

White Paper

Business Continuity: Proactive Telecom Strategies for Decision Makers

Build Smarter Networks



Table of Contents

1. Executive Summary.....	3
2. Overview of the Problem	3
3. Wired Strategies for Redundant Access	4
4. Wireless Strategies for Redundant Access	4
5. Equipment Selection.....	4
6. Return on Investment versus Downtime-related Losses.....	5
7. Conclusion	6

1. Executive Summary

Most organizations have created a dependency on the ability to access the Internet for information searches, financial transactions, customer interaction, value proposition delivery and much more. Law firms need to be able to review cases quickly, merchants require instant transaction processing, hotel guests need to stay in touch with work and home, and doctors need to consult medical databases. Without this connectivity, any organization can suffer operational and financial losses which could be averted through strategy and planning.

2. Overview of the Problem

Internet links will sooner or later be unavailable, since multiple points of failure are present in any organizational network and any carrier infrastructure. According to research by Infonetix Research, organizations need to assume that their links will fail for some period of time every year, where 99.5% reliability results in nearly 2 days of downtime. This amount of downtime may lead to an array of consequences depending on the type of organization, from mild productivity drops to significant losses of business related to the unavailability of systems required to perform transactions.

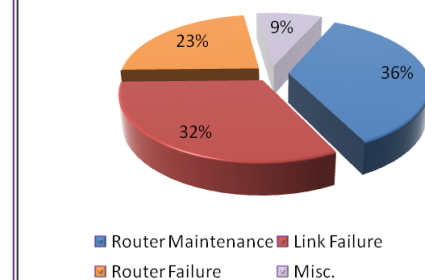
Average hard downtime per month ⁽¹⁾

Average hard downtime per month	1.7 outages
Average duration per hard downtime	67 minutes
Average total hard downtime per year	23 hours
Average percent of employees affected	28% of employees

Sources for these issues are varied and start within the organization's network and commonly end at the ISP's infrastructure. Here is a list of common failure points:

- **On-premise equipment:** Routers and firewalls, like any other piece of equipment, are subject to failure, either through software defects or physical defects such as mainboards or power supplies.
- **Physical carrier networks:** Interventions by utilities are normally planned with the network diagrams of carriers, but site crews may sever the fibers connecting the customer to the central office (CO), causing severe downtime periods until the fibers are repaired or replaced.
- **Central office equipment:** Equipment installed at the carrier's central offices (COs, where local connections join the carrier's network) is designed for reliability, and uptime but is still subject to defects or physical damage relative to the hosting environment.
- **Human intervention:** Human errors and system maintenance are common causes of downtime. While applying the remedy can be fairly quick, locating the trouble can prove to be time-consuming.

Contributions to Network Downtime ⁽²⁾



3. Wired Strategies for Redundant Access

While planning an organization's WAN architecture, diversification is the key to success. When keeping a single source supply chain, a planner exposes his organization to the potential points of failure described in section 2 above.

Diversification can happen at multiple levels:

- **Utilization of multiple ISP carriers:** Combining multiple carriers utilizing multiple carrier technologies significantly reduces the risk of downtime. With multiple routers, different CO connection points and physical carrier networks, should a failure occur, other systems are in place to compensate to avert downtime.
- **Multiple COs:** When using multiple carriers, a good practice is to utilize multiple COs to prevent failure. A common easy and affordable way of reaching this goal is with multiple carrier technologies. Using a selection of telco, cable, utility and fixed wireless providers will significantly reduce the risks of managing downtime since they have separate physical networks.

With multiple concurrent providers utilizing different technologies and different COs, an organization can prevent downtime almost completely, while human error remains a key component to manage.

Alternative carriers using fixed wireless technologies have been making significant inroads in the past few years and are offering viable alternatives, where they will connect a site to one of their endpoints. Their carrier links require line of sight access from the building to the access point, which can be up to 14 miles/22 kilometers away. Performance can range from 1.5Mbps to 100Mbps depending on technologies and carrier offerings.

4. Wireless strategies for Redundant Access

Wireless networks have become quite attractive for planning uptime strategy. Carriers are providing more options with reasonable throughput to ensure that a network will have a reasonable link for emergency conditions.

Key technologies currently available for use to ensure uptime:

- **3G Mobile Networks:** Commonly available IP links from mobile carriers can be a viable temporary solution during outages. Low upload speeds and potentially costly pricing plans discourage organizations in most regions from making this a permanent choice, and most carriers do not allocate static IP addresses to these links.
- **4G Networks (WiMAX and LTE):** Carriers offering these types of access are becoming more available as rollouts enable availability and faster throughput. Some carriers offer permanent links with static IP addresses which provide a key alternative technology for maximal uptime strategies.

5. Equipment Selection

The equipment selected to deliver a bandwidth-based project for optimal continuity will prove to be critical. The classic tool for connecting bandwidth is a router, and it has been performing failover tasks well but its range of functions can be limited to provide the best results. Link balancers are, in

most cases, better suited to delivering these projects, where they can add incremental value to the organization with the following items:

- **ISP independence:** Organizations are no longer tied to a single provider or carrier technology, thus making diversification quite easy.
- **Low-cost alternatives:** Most link balancers should be able to support any type of IP link, including low-cost carriers which offer viable solutions to the topics discussed in section 3 above.
- **Seamless failover:** With the proper rules in place, failover for bandwidth is easily achieved, and rules can be applied based on available ISPs and service criticality. Also, quality of service (QoS) can complement this process to ensure optimal bandwidth distribution.

The physical aspect of these products needs to be addressed as well, simply because equipment can fail or lose power. To remedy this strategic point of failure, two options are available:

- **Failover units:** In this context, a primary link balancer will be handling traffic management operations and a second will be monitoring the first. Should the primary unit cease to function normally; the second unit will take over and continue operations.
- **Bypass ports:** This option is quite attractive for organizations with limited budgets. Should the unit cease to operate and lose power, two ports will act as a “pass-through” to reconnect an ISP link to the gateway (firewall or other device). While this function is running, no balancing feature will be used, but traffic will continue to be processed. Layer-2 based link balancers offer this type of functionality, Layer-4 devices cannot permit this.

6. Geographic Solutions

When planning business continuity for multiple sites, options are available to ensure continual operations when one or more ISP circuits are unavailable or damaged. Two common scenarios can be addressed easily to prevent downtime:

- 1- **Geographic balancing:** By connecting two or more sites and performing DNS reconfigurations, these sites can share the load or act as a failover for business continuity or disaster contingencies. Link balancers are well suited to this task as DNS-based approaches offer much improved performance over BGP strategies for responsiveness and failover times.
- 2- **Site to site applications:** The two most common site to site deployments of applications are VoIP and VPNs. When an ISP fails or becomes congested, service suffers accordingly. Link balancers provide a valuable approach to this situation by utilizing multiple carriers on each end point to multiplex the point to point application, so when there is a service interruption, the application operates normally.

7. Return on Investment versus Downtime-related Losses

Since every organization is different, this metric can be either simple or complex to measure. Key items commonly used to determine the return on investment of a bandwidth improvement should include:

- Number of outages in the last year with duration
- Number of significantly degraded periods in the last year
- Financial losses/lost sales due to downtime
- Average productivity losses per employee per outage
- Metric for existing links before and after implementation.

Elfiq offers a free ROI calculation tool at www.elfiq.com, so organizations can start building estimates based on these calculations.

8. Conclusion

Internet access has become a critical business asset which most organizations depend on to deliver their value proposition. While its value is clearly understood, many organizations do not understand fully their connectivity situation and how to plan for contingencies.

With a strong understanding of key assets and providers, a plan can be devised which will ensure constant Internet access and guarantee the organization continuous normal operations through which a greater level of profitability can be achieved.

Produced by Elfiq Networks

Elfiq Networks is a technology leader and innovator in the field of WAN link management and balancing. With successful installations in over 50 countries, Elfiq's Link Balancer products help organizations of any type and size perform more competitively every day with the ability to use multiple Internet and private links easily and securely.

For more information on Elfiq Networks' products and technologies, please contact:

Elfiq Networks
1155 University, #712
Montreal, Quebec, H3B 3A7
Canada
Telephone: 888-GO-ELFIQ / 514-667-0611
Internet: www.elfiq.com
Email: info@elfiq.com

1,2: The Costs of Downtime: North American Medium Businesses 2006, Infonetics Research, March 2006.

May 2009

© Copyright 2009, Elfiq Networks (Elfiq Inc.). The contents of this document are protected by copyright. Any modification of this document, in any shape or form, is prohibited. Any redistribution, publication or derivation of the contents of this document without written authorization from Elfiq is also prohibited. All rights reserved.