Internet Performance during Disasters: Theory and Practice

Executive Summary

- The Internet is not a centralized or monolithic system, but rather a connection of independently managed redundant networks.
- The Internet does not "go down" during disasters, but rather local connectivity can be disrupted.
- Local Internet connectivity has proven robust in recent disasters, and has been the "lifeline" in many cases as the only remaining channel of communication.
- To ensure reliable connectivity, organizations need to provide multiple independent connections to the Internet. Service providers offer many products to ensure reliable connectivity, from self healing local ring networks to wireless and satellite backup connections.

Introduction

Disasters, by their very nature, are largely unexpected and unavoidable events. Perhaps the only thing we know about them with certainty is that they will create a powerful need for reliable communication, coordination, and information. But what happens when the disaster is so severe that traditional communications methods are compromised?

More than ever, the Internet is playing a role in all phases of emergency information management: before, during, and after. As both an information network and communication system, the Internet can be a lifeline during disaster situations (as shown by the quotation at right). Increasingly, it is being used to help manage crises, but how effectively is it serving this role?

> "All the phone lines were overloaded; even the mobile phones were not working. It soon became apparent that the only reliable working telecommunication medium was the Internet. As a consequence, it became the medium of choice for informing volunteers and nongovernmental organizations (NGOs), both nationally and internationally, about the needs of the earthquake region."
>
> Zincir-Heywood and Heywood, 2000. "In the Wake of the Turkish Earthquake: Turkish Internet," Proceedings of the Internet Society's iNet 2000 conference.

This paper discusses how and why the Internet is well suited to supporting disaster management efforts. It begins with a brief history of the Internet and an overview of its current "design." The paper then reviews the status of the Internet in recent disasters, concluding with recommendations for facilities to ensure that they have ready Internet access for the next disaster.

A Brief History of the Internet: A Network to Survive a Nuclear War

In 1962, the US Air Force commissioned the RAND Corporation to study how the United States could maintain its command and control over its missiles and bombers in the event of a nuclear attack. It envisioned a military network that could survive a nuclear strike, decentralized so that if any locations (cities) in the U.S. were attacked, the military could still have control of nuclear arms for a counter-attack.

RAND's final report outlined several ways to meet this objective, including a packet switched network. In a packet switched network, data (documents, files, and voice) is broken down into "packets" that can be sent from one computer to another and reassembled by the computer at the other end. Each packet is labeled with a "to" and "from," and can be resent continually should one packet not reach its destination.

> The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for the Department of Defense (DoD). It manages and directs selected basic and applied research and development projects for DoD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions. (http://www.darpa.mil/)

As part of a separate effort, in 1968 the US Defense Advanced Research Projects Agency (DARPA) awarded the ARPANET contract to BBN. A physical network was constructed in 1969, linking four nodes. In 1973, DARPA began to investigate protocols that allowed networked computers to communicate seamlessly across multiple, linked packet networks (the "Internetting" project). The system of networks that emerged from the research was known as the "Internet." In 1986, the National Science Foundation funded NSFNet as a cross country 56 Kbps backbone for the Internet. They maintained their sponsorship for nearly a decade, setting rules for its non-commercial government and research uses.[1]

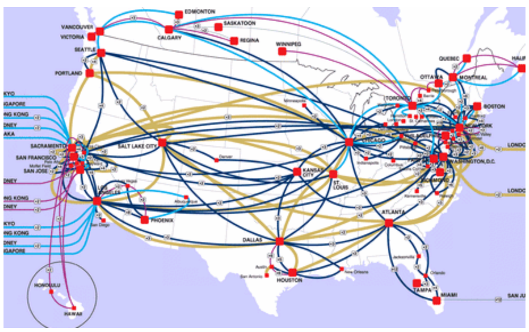
When independent commercial networks began to grow in the early 90's, it became possible to route traffic across the country from one commercial site to another without passing through the government funded NSFNet Internet backbone. In May 1995, the NSF ended its sponsorship of the Internet backbone, and all traffic began to rely primarily on commercial networks. AOL, Prodigy, and CompuServe entered the scene.

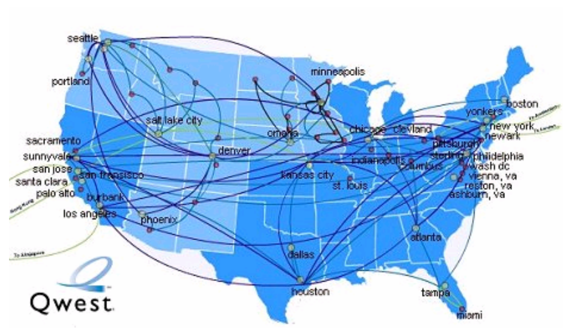
[1] The early Internet was very user "unfriendly" and used almost exclusively by computer experts, engineers, scientists, and librarians who cataloged their university holdings. In 1989, a team at CERN proposed a new protocol for information distribution. This protocol, based on a system of embedding links in text that linked to other text (a.k.a. "hypertext"), eventually became the World Wide Web in 1991. Browsers followed, beginning with Mosaic, Netscape Navigator, Microsoft's Internet Explorer, and now Firefox (to name just a few).

The Internet Today: “Designed” for Redundancy

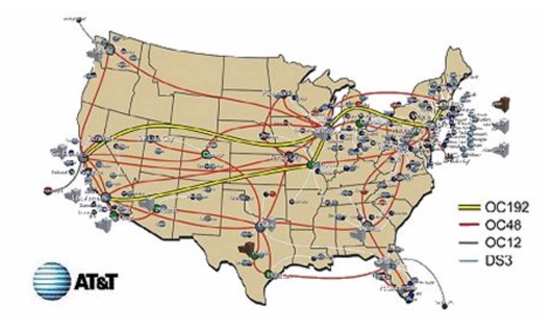
Today, the Internet is a worldwide collection of networks (called Autonomous Systems, or ASes), operated by approximately 16,000 Internet service providers (ISPs). This interlocking system of networks includes multinational telecommunications carriers (see four example backbone networks, below), cable companies, corporate networks, nonprofit-organization networks, government-agency networks, and even home networks. Each network consists of a set of optical-fiber, copper-circuit, or wireless communications links that connect to “end-hosts” (e.g., desktop personal computers or servers that provide Web content) and routers that control the paths taken by data packets between the “end-hosts”.

Four Interconnected “Backbone” Networks

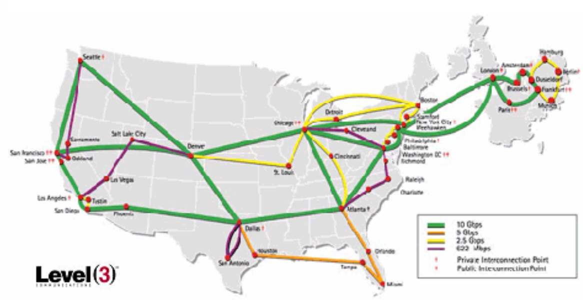

UUNET(MCI)'s OC-192 IP Backbone Network



The Qwest Network



AT&T’s OC48/OC-192 IP Backbone Network


Level 3 Internet Backbone[2]

[2] All images and network descriptions can be found at http://www.cybercon.com/tour_network-b.html.

Local Internet access may be provided through a number of different companies employing various technologies, including integrated services digital network (ISDN), DSL, T-1, cable modem, wireless, and SONET fiber. Finally, there's the old-fashioned way[3]: dial-up customers use the LEC local network to place phone calls to modems operated by their ISPs.

Every autonomous system owns a number of border BGP[4] routers that are connected to its own internal network as well as border routers of neighboring networks. The BGP routers of neighboring networks manage the traffic to route each information packet to its final destination efficiently. Each network asks its neighbors if they can pass the packets of information along towards their destination. If one neighbor is not available, the network will ask someone else to pass along the message, until all packets reach and are reassembled on the other end. As a result, the Internet is dynamically adjusting the routes that packets follow through the connected networks in response to changes in the networks (e.g., failures of communications links). Even under normal conditions, Internet routing patterns are continually adapting to changing availability of networks. This "re-routing" is increased in disaster situations where some networks may be damaged.

Can the Internet "Go Down?"

Of course, the redundancy of the Internet does have some limits. That is, there are a finite number of paths that connect any given point to the rest of the system.[5] As a result, the Internet connection points or cables could be sufficiently damaged that the interconnected networks could be split apart; essentially a location could be "cut off" from the rest of the Internet. Alternatively, the number of interconnections could be reduced to such a point that the remaining connections cannot accommodate the traffic that was previously dispersed through the other connections. When some links are damaged, new routes are constructed by the BGP routers to bypass the failed connection points. However, in many cases, the backup paths are of lower bandwidth. Lower capacity connections can lead to increased network congestion and slower transmission times.

---

[3] In 1965, Lawrence Roberts of MIT connected a Massachusetts computer with a California computer over dial-up telephone lines, one of the first recorded dial-up connections.

[4] BGP (Border Gateway Protocol) is a software protocol that is running on the border routers. Basically, BGP routers tell their neighbors what they see as the best routes to the networks of which they are aware. By compiling such information from all neighbor BGP routers, a BGP router directs traffic to one neighbor that then passes it along to the next router, until the packets reach their final destination.

[5] The economics of deploying cables as well as geographic barriers result in some locations having a high concentration of Internet facilities while others have only a few.

The Internet during Disasters: Actual Experiences

So how has all this redundancy held up in practice?

Humble Beginnings: 1995 Earthquake in Kobe, Japan

Within days of the 1995 earthquake in Kobe, Japan, messages and images traveled around the world through e-mail, discussion groups, and both news media and homegrown Web sites. But Japanese researchers reported that, during relief and recovery activities, "the Internet and other computer networks did not function as we expected" because of technical difficulties and limitations in the media's news distribution systems. Yet, those same researchers stated that, with time and effort, the Internet had the potential to become an "information lifeline" in emergency situations (Shinoda et al, 1996).

September 11th, 2001 Attacks

After the terrible attacks of September 11, 2001, the Computer Science and Telecommunications Board (CSTB) of the National Research Council formed the Committee on the Internet under Crisis Conditions. This committee gathered data and accounts of experiences relating to the Internet's performance that day and offered conclusions about preparing for and responding to future emergencies.

> **"The events of September 11 had little effect on Internet services as a whole. The network displayed considerable flexibility that underscored its adaptability in the face of infrastructure damage imposed by the crisis."**
>
> ***Computer Science and Telecommunications Board (CSTB) of the National Research Council***

The full published report, The Internet under Crisis Conditions: Learning from September 11, is over 80 pages.[6] Overall, the report concluded that, while localized physical damage occurred to one of the Internet's most important hubs, the Internet was not seriously affected by the attacks. Automatic rerouting allowed traffic to bypass many of the damaged parts, and system reconfiguration or rapid deployment of new equipment resolved most of the remaining problems. These actions highlight the flexibility of the network's design; significantly, the responses required no central coordination.

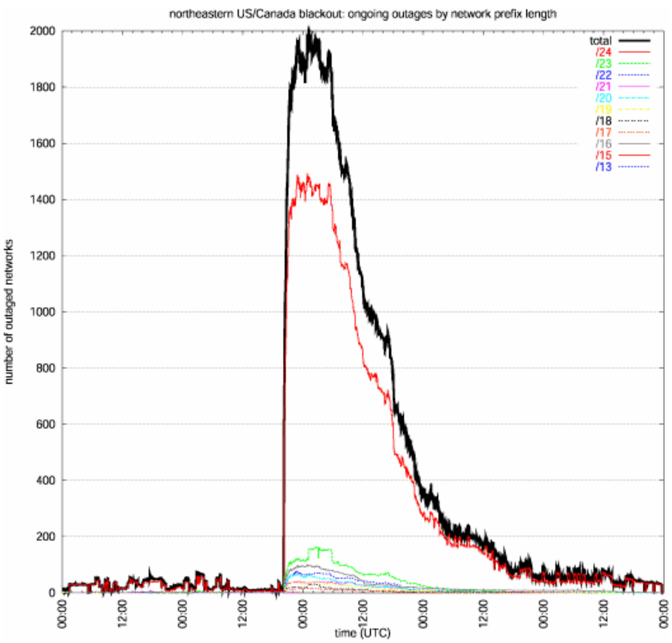
Connectivity recovered quickly and the loss was less severe that seen in other incidents affecting the Internet. Other communications media, such a cellular telephone service in greater New York experienced much greater stress.

> Instant messaging became one of the stars in the early hours after the attack as consumers and businesses corresponded one-to-one when phone lines quit working in part of New York City. **America Online reported that 1.2 billion messages were sent via instant messaging and on AOL's proprietary client software on September 11 alone.**
> -- ***Heavy Online Usage during Crisis*** by Rob Spiegel[7]

[6] http://darwin.nap.edu/books/0309087023/html.
[7] Online version available at http://www.businessknowhow.com/Editorials/netcrisis.htm.

Northeastern Blackout of 2003

Starting on August 13, 2003, power blackouts spread across the northeastern U.S. and Canada, ultimately affecting 50 million people. While backbone networks remained intact using emergency power supplies, many regional and corporate networks were unreachable.

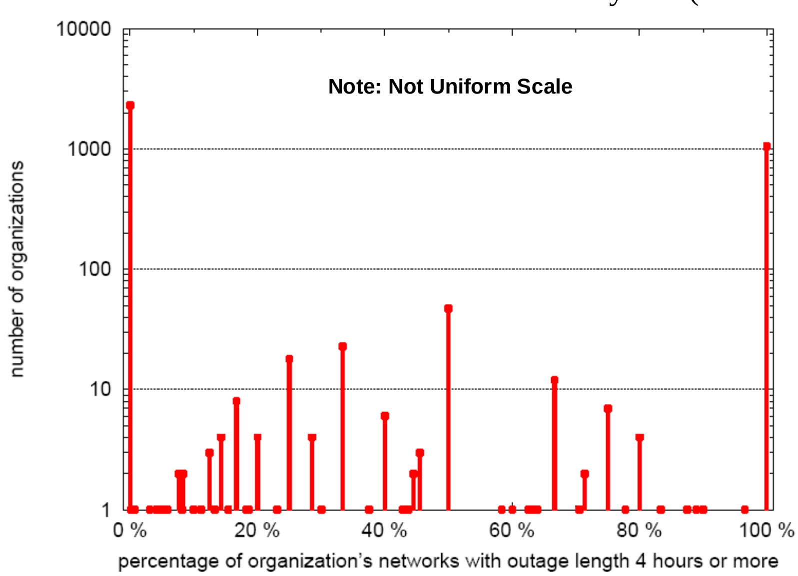


Concurrently Ongoing Network Outages in the Blackout Area
Source: Renesys.

According to Renesys estimates[8], on August 14, 2003 there were over 9,700 globally advertised networks in the geographic area affected by the northeastern blackout. Renesys calculates that only 33% (3,175) of these networks suffered from abnormal connectivity outages, with over 2,000 networks suffering severe connectivity outages for longer than 4 hours and over 1,400 networks for longer than 12 hours.

On an organizational basis, Renesys estimates that, though more than 1,000 organizations were unreachable by the Internet for more than 4 hours, more than twice that many (2321 organizations) had none of their networks out for more than 4 hours.

As discussed below, organizations advertising larger numbers of networks tended to be more resilient to the power outage.



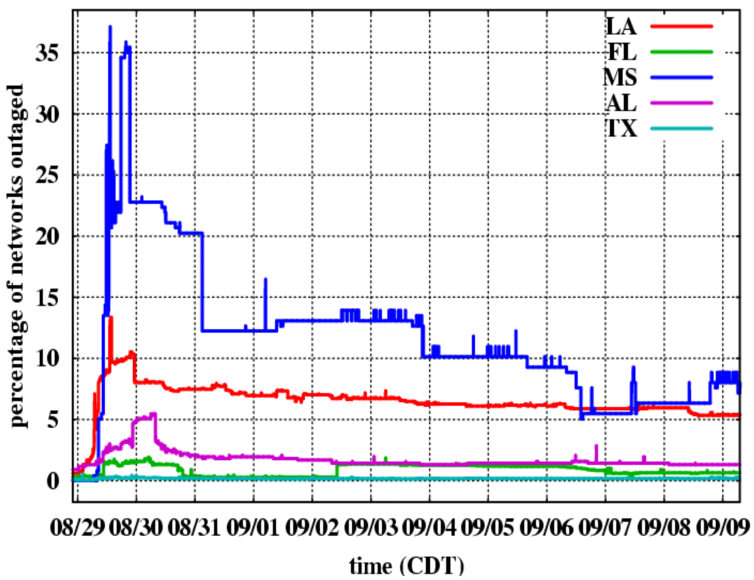
Source: Renesys.

[8] Cowie, J., Ogielski, A., Premore, B., Smith, E. and Underwood, T. ***"Impact of the 2003 Blackouts on Internet Communications."*** http://www.renesys.com/resource_library/Renesys_BlackoutReport.pdf, November 2003.

Hurricane Katrina

Katrina was one of the strongest storms to impact the coast of the United States in the last 100 years. With sustained winds during landfall of 125 mph and minimum central pressure (the third lowest on record at landfall), Katrina caused widespread devastation along the central Gulf Coast states of the US.

In the hours after Katrina's landfall, both Louisiana and Mississippi suffered a significant loss of Internet access. As shown in the chart below,[9] Alabama and Florida were also affected measurably, though to much lesser degrees.



Impact of Katrina on Globally Routed Networks in the Affected Region
Source: Renesys.

The chart at left shows that, at the second landfall at the Louisiana border (approximately 10am CDT, 8/29/05), ***86% of the networks that Renesys geolocates in Louisiana were experiencing no loss of connectivity.*** In Mississippi, 62% of the networks showed no loss of connectivity.[10]

Of course, with a significant portion of the city of New Orleans under water and without reliable power, many Louisiana-based network outages continued for prolonged periods.

> "Operating on the power supplied by a back-up generator and with the availability of local phone service but no long distance, [Baton Rouge General Hospital] turned to technology to keep information flowing. Fortunately, the hospital still had its broadband Internet connection … The hospital ultimately used nine voice-over IP converters and wireless-enabled laptops with VoIP software installed for long distance communications and to set up a public branch exchange for communications within the hospital and sharing patient data."
>
> ***Internet Telephony Keeps Baton Rouge Hospital in Touch When Hurricane Hits*** by Corey McKenna
>
> GOVERNMENT TECHNOLOGY

[9] A full report is available at http://www.renesys.com/resource_library/Renesys-Katrina-Report-9sep2005.pdf.

[10] The actual number of affected networks in Mississippi was lower than in Louisiana, but the difference in percentage is due to the small number of normally available networks in Mississippi.

What Can I Do to Stay Connected in a Disaster?

This section outlines multiple approaches to maximizing your Internet availability in the event of a disaster. The appropriateness of these solutions for your organization depends on your organization's location, risk tolerance, and budget.

Shore Up Your Existing Connection Infrastructure

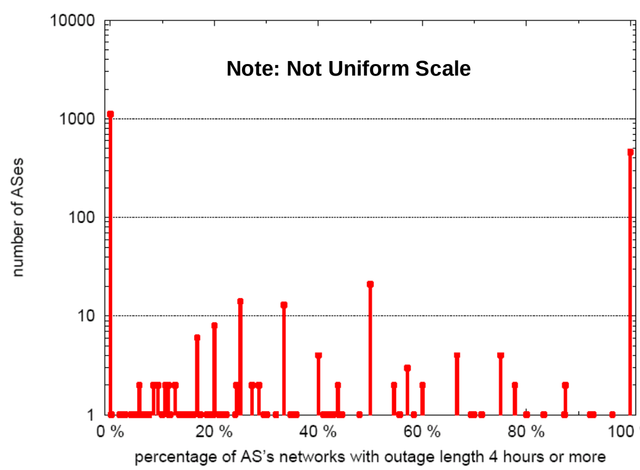
Perhaps the most important thing organizations can do to maximize their Internet connectivity is to assess their current infrastructure. That is, perform an end-to-end audit of Internet dependencies to see how your information packets move through your networks. By tracing these paths, some risk mitigation opportunities may present themselves. For example, one hospital, located in flood zone, hosted 166 servers in its basement. On the floor above, it had 6 hot tubs, each containing 1000 gallons of water.[11] This situation clearly presented an unacceptable risk, and changes were made to increase security of the servers. By assessing the current state of your organization's Internet architecture, your organization may be able to make some simple changes to maximize your chance of staying connected in a disaster.

Establish Multiple, Redundant Connections to the Internet

Once you've made corrections inside your organization, you should explore establishing redundant connections to the Internet (ideally with multiple carriers). If you can get on multiple carriers, then your chances all of your links to the Internet being severed simultaneously can be reduced. Even if your data has to go across the country and back via BGP routers, it can get through.

The chart at the right shows that there were 1,110 networks that had no outage of more than 4 hours in the Blackout of 2003. These were networks that largely had multiple connections to the Internet. On the other hand, the 460 networks that had outages of longer than 4 hours tended to be smaller organizations with few networks.

Having multiple networks, with multiple Internet connections improves the chances that your organization will stay online during a disaster.



Source: Renesys.

[11] Securing your Storage Assets by Drew Robb (July 12, 2004): http://www.enterpriseitplanet.com/storage/features/article.php/3379331

Explore Advanced Connection Types: Self-Healing Networks

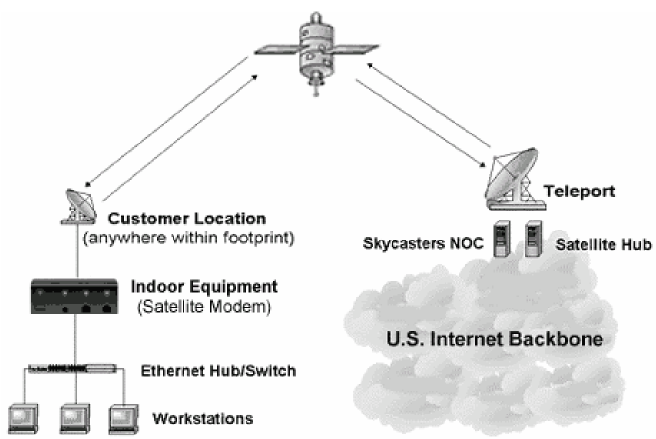
Today, many ISPs offer advanced connection options. For example, Qwest offers SONET Ring Service (SRS) and Self Healing Network Service (SHNS):

- SRS: "the ring topology of SRS continually monitors service quality, detects any failure or degradation and automatically self-heals around a point of failure via a protect path to ensure uninterrupted transmission flow. Rerouting is accomplished within 50 milliseconds."
- SHNS: "is a dedicated network using two concentric rings connecting multiple node locations with fiber optic cable pairs. A combination of fiber ring technology and a series of Intelligent Network Elements (INEs) allows SHNS to automatically detect network failures and reconfigure around them."[12]

Other ISPs may offer similar services in your area.

Wired, Wireless, and Satellite

Beyond wired connections, many organizations with backup power systems have begun to install wireless and satellite systems to mitigate the risk of being cut off by damaged land lines.



Source: www.skycasters.com

As with landlines, connectivity is priced based on bandwidth and connection speeds. Some companies provide secure DSL-equivalent speeds for around $149/month and full 2Mbps down/ 512Kpbs up for $479/month. Inaddition, other companies provide hardware for protecting the satellite dish from high winds and other debris.

> "Satellite Internet connectivity has advanced enough during the last year or so to allow a specialist to view highly detailed graphical information (x-rays or scans from MRI equipment) in a HIPAA compliant Internet environment that can be deemed "high speed". . . . [More] and more medical groups are seeing the benefits from this type of connection and adding satellite Internet "ground stations" at the remote homes of resident doctors, medical professionals like transcribers and smaller clinics they serve."
>
> **Remotely Connecting by Satellite to the Hospital – 2005**
> http://www.thunderhawk.com/broadband-Internet/11948.php

[12] For a more complete list of Qwest advanced offerings, see http://www.qwest.com/pcat/productList/1,1012,4_2-3,00.html?theStart=21&theEnd=40&indexLetter=&chooseRegion