MorganDoyle

# Implementing VoIP? Cover the Bases.

## White Paper

# Contents

# 1 Introduction

Convergence of voice and data networks, in the first instance by implementing a VoIP telephony system, is gaining huge momentum in the marketplace. For example, the telecoms research company, Analysis, believe that mobile and VoIP will account for more than 60 per cent of residential voice spend in Western Europe by 2010, whilst amongst enterprises VoIP uptake is being driven by 3 strong factors that directly affect the bottom line:

- Low cost phone calls;
- Add-on services and unified messaging; and
- Merging of data/voice infrastructures.

If you have made the decision to move to VoIP on these grounds, you need to consider carefully a number of issues and make firm decisions before proceeding if the implementation is not to end in tears.

In this white paper we look at some of the most significant of these issues.

# 2 Disaster Recovery and Business Continuity

The fundamental change in architecture brought about in moving from traditional telephony to VoIP means that disaster recovery and business continuity plans are likely to require updating. They should be reviewed before implementation and their requirements re-assessed in the light of the up-coming changes in vulnerabilities. DR/BC requirements should be fed into the VoIP procurement exercise not retrofitted once VoIP has been implemented.

In many organisations telephony is not only a core business service but also an indispensable “lifeline” service but it may be that insufficient attention was paid to it in the old plans because of the high availability maintained by service providers with years of experience with the traditional telephony arrangement. Now telephony will be part of the data network and again continuity requirements for this may have been less stringent in the old plan than will be acceptable once voice is carried. Remember that if your data network fails for whatever reason you will have no telephones unless you make some arrangement beforehand.

As in all DR/BC planning exercises it is important to examine all business processes to assess their reliance on telephony, their priority for restoration, the length of time they could survive without telephony, their geographical distribution where a network spans multiple locations and alternative methods of provision. This analysis together with risk assessment will allow you to define the appropriate resiliency and fall-back features for your new telephony arrangement, which may include:

- Duplication of major PBX nodes;
- Fallback to POTS (Plain Old Telephone System) at all or strategic locations;
- Protection against loss of power;
- Emergency use mobile phones (which could be pay-as-you-go);
- Emergency facilities with pre-provisioned network connections;
- Re-routing via the public internet;
- etc.

Regular testing is essential if DR/BC plans are to be of any use. In particular it is essential to regularly test UPS devices and generators for degraded performance and immediately correct any problems.

# 3 Power

There are two aspects of powering an IP telephony network that need consideration. Both stem from the fact that traditional phone systems have separate power circuits and may have the appearance of being immune to power cuts.

In traditional phone systems the PBX is powered by a DC supply with, in normal, non-mission critical business systems, battery backup providing 2 hours of continued operation in a power cut. (The received wisdom is that this allows one hour waiting for restoration and then a second hour to implement contingency plans – see disaster recovery section.) In IP telephony systems the equipment providing equivalent functionality to the PBX are AC-powered servers and routers/switches. The norm for these data network devices is UPS backup power sufficient only to allow for clean shutdown, i.e. 15-30 minutes. Larger organisations may further protect those servers and switches centralised in a major "datacentre" with longer period UPS or a standby generator.

To protect the new VoIP implementation against power cuts requires identification of all key servers and routers/switches and connection of these to the appropriate backup supply. You need to ask whether all devices currently have UPS, whether the UPS's are rated to provide power for the time required by your organisation's disaster recovery / business continuity plan, and whether the current UPS and standby generator facilities have sufficient spare capacity to cope with the additional devices being connected with the implementation.

In traditional phone systems handsets take their power from the wall socket which is supplied directly from the Centrex or in-house PBX system and again these are protected against AC power failure for 2-8 hours by battery backup. In contrast VoIP handsets are connected to the data network and normal data network cabling does not include a power supply. However, there are enough spare wires to allow normal data network cabling to carry power. This gives a number of options for providing power to VoIP handsets:

- AC adapter plugged into the mains;
- USB connection from the PC;
- Power from the data network connection (in-line power injector); and
- Power from the data network connection (router/switch module).

Each has pros and cons. For the first two options as well as the possibility of power being turned off, there is a major problem of providing backup power during a power cut. Individual UPS systems become increasingly expensive for larger installations and logistically extremely problematic. Imagine the extra burden on support of ensuring that a set of individual UPS systems are all connected properly and all functioning properly with adequate battery life. So the first two are probably only suitable for small installations, in other cases centralized power and battery backup provided over the Ethernet is the only realistic method, i.e. one of the latter two options

Inline power-injectors are placed between a switch and patch panel. They require extra space in your racking, another set of patching and identification of ports to be powered (unless all ports are). They are ideal if you do not wish to upgrade your switches or, in some circumstances, replace them with a new proprietary solution, and are also useful for gradual migration or evaluation purposes. New switch modules are cleaner, in the sense of space required and patching, but they may be more expensive and lead to lock-in of supplier for both switch and handset equipment.

In either case the devices should conform to the emerging Power Over Ethernet (POE) standard, IEEE 802.3af. This standard mandates the use of a discovery voltage so that power is not given to non-power-using devices connected to network outlets. It also defines an optional graded, four-tiered power consumption classification scheme intended to minimize power consumption and,

therefore, overall power requirement. We suggest that preference is given to POE devices that support this option.

Two further considerations for POE are that Cat 5 wiring is required (Cat 3 is unsuitable) and 1000base-T (Gigabit Ethernet) is excluded (because the spare wires are used for data signaling). This is not a problem if you don't use Gigabit Ethernet or use it only for backbone networking, i.e. it does not service the desktop.

# 4 Security

VoIP is an IP application. All VoIP components - IP-PBXs, gateways, servers (proxy, registrar, and locator servers), and IP phones - are addressable and accessible over the data network, and as such are subject to all of the security threats that endanger other network connected data applications. For example:

- Denial of Service (DOS). Attacks via a weakly protected VoIP element could flood the network disabling data applications, or conversely a DOS attack on a data application could inhibit voice traffic.
- Hackers making free use of the telephone system, for example by fooled billing (making the call appear to terminate internally when, in fact, it continues externally).
- Snooping on network traffic, soft phones and voicemail by various devices, or by call hijacking (routing a call to a different destination).

Attacks on VoIP can also be made in the network on either the signaling path, e.g. to steal account codes, or the payload path, e.g. for eavesdropping. VoIP poses additional problems where NAT (network address translation) is being used to hide internal IP addresses from the outside world, because, whereas NAT deals with addresses in layer 3 protocols, VoIP uses layer 5.

Security and securing the telephone system should be well understood and implemented before connecting a new VoIP installation to the outside world. You should:

1. Engage your security experts to thoroughly update your security policy to account for the new risks posed by VoIP, and to apply existing security policies to new equipment, e.g.
    a. routinely update the IP-PBX operating system with the latest security patches; and
    b. ensure default login and administration passwords on new equipment are changed immediately they are put into service – remember VoIP handsets will probably become the commonest device on the data network.
2. Ask your prospective suppliers, unprompted, of their views of security risks and how their proposed solutions deal with them.
3. Make sure your existing infrastructure, including firewalls, routers, VPNs, etc are capable of supporting VoIP security features (e.g. dynamic port allocation, application level address inspection) with the required performance for voice QoS and are configured to do so.
4. Ensure encryption of voice traffic traveling over unsecured channels, such as the Internet, is turned on – it may not be by default.

# 5 Network Capacity

It is obvious that telephone calls require a network and that they use bandwidth on that network – they don't come for free, so switching telephone calls from a dedicated network onto your data network is going to have some impact. Calls also require a different dynamic to most data applications because the device at each end of the network (a human) is not very tolerant of delay

or variation in delay (jitter). So not only must the bandwidth previously being used on dedicated telephone connections now be found on the data network, but the Quality of Service must be assured for the new traffic. It is as well to discover if your existing data network will be able to cope with these demands before implementation by commissioning a baseline network assessment, or network readiness test. These typically run simulated voice traffic over your entire IP network (LAN & WAN) checking:

- Network devices (routers, switches, etc) have the capacity and QoS features required for voice;
- LAN and WAN utilisation;
- Interaction with, and affect on, data applications;
- Effectiveness of network-optimisation tools to maximize utilization through compression and latency-reduction techniques

You can make your own estimates of the bandwidth requirement for voice traffic by using the calculator at:

http://www.packetizer.com/voip/diagnostics/bandcalc.html,

get a feel for the quality of phone calls on your existing network by using the Mean Opinion Score (MOS) calculator at:

http://davidwall.com/MOSCalc.htm

and get a feel for the suitability of your external, Internet connection for voice traffic by using the tool at:

http://www.testyourvoip.com/.

MOS is a qualitative measure of voice quality that can be assessed by human testers or by standard calculations on various measured parameters of network performance (e.g. packet loss). Since the telephone system is such a key element of business it is as well to consider including monitoring tools, including MOS, within your procurement so that upcoming problems can be addressed before they affect business performance.

# 6 Standards - SIP or H.323?

All communication systems rely on standards. From the end user / customer perspective the ideal is a single standard, internationally agreed and adopted by all vendors. Unfortunately, VoIP suffers from two competing standards for call signaling and control issued by international standardization bodies:

- H.323 (Packet-based multimedia communications systems) issued by the ITU; and
- SIP (Session Initiation Protocol) issued by the IETF.

There are other, proprietary protocols in use, for example Skype.

Call signaling and control is responsible for call set-up (locating the called device and negotiating how information will be exchanged) and many of what ordinary users would regard as PBX features. And newer features envisaged for converged applications (e.g. instant messaging).

Work started on both standards in 1995, but H.323 was the first to be published (in 1996) and implemented by vendors. It remains the most widely deployed and handles literally billions of call minutes every month. It builds on the ITU's wealth of traditional telephony standards and so it

interfaces well with the PSTN and is rich in support of traditional PBX features. It is seen by SIP proponents as monolithic, unwieldy and difficult to expand to include new services.

Even though SIP had a longer gestation (first published in 1999), it is a simpler standard. Following the IETF philosophy of many, modular components, SIP, as it name suggests, was originally for session initiation only. Whilst this had the advantage of being simple to implement, it s features were insufficient for complex situations which are much closer to the norm in telephony, and so different variants of SIP with additional features have been created. A further problem which has made for slow adoption by service providers and enterprises, is that service logic (e.g. call hold, call transfer, call park, etc) is in the end-user device. This makes problem resolution more difficult, tends to restrict the choice of end-user devices and makes the introduction of new services more complex and expensive. Amongst SIP's advantages are its more human meaningful addressing/numbering – something akin to an email address rather than a number – and its support for instant messaging both of which make it more amenable to convergence with the data world.

However, both protocols work and do the basic job of supporting voice calls, and both have their advantages and disadvantages. There is no guarantee that one or the other will eventually dominate the market and since no-one can predict the future and you should never believe the hype, we suggest that you carefully determine and prioritise your requirements, including the requirements of key business applications in your long-term strategy and then judge on today's functionality and availability which suits best. It may be helpful to study the following comparison tables one with a H.323 bias (http://www.microtronix.ca/sip_vs_h323.htm) and one with a SIP bias (http://www.iptel.org/info/trends/sip.html).

One final note. Even proprietary solutions like Skype may have their niche in enterprise telephony, for example as another gateway into the organisation's call centre made available for customers who know and accept its quality issues.

# 7 Phone type

The popularity of softphones waxes and wanes, and is dependent on the type of job a user does. For call centre operative they are almost obligatory; for a salesman almost irrelevant. But what about all of those roles that sit between these extremes? Currently they are perhaps on the wane because:

- Application suites whether related to telephony or not tend to increase in complexity and demand on the PC's resources whilst maintaining good quality voice using a softphone also uses a significant amount of a computers resources;
- Voice processing is done in hardware in a hard phone, which is always likely to be more efficient and higher quality than software processing;
- Standard phone features, even something simple like a message waiting light, are not always well supported in a softphone; and
- Some advanced mobility features are based on easy access to any of the various telephony devices available to a user and yet softphones may often be unreachable.

Having said that, softphones have their place and can represent a considerable cost saving depending on the quality of headsets demanded by users.

# 8 Contact Details

For further information or advice contact *MorganDoyle* Limited. The latest contact details can be found on our website at http://www.morgandoyle.co.uk/