

## From the MD

Hello everyone and welcome to the July newsletter.

Some interesting stuff on the boil this month, with our new marketing campaign nearing completion - we will be showing this with you next month. We have finally had time to draw breath on the VOIP trial and put our thoughts down this month. Also, we are going to try a new technique with the newsletter this month.

In the past we have struggled to say everything we thought we needed to about a topic to give good rounded information, while also keeping it brief. This month we are going to put some "further information" links in the newsletter, so if a topic takes your interest and you want to know more put the URL into your browser and follow it back to the website for more info.

See you next month.

Clem.

## From the Editor

This edition I'm wearing two hats as they say, not only as editor of the newsletter, but also as the developer of the software that helps run ColmanComm. You'll notice in our newsletter's HelpDesk Hints we make reference to a Task Number which you receive when logging a job. This helps us track jobs, and is particularly useful for our larger clients who may have many tasks running concurrently. Of course, you need to write it down, and keep track of which task is which in order to follow it up or check how or when an issue was resolved. But not for much longer...

Internally we use a system we developed called FORGE. A traditional forge is a device to collect, refine and process materials, usually using intense heat, to produce something useful. We use our FORGE in much the same way to collect and process information, without the intense heat. We've been using it for several months now, and it's made a definite improvement to our ability to track and manage tasks, so we'd like to give you the same benefit. Over the next few weeks we'll be setting up access for our clients to log in and view the status of all their current and resolved tasks. You will receive your login details by e-mail. At this stage we expect to only provide logins to key staff within each client organisation. The next step will be to let you raise a task with us online. We're looking forward to your feedback and suggestions regarding this feature and how else we can get the best value to you.

Until next month,  
Steven Craddock

### In This Issue:

- Message From the MD
- Message from the Editor
- About VOIP
- Client Profile - ISP Dr. Internet
- Disaster Recovery
- Service Life of IT Equipment

### HelpDesk Hints:

- Log all queries and requests through the helpdesk;
  - [E-mail: helpdesk@colmancomm.com](mailto:helpdesk@colmancomm.com)
  - Phone (02) 6287 3036
- Please record your **Task Number** for future reference

## About VOIP

VOIP (**V**oice **O**ver **I**nternet **P**rotocol) is a technology that allows telephone calls to be made using a computer network (including the Internet) rather than a normal telephone connection.

A VOIP device takes sound (such as you talking) and then turns that conversation into a stream of packets which is transmitted across a network to another VOIP device, where the stream of packets is turned back into sound.

If you are having a conversation between two VOIP devices (and VOIP devices come in lots of shapes and sizes – many of them look, and behave, identically to a phone) then nothing more is needed. However, if you want to speak to someone on a normal phone, then you need a VOIP provider that connects your call over the Internet to the normal telephone network.

## What Are The Benefits?

### VOIP Can Save On Call Costs for Small Businesses

If you use VOIP over the Internet then your VOIP provider is normally able to offer a cheaper call tariff. The typical call tariff from VOIP Providers in Australia at the moment is 10c untime for all calls to land lines anywhere in Australia. International calls represent even better savings relative to normal phone company tariffs. However, calls to mobiles don't have as great a savings.

Whether or not your organisation can make significant savings using VOIP will come down to your call patterns. You need to study your phone bill and work out what sort of calls your organisation makes the most of.

### Distributed and Mobile Telephone System

VOIP allows you to have a phone system that transcends the physical location of your office/PABX (sorry – we don't get to use words like transcend all that often in our work, so when the chance comes up we are going to grab it).

If you use an online VOIP Provider, and your VOIP phone can reach the Internet then your phone is good to make and receive calls.

In our trial here at Colmancomm, where we work in different offices, we are using VOIP phones to provide a unified telephone system, with free internal calls, call transfer, PABX etc. But more than that, if we need to work in another location we can take our phone with us.

The reverse of this can be applied too. For example, you may want to hot desk staff, but always have an issue putting calls through to the correct desk. VOIP allows staff to “log into” the VOIP phone that is on their desk of the day.

(continued...)

### VOIP @ Work:

- Make sure you understand your call patterns.
- Buy quality VOIP equipment.
- Make sure you have enough bandwidth.
- Get your bandwidth tuned correctly.
- Run a trial before stepping to a full install.
- Understand the limitations of your network.

## What are the Drawbacks?

### Call Quality Hard to Guarantee for VOIP Over the Internet

With proper configuration and equipment call quality will normally be OK. Normally. Normally it might take you 10 minutes to drive to work, normally. Some days it takes 12 minutes, and every now and then there is a major snarl and it takes 20 minutes.

Call quality when you use VOIP over the Internet is a bit like that drive to work – it should normally be okay, but it is subject to a whole lot of factors which are beyond your ability to control.

During our trial we have been keeping track of calls with poor call quality versus total calls. Out of 107 calls, 5 had call quality that was sub optimal, and 2 had call quality that wasn't really acceptable. That's on a lightly loaded link, after tuning for VOIP.

### Step Up In Standard Of Engineering

Computer networks often aren't built to the same standard of engineering as telephone systems. For example, although your servers may have battery backup, your network switches probably don't, so if you loose power, you will lose your phone system. That may be okay, particularly with almost everyone having a mobile phone these days, but you do need to keep in mind that in life and death emergencies people rely on the telephone working.

### Bandwidth Hungry

A good quality VOIP conversation is going to use about 100Kb of bandwidth. On a standard 256Kb/1.5Mb ADSL 1 service that is two concurrent conversations max (and chances are you would be experiencing call quality issues already) assuming nothing else was happening. ADSL 2 offers greater promise for small organisations.

## Conclusion

VOIP, and VOIP over Internet offers the possibility of having a more capable, and geographically distributed telephone system for a fraction of the price that it would cost with a traditional PABX type systems – particularly for very small businesses. Further, the opportunity to save on call tariffs is also welcome.

However, the technology is, for all those capabilities and cost saving opportunities, not as reliable as the telephone system.

If you were setting up a new office or business it would be well worth considering going with VOIP over the Internet from the outset. If you were planning to implement VOIP with an existing business it would be good idea to, once you have identified what you want to achieve, conduct a trial first.

As for us, we will be sticking with it. There are some issues, but it suits our geographically distributed work force beautifully.

### VOIP @ Home:

- Great savings for speaking to interstate/overseas family.
- Will work OK on most home ADSL Connections.
- Call Quality constraints less of an issue for home use.
- Buy quality VOIP equipment to beat the "softness" issue.

### **Disaster Recovery**

In our last edition, we covered the topic of catastrophic failure. It can happen, does happen, and probably will happen – to you. The longer you rely on IT infrastructure the more exposed you become to a failure occurring. It may be minor, but in many cases, a failure of an essentially cheap piece of equipment can stop a business in its tracks entirely, often for days.

So assuming it will happen eventually, and there's no way to stop it, how do you recover from such an event? We'll use an analogy which most people will be familiar with to illustrate first. Car accidents. If you haven't been in one, you've seen one, or know someone who has, and generally understand the process. We often see clients say the equivalent of "I've just been in a car crash, should I put my seatbelt on now?" Obviously the time to put the seatbelt on was before you started driving, and the same goes for disaster recovery. Preparedness is everything.

The two fields information technology primarily services in small business are information processing, and communications infrastructure. Information processing is your word processing, spreadsheets or databases. Communications infrastructure is your e-mail, VOIP telephony, office networks and so on. We'll tackle information processing failure first. Regardless of the exact nature of the failure, we have one thing working on our side. Essentially, and I'm drawing a fairly long bow here, all computers are exactly the same. At an abstract level at least, they're all the same. That's how I know that if I install Word on 50 desktops in an office, they will all operate in the exact same manner. I can save my word document, send it via e-mail across the world and back, and a computer in America, or Taiwan or Antarctica will be able to read that document in exactly the same manner. So the actual computer becomes almost disposable, and should be viewed as such. The key component here is the information itself (the Word document), and the application processing it (Microsoft Word, or Open Office if you're that way inclined). As long as the information is safe, we can get you up and running again relatively quickly. This means backups. And like wearing a seatbelt every time you drive, backups require consistent, disciplined application if they are to be of any real value. There are a range of backup solutions available to choose from depending on how risk averse you are and how much data you need to back up, but they all have one thing in common. You need to plan them, put them in practice, and importantly, review their effectiveness. This means doing what we call a "trial restore" where a file or selection of files are restored from the backup to ensure they were recorded properly. This is essential, because like any other device, there is always the chance that whether your backup device is tape or CD or DVD or an external hard drive or network copy, it could itself be malfunctioning. Obviously, the worst time to discover this is when something else has failed. If you effectively back up your data and retain a copy of that backup which can be loaded onto another computer, the failure of a single computer becomes an annoyance more than a disaster.

Now that you have a regular backup scheme in place, and periodically confirm that it's working, how do you actually recover from a failure? Do you need to repair the fault first? Not necessarily. If you have more than one computer in your organisation, chances are you can limp along by restoring the data and applications to another PC and using it. You may end up with staff sharing that computer which is frustrating, but it will get you up and running again quickly. If you need to replace a failed component, in most cases you can do so in around 12-24hrs. The caveat here is that only applies if the component which failed is still in production. The internal organs of PCs which users are most often blissfully unfamiliar with aren't exactly Lego bricks.

While you can swap them around from time to time the way they plug together changes and manufacturers stop making the older versions. If you have server which is five or six years old, which is not uncommon, not only is it nearing the end of its useful life and likely to fail, the chances that you'll be able to find replacement components to match are rapidly diminishing. This rules out the option of ducking down to the local computer hardware store, grabbing a new hard drive or whatever failed, and getting up and running quickly. You may find that a whole new server will be required. Read that again, whole new server. As we've mentioned numerous times in the past, this is an unfortunate but unavoidable aspect of IT. You need to be prepared to replace hardware periodically. It is obviously by far preferable to go about this in a planned and orderly manner, rather than a rushed panic due to a failed component bringing your business to a halt.

Communications infrastructure failures can be more frustrating, especially when multiple service providers are involved. For example, the failure of an Internet connection may be rats gnawing through cables in your roof cavity, fallen tree branches taking down your phone line and associated ADSL connection, a failure at your ISP, a failure at the phone exchange or any combination of the above. Once again, the concept of a backup comes to the fore, but in a slightly different manner. We're now talking about "redundant architecture". Redundant, because you don't really need it, until your main infrastructure fails. We'll use an internet connection as an example. Typically a small business will have a server connected to an ADSL service by a router. The kind of hardware you can buy at the local department store. If the router fails, and you don't have one in the cupboard, you'll be off air for as long as it takes to drive to the shops and buy a new one, then reconfigure it. What if the phone line fails? You can have a second line with a backup ADSL service waiting at the ready, but chances are better than good that a stray tree branch won't discriminate between lines. Also, if both lines are with the same service provider and the ISP fails, you've now got effectively double the useless bandwidth. Not an improvement. Similar arguments exist for many redundant schemes. Your most effective option, and one we've employed frequently is a service with as little in common with your regular service as possible. As an example, when a client's wired broadband service fails (ADSL/TransACT or similar), we can deploy a wireless service using a different provider altogether. This helps overcome failures on a local level. In the past we've been able to allow a client to keep operating for several days while their ISP attempted to diagnose and repair a fault. We did this by loaning them a wireless router which connected to the Internet via the same kind of network mobile phones use, but optimised for data transmission instead of voice calls. It meant their e-mail was disrupted for a matter of hours, instead of the week or so it took to get their normal service restored.

There are however bona fide show stoppers. The classic example is "What if the building burns down?" While this rarely happens, it is often presented as the worst possible scenario. We get asked how quickly we can get everyone back working. The truth of the matter is, that even with the most regimented backups, your IT needs will be far from the fore in terms of urgency. If your building has literally burnt down, you'll need a new fleet of computers. And desks. And chairs. And phones. And a building. It's also true that once you have these things, if you have followed your backup procedures properly, it will be a relatively routine procedure to get the new equipment loaded with your old data and productive again. By comparison, finding new premises, furniture, hardware etc. will be a much bigger challenge.

(continued...)

So to summarise, disaster recovery has more to do with prevention than reaction. In the case of information processing, having a backup of your applications and their data is absolutely vital. We cannot stress how important this is. In the case of communications infrastructure, having a distinct fallback service is vital. If you are to rely on these backups, they must be tested periodically to ensure they actually work as expected.

### Client Profile – ISP Dr Internet

Continuing our series of client profiles, this month we cover our invisible client. I say invisible, because we very rarely see them for a couple of reasons. First, they're located in Narellan, on the south most edge of Sydney. Second, and importantly, they are a testament to the stability of the software we developed for them. We generally have no need to see them, which is good, because it means nothing has gone wrong or needs improving.

ISP Dr Internet is an Internet Service Provider with clients not only in the Sydney region, but also in regional NSW. To maintain a stable and profitable ISP requires subscribers. Thousands of them. Literally thousands. Most of these subscribers pay by credit card, on a monthly basis. As an exercise to highlight the main reason they needed our assistance, write down ten sixteen digit numbers, random credit card numbers. Now next to these write random expiry dates. Next to that, write a CVV (Card Verification Value, the three digits printed on the back of the card). Next to that, write down an amount to pay, and an account name to credit the amount to. Getting tedious? This is just the setup. Now, grab a stopwatch and time how long it takes you to enter all ten credit card numbers, and expiry dates and amounts and so on into a spreadsheet. For realism, add five or ten seconds between each one to allow processing time. Then record the result of that transaction in an imaginary billing system. Now imagine processing *thousands* of these each month. It required a full time position just for processing payments in addition to existing admin staff processing when their other duties allowed. The sheer volume made the data entry, punching numbers into a keypad, time consuming and error prone.

Several years ago we came to their aid by developing an automated credit card processing system for them. Like most ISPs, they already had a system to track their client data, so we needed to integrate our payment gateway with their accounting system. This dramatically reduced the labour involved. It also improved the accuracy, and dramatically reduced the processing time. Staff didn't even need to watch as the payments were processed by the bank, just read the report at the end of the batch. The system even automatically sent the results to their accounting system so the clients accounts would be automatically updated. The same gateway was also incorporated into their web site so users could make ad-hoc payments without leaving their card numbers with ISP Dr at all.

In a fiercely competitive market space, ISP Dr's choice of implementing a system which reduces the need for labour has saved them tens of thousands of dollars each year. We can't claim all the credit here, a vital component of the whole system is the integration with their existing software. Under their direction, we tailored a solution to best suit their business, rather than forcing them to adapt their business processes by using readily available banking software. We let them get keep their existing practices and systems while providing a much needed speed boost, so they could get on with managing the technical innovations to keep them at the forefront of ISPs, and service their clients better.

## Service Life of IT Equipment

All too often we encounter customers who have suffered incidents because they have kept IT equipment in service for too long, rather than turning over equipment after it reaches an end of its reliable lifetime. But how long should you hold onto equipment?

The reliability of IT Equipment over time follows a predictable curve, being slightly less reliable in the first few weeks (we sometimes call this the “burn in” period), becoming more reliable in the first six months, peaking in year two and then starting to fall away.

The curve can be shorter for certain types of equipment (laptops tend to have short lives), while equipment with no moving parts (like routers) can have longer lives.

Here are our recommended lifetimes for systems:

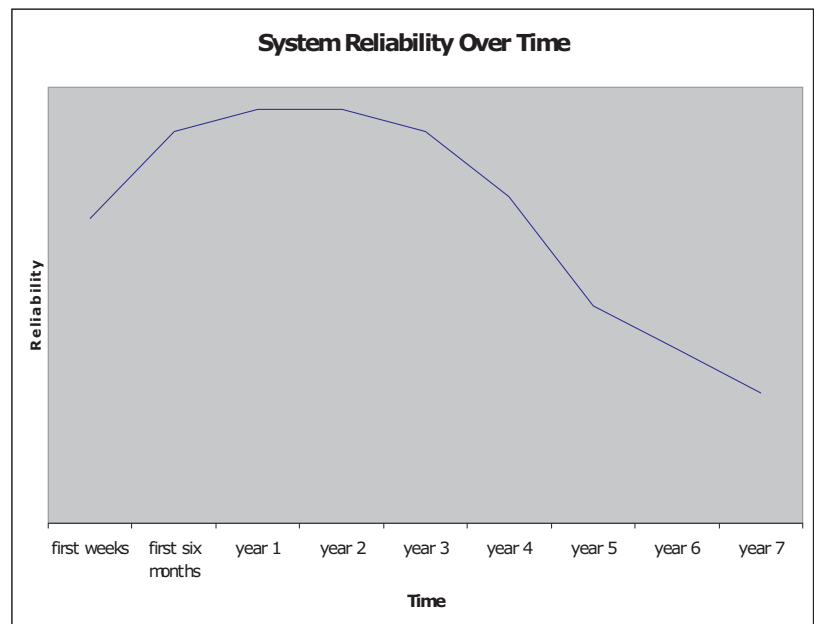
Servers: 3.5 years.

Workstations: 4 years.

Laptops: 3 years.

Network Switches and Routers: 4 years.

Pushing your systems past a reasonable lifetime is going to have an impact on your organisation – even if you don't have a fault that brings your business down your computers will still be afflicted by “slowness” that your staff will come to accept as “normal”.



### That's all for this month...

We'll be back next month with another edition. In the mean time, previous editions of the newsletter are available on our web site. <http://www.colmancomm.com/news.html>

Until next month, all the best from the team at Colman Communications Consulting