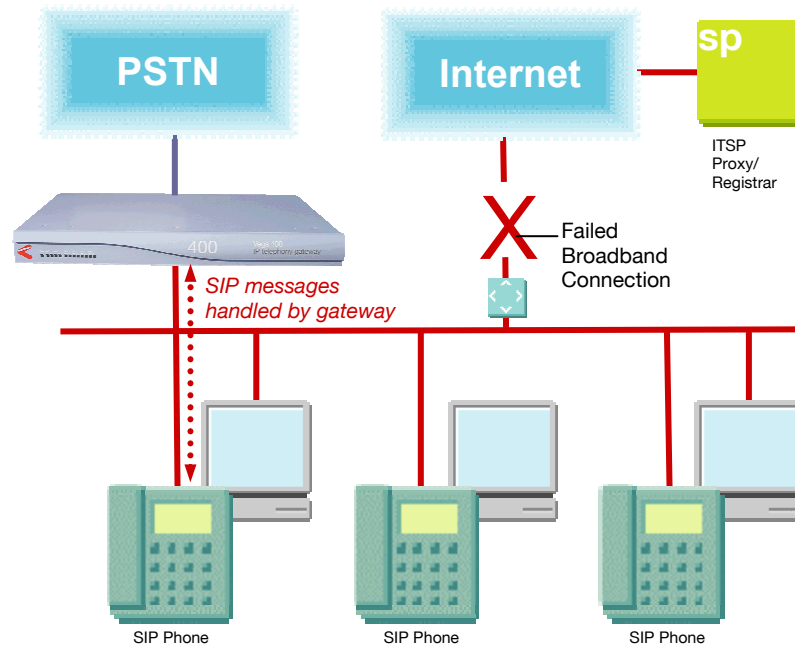


Figure 5: Resilience Proxy in Action

The Resilience Proxy feature maintains communications, even when access to the internet is unavailable. However, it cannot support all of the enhanced features that a SIP proxy enables. A resilient network will, therefore, have more than one proxy and there is more than one way to access alternative proxies:

- Multiple proxies can be defined within a **dial plan** or group of dial plans, to be used in the event that an error occurs.
- A list of **multiple static proxies** can be defined within the gateway and, if the gateway times out whilst waiting for a suitable response (often 'RINGING'), the next proxy on the list will be tried. A gateway operating in cyclic mode will use the next proxy on the list for each call, for load-balancing purposes.
- With **DNS SRV**, a Domain Name Server (DNS) can be used to provide a prioritized list of proxies, along with a weighting, for load-sharing purposes. The benefit of using this method is that only one name needs to be programmed into each gateway and any changes can be made centrally, at the server.

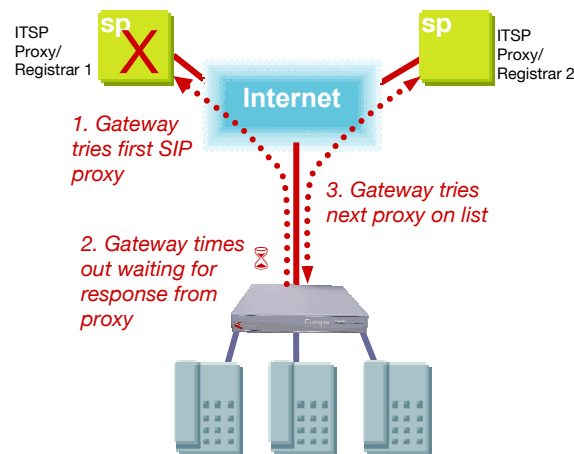


Figure 6: Alternative Proxy

Alternative Routing

Call Re-presentation is the ability to locate and use an alternative dial plan when call setup fails initially. The alternative route should take account of the initial call failure cause (The reason why the initial call setup failed, as defined in ITU-T standard Q.850).

In the event of a power failure, emergency power systems can provide continuity of service in the short-term. If the outage is a major one, however, these systems may eventually fail. In this case, a physical link to the PSTN will enable essential communications to continue. **PSTN Backup** can be achieved by using magnetic relays that switch to the PSTN when power is lost. This ensures continuity of voice services, as well as access to the emergency services, whatever happens on-site.

Maintainability

Once you've established your resilient network and taken measures to ensure continuity of service, you will want to be able to get your network running normally as quickly as possible, in the event of a problem. The key to maintainability is:

- Ease of fault diagnosis: comprehensive logs, alarms and SNMP support
- Ease of software upgrade
- Ease of equipment swap-out
- Local support, 24 hours a day, 365 days a year



5 Conclusions

Making the switch to VoIP may seem like a leap of faith but by taking a pragmatic approach to network design and equipment selection it doesn't need to be.

By:

- Securing your network using encryption and authentication
- Selecting a supplier that addresses resiliency and security across its entire equipment portfolio, not just one flagship product
- Using clever routing algorithms so that when there is a problem, calls can still reach their destination, with minimal disruption to the user
- Ensuring that you have the level of logs, alarms and SNMP support that you need to identify and fix problems quickly and efficiently
- Knowing how you are going to handle calls to the emergency services and speaking to a supplier that understands the issues and how to solve them

you can give your VoIP users the high functionality and value for money that they want, without the risk.



Acronyms and Abbreviations

| | |
|------|-------------------------------------|
| CLI | Calling Line Identity |
| DNS | Domain Name Server |
| DoS | Denial of Service |
| HTTP | HyperText Transfer Protocol |
| IETF | Internet Engineering Task Force |
| PSTN | Public Switched Telephony Network |
| QoS | Quality of Service |
| SIP | Session Initiation Protocol |
| SIPS | Secure SIP uri |
| SSH | Secure SHell |
| SRTP | Secure Real-time Transport Protocol |
| TLS | Transport Layer Security |
| VoIP | Voice over IP |

References

- [1] ITSPA White Paper: Emergency Services – Technical Issues, Potential Solutions and Benefits, April 2006
http://www.itspa.org.uk/060502_whitepaper_emergency_access.pdf
- [2] OfCom, Office of Communications - Regulation of VoIP Services: Access to the Emergency Services, Consultation. 26th July 2007
<http://www.ofcom.org.uk/consult/condocs/voip/voip.pdf>
- [3] IETF RFC 3261, SIP: Session Initiation Protocol
- [4] IETF RFC 3711, The Secure Real-time Transport Protocol (SRTP)