Ensuring Business Continuity with Last-Mile Diversity and Redundancy
Michael Harris
Kinetic Strategies
Ensuring Business Continuity with Last-Mile Diversity and Redundancy

“Internet outages and service degradation cost midsized companies $189,000 per year.”

Michael Harris, Principal Consultant, Kinetic Strategies

In support of their business continuity plans, many midsized companies endeavor—as the proverb advises—to avoid putting all their eggs in one basket.

Understanding the critical role of last-mile connectivity and always available Internet access for their enterprises, savvy firms utilize redundant connections from multiple service providers. Despite the good intentions, their Internet connectivity risk may still be in a single basket. That is because internet service providers (ISPs) and competitive local exchange carriers (CLECs) may operate using leased network infrastructure from the same incumbent local exchange carrier (ILEC).

The Cost of Failure

Businesses in Silicon Valley were reminded about the importance of network redundancy during an April 2009 incident. Early on a Thursday morning, vandals cut ten fiber-optic cables in San Jose, Calif. While most of the fiber lines were owned by AT&T, numerous service providers were impacted, including Verizon and Sprint. More than 50,000 business and residential customers lost service. Following the network failure, doctors could not access electronic medical records, 911 calling was interrupted for first responders, ATMs were unavailable, and businesses could not process customer orders or payments. Even mobile services from multiple carriers were disrupted as connections to cell phone towers failed¹.

When Hurricane Sandy roared ashore in New Jersey in late October 2012, landline and mobile communications services throughout the Northeastern U.S. were severely disrupted. Even those carriers that were “too big to fail” did. As a result, many customers on Wall Street and other Big Apple business districts lost Internet connectivity².

Internet service outages may result from myriad causes: from sabotage, natural disasters or terrorist attacks, to unexpected utility line cuts and regularly scheduled network repairs, as well as equipment or application software failures. Additionally, IP network configuration errors, hacker attacks or congestion can severely degrade Internet services, undermining service availability. Whatever the cause, when the flow of Internet data stops, business does too. A survey by Infonetics Research found that medium firms experienced an average of 32 hours of

¹ Internet outages and service degradation cost midsized companies $189,000 per year.”

² www.twcbc.com
network downtime each year due to service provider failures. The cost to each midsized company of lost revenue and productivity caused by outages and service degradation averaged $189,000 per year³.

Similarly, a survey of medium and large businesses by IT firm CDW estimated that network outages cost U.S. businesses a combined $1.7 billion in lost profits, with 21% of that total resulting from service provider problems.⁴ More than half of businesses reported lost productivity from recent network disruptions, while nearly a third experienced a complete business shutdown (see Figure 1).

CLEC Reality Check

In larger U.S. cities businesses may have a choice among several Internet access and network service providers. The menu typically includes the ILEC, CLECs, ISPs and cable company. CLECs can often afford to build facilities to reach business customers in densely populated commercial districts and office parks. In other cases, CLECs and ILECs utilize the same local and regional physical network infrastructure. A brief history lesson will help explain why.

The original Bell telephone system operated by AT&T enjoyed a monopoly on local and long-distance telecommunications services in the U.S. for more than a century. In 1984 a groundbreaking court ruling split AT&T into separate local and long-distance companies, creating a gap for alternative providers to enter the telecom marketplace. However, the high cost of constructing local access networks separate from the ILEC proved to be a major obstacle for many upstart competitors. CLECs could typically only justify constructing their own facilities in highly concentrated business districts.

“CLECs and ISPs are the new middlemen between the customer and the local exchange carrier.”
Congress and the FCC worked to address the problem through the Telecommunications Act of 1996, which required ILECs to sell unbundled network elements (UNEs) to competitors on a wholesale basis. Competitors could enter the market without having to construct their own facilities. The breakthrough offered more businesses a choice for their communications needs, applying pressure on the ILECs for better pricing and service.

The downside is that, when it comes to local network infrastructure, some CLECs and ISPs started to serve merely as an intermediary between the customer and the ILEC. In this situation, the competitor’s ability to innovate on pricing is limited by the network fees charged by the ILEC. Additionally, the ability of CLECs and ISPs to provision, monitor and repair services is dependent on ILEC assistance. When the ILEC network fails, so do the services of alternative providers utilizing the same physical infrastructure. Through network unbundling and resale arrangements, not only do these CLECs and ISPs use ILEC lines to offer service, they may also use ILEC central-office equipment to deliver broadband Internet access over local copper loops. Where else can businesses look for facilities-based redundancy?

**Calling on Cable**

Cable’s infrastructure is physically separate from the telephone company networks at the local last mile, metro and regional levels, enabling genuine network redundancy and diversity, as illustrated in Figure 2. Cable operators have built extensive hybrid fiber and coax networks to deliver video, Internet and telephone services. By leveraging this vast infrastructure footprint, cable operators are able to provide communications services to business of all sizes. Insight Research Corp. estimates that cable operators’ business-service revenue topped $7 billion in 2012. Their networks include high-capacity metro fiber rings, fiber access networks with deep reach into commercial areas, retail districts and residential neighborhoods. Depending on the location and business needs, fiber or coax connections are available to the customer premises.

Additionally, by owning and operating their networks and construction teams, cable operators may more quickly provision and better monitor services than can CLECs or ISPs that merely resell ILEC capacity. Through the broad reach of their networks, cable operators can also serve a wide range of locations, from office parks and business centers, to small office, branch office, retail, medical and municipal buildings. By comparison, reseller ISPs and CLECs are dependent on a competitor to install and provision services. This means they operate on ILEC schedules, rather than their own, and their network footprint is limited to the ILEC’s.

**Can You Say SLA?**

To enhance the resiliency and redundancy of their network connections—and to hedge against the cost of losses from connectivity interruptions—many businesses enter into a service level agreement (SLA) with their network and ISPs. These agreements set performance benchmarks for service reliability and, should an unplanned outage occur, responsiveness for repair and restoration.
Performance characteristics for an SLA may include total uptime for the connection, measured bandwidth and latency between defined IP access points. The availability of essential IP infrastructure, such as domain name servers (DNS) and dynamic host configuration protocol (DHCP) servers may also be specified. Should a problem arise, response and repair times are defined in the SLA, along with penalties for noncompliance.

It is important to understand that SLAs supplement, rather than replace, strategies for facilities-based IP access redundancy and resiliency in business continuity plans—particularly since SLAs typically exclude catastrophic interruptions, such as those caused by natural disasters or acts of war.

**Moving to Multihoming**

After installing diverse or redundant connections for IP access, businesses need a method to switch from one network route to the other should a service interruption occur. Multihoming provides this automatic failover function among Internet connections as well as other benefits.

A multihoming approach frequently employed by larger businesses is Border Gateway Protocol (BGP). A common Internet routing protocol, BGP supports redundant routes for traffic flows to and from a business location. The challenge is that the effective use of BGP requires close technical collaboration with competing ISPs, as well as internal IT staff or consultants with the expertise to handle complex router configurations.

Fortunately, a number of vendors offer network appliances—essentially purpose-built routers and switches—that may simplify multihoming implementations, giving small and midsize businesses Internet access redundancy through virtually any type of connection or service provider. Additionally, many of these solutions offer load-balancing capabilities, allowing traffic to be directed across multiple connections to ensure adequate bandwidth is available for everyday operations.

**Ready for Disaster**

Enterprise planning for business continuity and disaster recovery are closely linked. As the names imply, the goal of a business continuity plan is to prevent interruptions to operations, while a disaster recovery plan is aimed at restoring operations following an ordinary or catastrophic disruption. Redundant facilities-based Internet connections are an essential support for both.

Offsite data storage and backup are at the heart of most disaster recovery plans. Historically, critical enterprise data has been backed up on drives and discs and physically transported to alternate locations for safe storage. Increasingly, however, businesses of all sizes are storing and backing up data through the cloud. This way, regularly scheduled backups are performed automatically to remote servers through a company’s secure Internet connection. However, should a data loss occur in a disaster
scenario, businesses must be able to connect to the Internet to remotely access and download their backed-up data. Clearly, continuous availability of IP network access is essential for regular cloud data backup as well as retrieval following a disaster.

Some service providers integrate cloud storage and backup offerings with access solutions. For example, Time Warner Cable Business Class offers facilities-based Internet access and network services with a diverse path from the ILEC, as well as cloud services for businesses of all sizes in collaboration with NaviSite Inc., also a division of Time Warner Cable.

Companies can take their business continuity and disaster recovery strategies further with remote access solutions. After a disaster, buildings and facilities may be damaged or unavailable, sometimes for extended periods of time. Thus, employees must be able to work remotely for business operations to continue. Since working from home is often the optimal solution, a service provider that can provision facilities-based broadband Internet connections to both business and residential locations is an attractive solution. Many cable operators offer teleworker access with centralized administration, billing and support for residential broadband service.

**Deploying Different Baskets**

Last-mile diversity and Internet access redundancy are essential to ensuring business continuity in today’s networked economy. When selecting service providers, choose reliable and diverse network solutions that can be efficiently configured to support your business continuity needs. Carefully investigate the network infrastructure of prospective providers to ensure they use different facilities, reducing risk from a single point of failure. Find out if they can rapidly scale capacity to deliver extra bandwidth when your business needs it most. And, consider a provider that can deliver cloud-based backup, storage and alternate site support. This way you can be sure your eggs are in different baskets.
About the Author
Michael Harris is principal consultant at Phoenix, Arizona-based Kinetic Strategies, Inc. Applying more than 15 years of experience as a strategist, research analyst and journalist, Michael consults with select clients in the networking, Internet and telecommunications industries.

About Time Warner Cable Business Class
Time Warner Cable Business Class, a division of Time Warner Cable (NYSE: TWC), offers a full complement of business communications tools to small, medium and enterprise sized companies. Its phone, Internet, Voice, Television, Network Services and Cloud Services are enhanced by award-winning customer service and local support teams. It serves approximately 500,000 business customers throughout Time Warner Cable’s markets.

5 “Cable TV Enterprise Services, 2012-2017,” Insight Research Corp.