

Bayly Communications White Paper Version 4.0, October 22, 2004

Network convergence over IP – one size does not fit all!

Originally, the compelling cost savings of consolidating voice, video and data transmission over a single network sparked interest in network convergence over Internet Protocol (IP). Today, network convergence over IP is largely being driven by the promised cost savings of IP Telephony. In fact, In-Stat/MDR predicts that the number of IP lines shipped in PBX systems will grow from 5.5 million in 2003 to 15.9 million in 2008. In the same report, they predict that while the PBX market is mature and slowing, between 2003 and 2008 shipments of converged PBX lines will grow at a 11.2% CAGR, while pure IP PBX line shipments will grow at a 28.9% CAGR.¹

This is leading many organizations to create infrastructures based entirely on IP. But is this the right solution?

Convergence should not necessarily equate to pure IP

Through aggressive marketing by IP vendors, general market perception is that convergence is synonymous with IP. In a recent article in TMC Internet Telephony², author Tony Rybczynski defines convergence as follows: “Network convergence is the act of bringing voice, data, and video onto an IP, Ethernet, or optical network. Enterprises striving for uniformity have focused on the IP protocol suite, as the protocol of choice for networking and applications, spurred largely by the Internet and by the economics of having fewer protocols to manage.” This article and others like it suggest that IP is the protocol of choice: we believe that many I.T. professionals take this to mean that IP is the *only* choice. In fact, for certain applications, it’s definitely not the best choice.

We define convergence a bit differently: *“Network convergence is the migration of technologies from legacy based voice and data to IP based technology. This will be a gradual transition characterized by consolidation and optimization of existing network infrastructure where users will need to support a mixture of technologies on a common platform.”*

Critical information needs better than best effort

Critical infrastructure networks are those that require guaranteed, always on, service. They all have very similar requirements: they carry corporate non-critical traffic that can capitalize on the best path routing of IP — *but more importantly, they have critical traffic requiring guaranteed connection.* They typically have a separate network that carries their critical data over fiber and microwave – using transport mechanisms such as SONET/SDH (TDM), ATM or Frame Relay.

¹ IP PBXs: A Market Hitting The Tipping Point, May 2004, In-Stat/MDR

²“2004: The Year of Convergence”, Tony Rybczynski, TMC Internet Telephony, January 2004

Today, IP is known as a best effort network, that is, it does not provide guaranteed delivery. While this may be more than adequate for most enterprise communications, for critical infrastructures, the network must be “always on.”

Some examples of critical infrastructure networks include:

- Transactional information in financial networks such as banks, insurance companies, etc. In these environments, a network outage or traffic slowdown can translate into literally millions of dollars lost.
- Monitoring information in industrial and transportation environments with programs such as SCADA – real-time data gathering from remote locations to control equipment and conditions. Imagine the problems if data packets from a train monitoring systems did not arrive properly – it could result in track problems, causing accidents and even death.
- Voice communications in enterprise networks – while best effort Voice over IP (VOIP) may be acceptable for many organizations; voice is very sensitive to latency, which can cause echoes, or even worse, a delay in hearing what the other person is saying. In fast-paced business environments where good communication is essential, this may not be good enough.
- Monitoring systems in industrial applications such as oil & gas production and distribution. Reliability for SCADA applications is critical to ensuring that equipment in the field is operating properly — imagine the environmental implications if a report of a damaged or blown wellhead can't reach the central monitoring site!

We believe these critical infrastructure networks — such as utilities, oil & gas companies, financial institutions, government and transportation authorities — need to take a hard look at a **hybrid** approach to convergence, for several very compelling reasons:

- They have guaranteed delivery requirements for critical monitoring data and voice that just can't be answered with IP.
- They've already invested significant funds in their infrastructure, which can be extended for several years by using a hybrid approach.
- The infrastructure of leased lines and private fiber networks already exists, and can be effectively leveraged.
- In some of these private networks (like jungles & deserts), the Internet may not even be available, which could negate the benefits of using IP as a transport mechanism.
- Their critical infrastructure can be vulnerable to Internet-based threats, which puts the entire organization at risk. For some organizations, this is not an acceptable risk.

Real Life Rationale for Hybrid Networks

On-time, accurate signaling is key

In railway systems, getting the right signal to the system at the right time is critical – people's lives could depend on it. In these networks, security and reliability are key – can you afford to lose communication as a result of a virus, worm, or other malicious software that can infiltrate the network through the Internet? Consider this story...

"A computer virus was blamed for bringing down train signaling systems throughout the East today. 'The virus infected the computer system at CSX Corp.'s Jacksonville, FL, headquarters, shutting down signaling dispatching and other systems at about 1:15 a.m. Eastern time,' CSX spokesman Adam Hollingsworth said."³

Down time unacceptable

For many organizations with critical business operations, down time can prove to be an expensive issue. Recently, Merrill Lynch decided to protect themselves and ensure "always on" network availability and reliability. An article in Business Communications Review reported that "... Merrill Lynch announced it was replacing Cisco VOIP gear with a hybrid IP-TDM system from Avaya in its Hopewell, NJ location, citing security concerns that would seem to go to the heart of the convergence issue."

A Merrill Lynch spokesperson indicated "... there is an increasing concern associated with the risk of completely losing both voice and data communications as a result of an IP network outage. This exposure is amplified by the constant presence of IP security vulnerabilities, and the increase in the level of attacks over the past two years."⁴

If IP offers only best effort, then why use it for critical traffic that really requires guaranteed delivery? It makes more sense to create a converged infrastructure that utilizes the transport mechanisms that meet specific needs, particularly for critical applications such as industrial, transportation, utility and finance — much of the critical infrastructure is already in place! By doing this, organizations can prolong legacy investments while implementing solutions in a controlled manner that makes sense for their business.

³ *The Associated Press*, 8/21/03

<http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml>

<http://computercops.biz/article2856.html>

⁴ *Business Communications Review*, September 2003,

<http://www.bcr.com/bcsmag/2003/09/p26.php>

Building a hybrid converged network

We believe that organizations should seriously consider building a hybrid network, versus converging all network traffic onto IP. Existing network infrastructures should be evaluated, and either phased out or optimized into the hybrid network, potentially as part of a longer-term network evolution plan.

Any converged network – whether a hybrid of legacy and new technologies, or exclusively IP – must satisfy several key business requirements:

- It should support legacy voice and data, so that organizations can leverage these often-expensive investments for as long as possible, minimizing capital expenditures.
- It must support a multi-vendor environment, to allow organizations to transport all traffic, and use the solutions that best meet specific needs.
- It must provide the flexibility to support both bandwidth optimization (best effort) and guaranteed delivery.
- To ensure guaranteed delivery and equipment optimization, it should support mixed technologies including low latency TDM on SONET/SDH, legacy voice and data, ATM, Frame Relay, Multiprotocol Label Switching (MPLS), and of course, IP.

Encourage evolution, not revolution

While prevailing opinion suggests that pure IP is the way to go, we believe that organizations should take what they have today and migrate deliberately and cost-effectively, creating a hybrid network.

Before throwing out existing network equipment in favor of an all-IP infrastructure, organizations should objectively assess their business needs, and ensure that they match their network requirements to select the appropriate network elements. We believe the best network convergence solution for critical infrastructure networks is a hybrid approach: one that leverages the benefits of IP, but also that complements other legacy network technologies with the goals of improving network efficiency, consolidating network elements and optimizing network performance. The result is a hybrid network that provides all the benefits of IP while maintaining existing infrastructure to provide the right solution from a business and technology perspective.

Ian Graham
Product Manager
Bayly Communications
igraham@bayly.com