



If we open it, they will come...

Over the past few years we've seen the fundamental reorganisation happening in the ICT industry as the traditionally disparate technologies associated with data transmission and telephone-based telecommunications have collided to create what we now know as "converged ICT". The defining factor in this convergence has been the migration of real-time interaction capability into the application space, and the global "yes" vote for IP (Internet Protocol) as the standard for data transmission.

We've all heard the catch-cry "voice is just another application". By its very definition voice, like any other application, is no longer embedded in the infrastructure. It is now at the "edge", and the network infrastructure is simply a transport mechanism to be exploited so the application can perform optimally.

Everyone it seems has been on a spending spree in efforts to create the one-stop-ICT-shop. The carriers have bought up competency in the traditional IT arenas - Telecom acquiring Gen-i, TelstraClear buying IT services firm Sytec and across the ditch its parent Telstra Corp completing the well publicised purchase of KAZ. But the carriers aren't alone. IBM snapped up Logical (on both sides of the Tasman) a couple of years ago and other traditional IT players have been deliberate in their efforts to round out their competency bases to stay competitive in the converging ICT space.

You'd perhaps think that this would create a much more homogeneous supply environment with a certain "desirable sameness" at - all the big players essentially able to address the full breadth of the ICT domain and approaching the converged world in a more consistent manner for the benefit of the overall environment. But it hasn't worked out that way. Now that "telecommunications" is

no longer the exclusive domain of the carriers, it seems that the battle lines are being drawn around the role and provision of the transport infrastructure.

This isn't simply the Local Loop Unbundling (LLU) debate. LLU is only part of the issue and unitching the "last mile" from the incumbent could simply make the infrastructure available to a wider community of telcos and wannabe telcos so they could all continue to shackle the user with rate-limited, consumption-based service bundles.

I don't buy the argument that opening up the infrastructure will be detrimental to the New Zealand economy as it will result in decreased investment by the carriers.

As traditionally silo-oriented telecommunications has collapsed into the IT space, the wider issue is just how open should the access to this underlying, abundant infrastructure be? That is, to what extent should we be able to use the infrastructure to the limits of its capability - a bit like being able to pay once to drive on the road when you buy your car, instead of paying petrol tax.

The carriers maintain a firm stance that the real value is in the network infrastructure. Read the sub-text and what this really means is "we invested in it, and on behalf of our shareholders we're entitled to sweat the assets for maximum return". So the infrastructure is bundled with other capabilities, typically intelligence at the edge and/or value-added managed service overlays, in a commercial construct that is based on consumption. This is what's known as vertical integration and the carrier has its hands firmly on the value tap, controlling the extent to which

the network capability and capacity can be exploited, and therefore the value proposition of the intelligence at the edges.

Ironically, the internet, which has generated the explosion of end-user consumption of network resources, is the phenomenon that is sounding the death knell to the carriers' stranglehold on those resources. Why is this? The internet is one of the most universal illustrative examples of the old adage "if we build it, they will come". The internet is exploited by individuals and groups for all manner of

purposes that we could never have imagined. The same can be said of network capability. As applications are dreamed up daily, the opportunities to exploit capacity multiply at an exponential rate. The tragedy is that the value in all this smart stuff is fundamentally limited by the drip-feed meter that limits the use of the network. This is a key factor that constrains economic development by limiting the value that can be derived from innovation.

And I don't buy the argument that opening up the infrastructure will be detrimental to the New Zealand economy as it will result in decreased investment by the carriers. The truth of it is that there is a vast amount of infrastructure capacity already available here in this country. It's lying in the ground, strung on overhead wires or contained in available wireless spectrum. It's owned not just by the carriers, but by power transmission companies, media companies and public/private

partnerships that have deployed it for specific purposes associated with their businesses. Almost criminally the vast majority of that capacity is unused!

The answer to all this is a deliberate move to open up access to basic network transmission infrastructure.

And we're starting to see it happening. Corporations with vested interest in the intelligence and computing power at the edges are starting to move - their very survival depends on actively addressing the network transport considerations that constrain the value proposition of their core business offerings. And governments that need to stimulate the creation of value within their economies are moving to encourage the provision of telecommunications network infrastructure on open access principles. Elements of our own government's Digital Strategy provide examples of this wave - even if you might wish for more and faster progress.

So it seems there is a groundswell of opinion across business and government, both locally and globally, that if we open it they will, indeed, come. And the construct that will provide that openness, and that is already emerging as a global phenomenon, is the Infrastructure Utility. I'll look at this concept and the implications of the worldwide drive towards it in a later column.



Michael Foley is a director of i-solutions, a consultancy working in telecommunications and converged ICT.



SECURITY

The botnet threat

Botnets are one of the biggest threats to the internet.

Bots are generally scripts or executable code designed to provide remote control functions; they are tools, the majority of which are not inherently bad - often referred to as agents. These bots are often invisible to the user or inherently have the ability to hide themselves.

Bot capabilities include: Distributed Denial of Service (DDoS) attacks, Flooding attacks, DDoS extortion, exploit scanning and auto rooting. However, they

are often used for unattended system and user maintenance and are occasionally found on instant-messenger and mobile devices networks as robotic helpers for users. Legitimate examples can include Calendar bots, Directory bots, Alert bots, Lookup bots, and Wireless Access bots for PDAs, WAP-Phone or wireless hand-held devices.

Malicious bots though, are essentially Trojan-horses, backdoors or Remote Access Tools or software programs that open up a victim's machine to remote access. They are capable of spreading

through a number of methods such as email, viruses and worms, which can use IRC networks and network shares to propagate. Once executed or activated bots will typically announce their presence via numerous means and IRC channels to "call home" to their attackers. Bot worms have among the most variations of any kind of worm. These variations include Rbots, SDBots, Gabobots, spybots and half a dozen others.

Typically, a bot provides a communications link, normally via the internet, and may use many methods to communi-

cate, typically IRC (Internet Relay Chat) reference RFC 1459; update RFC 2810, 2811, 2812, and 2813. IRC is an open network protocol based on TCP and can be enhanced with SSL.

Other means of communication are actively experimented with such as Instant Messaging and Peer-to-Peer networks. Recently it was discovered that Skype, a Peer-to-Peer and VoIP network, is thought to be able to carry command and control communications for managing botnets.

CONTINUED NEXT PAGE

NO MORE CHIMPS!



We have exceptional people that will provide the right technology solution for your company.

BTG - Your trusted partner.

Visit our website www.btg.co.nz to learn more about BTG.

- INFRASTRUCTURE
- SECURITY
- COMMUNICATIONS
- REMOTE COMPUTING



Business Technology Group

Empowering Business Independence

Visit www.btg.co.nz
Phone +64 9 580 1374

