White Paper

Making Email Resilient through Telecommunications

Build Smarter Networks

ELFIQ NETWORKS

Table of Contents

1. Executive Summary

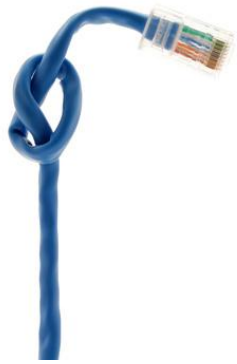
Since the explosion of the Internet, email has become an essential business tool for conducting normal communications, similar to telephone conversations and faxes. In some business environments, email has become the dominant form of communication with customers and partners.

With this reliance on email come user expectations of availability and near-instantaneous transmission of communications at all levels of the organization. With the emergence of smartphones in recent years, this business service has become positively vital, and should it be unavailable, it can have serious consequences on the ability to conduct normal business.

2. Overview of the Problem

Corporate users depend on email to conduct normal business daily activities; in 2006 the average user received 126 emails per day.[2] According to the Radicati Group, users are expected to spend up to 41% of their work time managing email messages.[2] With this type of organizational dependence, organizations feel the pain of downtime from a cost perspective, where customer requests and content delivery are delayed, with employee productivity suffering from "the Internet is down water cooler effect".

Email depends on a few specific systems, which can be implemented locally, at another site or outsourced to a service provider for a monthly fee. All these scenarios have the same core point of access: the Internet. Remove Internet access and email systems become completely paralyzed. "Software as a Service" (SaaS) providers such as Google (GMail) are also susceptible to downtime as shown by the documented outages that hit users in 2009. When smartphone users lose their connection to the office, it becomes problematic at all levels of the organization.

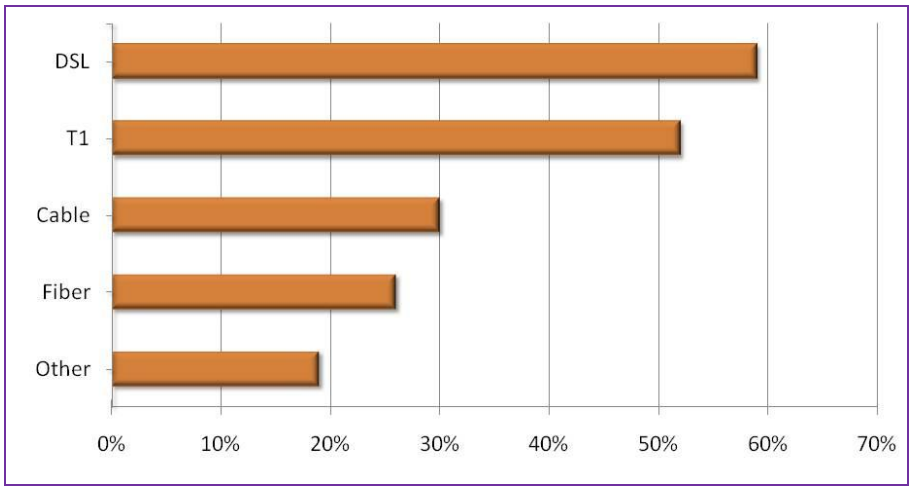


In the case of client-based email users, they can store emails locally until service is re-established. In the case of Web-based email services, when the Internet is not available, the entire system is inaccessible to users.

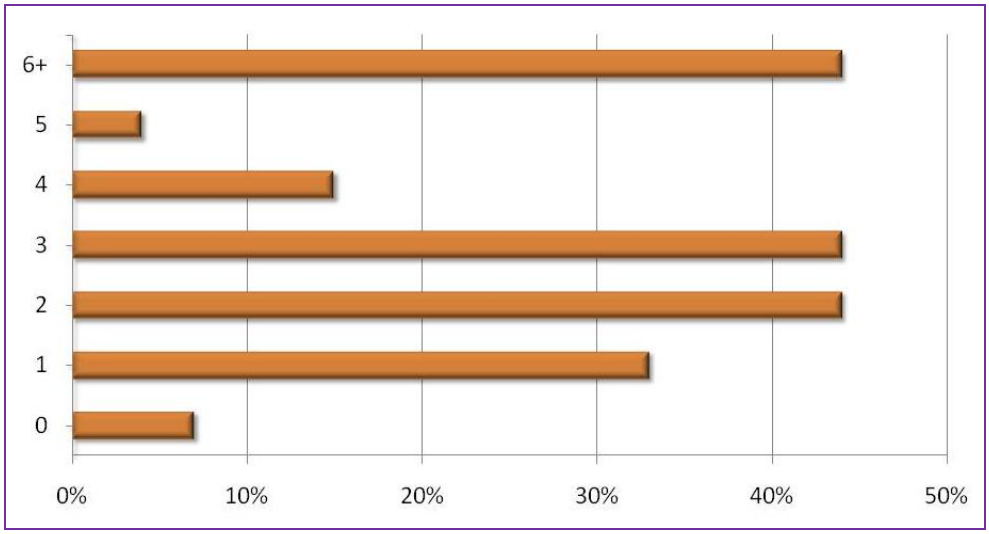
The most common source of email issues from a telecommunications perspective is the fact that most organizations rely on a single Internet service provider (ISP), and service is the core of the problem. Such deployments are susceptible to carrier outages and equipment failures which will cause downtime. According to a report by Dell, [4] **8% of email outages are related to connectivity issues.**

The following metrics outline what organizations are experiencing with their carrier services:

- Elfiq Networks customer survey: technology failure rate experienced within 12 months (2009):[3]



- Elfiq Networks customer survey: number of carrier failures within 12 months (2009):[3]



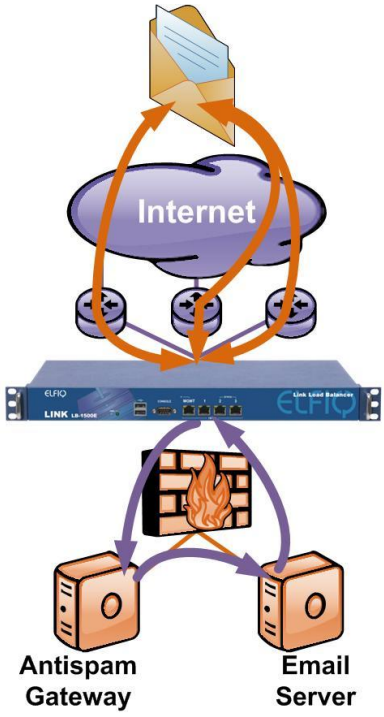
- Infonetics Research monthly downtime expectations (2006):[1]

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

3. Resilient Email for a Single Site

One of the most rapidly expanding methods of guaranteeing email resilience is the use of Link Balancers. They are network-based devices which enable the use of multiple concurrent ISPs for maximum uptime and performance. The mindset behind this approach is to use multiple concurrent ISPs that will provide greater resiliency should bandwidth providers and technologies be selected appropriately (www.elfiq.com/bandwidthdiversification). When a carrier is unavailable, at least one

Two primary scenarios need to be handled for email traffic with other will be present to provide a failover process and maintain connectivity.regard to bandwidth: outbound email and inbound email. For outbound emails leaving the organization, the Link Balancer will utilize the preferred ISP carrier based on policies defined by the organization to process those requests. Should the preferred carrier be unavailable, an alternative link will be selected to deliver the mail to the next hop.



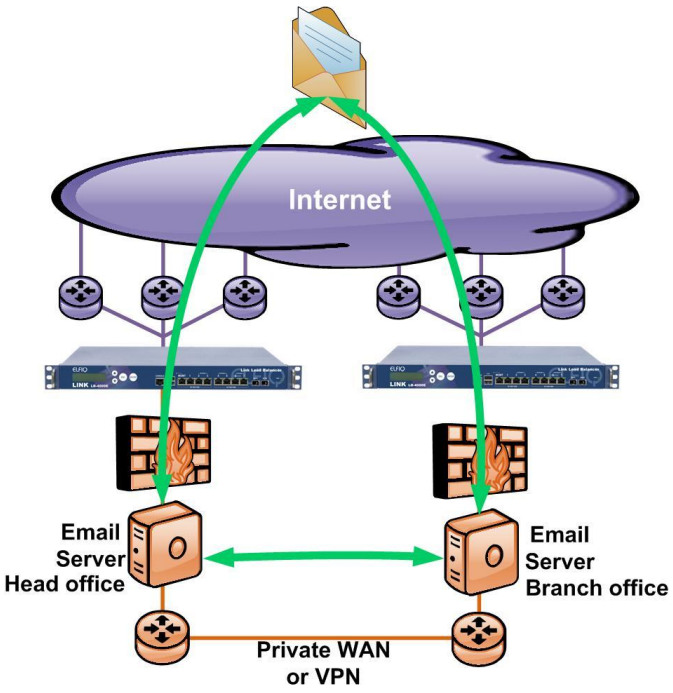
For inbound email, Link Balancers add a significant ability to any network: the ability to balance inbound traffic across multiple carriers. The process is managed through DNS modifications, where the A records on the DNS server will need to be supplemented by NS records for each MX entry. With this approach, not only can the Link Balancer provide a failover for the inbound email traffic, but the Link Balancer can distribute inbound email traffic on selected carriers based on policies and selected balancing algorithms to effectively increase performance and prevent the use of saturated links. The process for inbound traffic is documented in detail at www.elfiq.com/idns.

Link Balancers can deliver incremental benefits to the email management process through these capabilities:

- Traffic segmentation: Link Balancers can handle different traffic types on specific links so the traffic will be optimally distributed as per policies and preferences.
- Quality of Service (QoS): Link Balancers can reserve and/or limit the bandwidth used for specific services to ensure optimal use of bandwidth and prevent service degradation through abuse.
- Server verification: Some Link Balancers can verify the status of a server or service prior to passing traffic; this is useful in case an antispam relay or one of many servers fails to operate normally.

4. Resilient Email for Multiple Sites

In organizations with multiple offices, the same issues can occur and prevent normal email service operations. To strengthen resiliency, the Link Balancer approach can provide an extra level of resiliency to ensure maximum availability. The following diagram outlines a common scenario that has been deployed at a significant number of organizations.



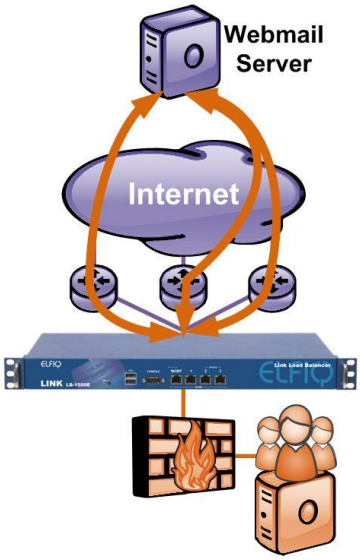
In the case where each site has its own email server, they are interconnected via private WAN link or a VPN tunnel. To prevent network outages, strategies can be implemented involving concepts such as:

- Geographic balancing: Should a site lose its connection to the Internet for SMTP transfers, it can rely on another site's connectivity to send and receive email. (Business Continuity White paper at www.elfiq.com/whitepapers)
- VPN multiplexing: Using multiple ISP carriers, organizations can prevent site outages by multiplexing multiple carrier links. (VPN White Paper at www.elfiq.com/whitepapers)

For sites that are all interconnected with only one central email server for all users and locations, the VPN multiplexing approach discussed above will similarly deliver significant benefits.

5. Hosted Email Deployments

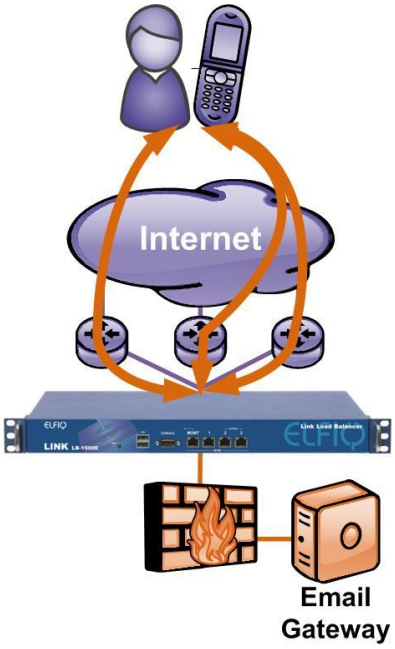
In recent years, many organizations have migrated from internal email servers to hosted email environments for the sake of simplification and cost reduction. In this context, dependence on bandwidth is critical. Should the location lose access to the Internet, it will lose access to email distribution capabilities.



Organizations need to plan for this contingency to ensure that communications are always available. This type of project also delivers benefits to any IP services at the location.

6. Webmail and Smartphone Deployments

Many organizations offer Web-based access to their email services, and their mobile force is likely to utilize smartphones to stay connected to the organization. Smartphone users are always expecting this service to be available, and their dependence ranges from very high to critical since they operate in the field and their roles are often time-sensitive. In December 2009, the BlackBerry network suffered two outages which caused major business disruptions to these users.



To plan for this scenario, the inbound balancing of services for Webmail and smartphone access will prove to provide a rapid return on investment as reliance on carriers is no longer a strategic point of failure. For more information on inbound balancing see www.elfiq.com/idns.

7. Conclusion

Email is a critical business communication asset that any organization, regardless of size, vertical or geography, depends on. From a telecommunications perspective, the strategic point of failure is how carrier services are managed.

Link Balancers enable organizations to break away from a single point of failure in terms of Internet-based service access and to boost performance by balancing inbound and outbound traffic for optimal access to email. This approach means organizations will no longer suffer outages that will cost time, productivity and, most importantly, business transactions.

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 60 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

References:

1: *The Costs of Downtime: North American Medium Businesses 2006*, Infonetics Research, March 2006.
2: *Addressing Information Overload in Corporate Email*, Radicati Group Inc., April 2007
3: Elfiq 2009 Customer Survey, www.elfiq.com/customersatisfaction
4: Dell Email Downtime Risk Assessment, 2009

January 2010