the Availability Digest

www.availabilitydigest.com

The Fragile Internet

May 2009

As cloud computing looms overhead, the Internet will become ever more important to corporate well-being. It is already the lifeblood of hundreds of thousands of small online stores hosted by a variety of software-as-a-service providers. The importance of email services reaches into the largest enterprises.

The availability of Internet services is of paramount importance to these companies, and its importance only grows with time. If the Internet is down, so are the operations of many companies, large and small. The Internet's mesh architecture is designed to provide the extreme availability demanded by these users. After all, a fault anywhere in the Internet is automatically routed around; and service continues uninterrupted.

But is the Internet really all that reliable? Can you bet your company on the continuous availability of the Internet? Unfortunately, experience says "no." As Om Malik, a well-known technology writer, said, "Our Internet infrastructure … is as fragile as a fine porcelain cup on the roof of a car zipping across a pot-holed goat track."

Is this a well-founded statement? Indeed, a recent report by the Business Roundtable,[1] a consortium of CEOs of large U.S. companies, says that there is a 10% to 20% chance of a breakdown of our critical information infrastructure in the next ten years. They suggest that this breakdown could be brought about by malicious code, coding error, natural or man-made disasters, or attacks by terrorists or other adversaries.

We review here real-life outages that expose the frailty of the Internet and discuss some of the defensive measures that companies should consider to protect themselves from similar experiences.

What? No Internet?

Recorded Internet faults range from metropolitan outages to wide-area outages and on to global outages. It seems that no one, and no company, is totally safe from such misfortunes.

Global Outages

January 30, 2008 – Anchor Severs Internet Service Between North Africa and Europe

In our *Never Again* article entitled, What? No Internet? (*Availability Digest*, February, 2008), we told of a ship's dragging anchor that cut two cables at the bottom of the Mediterranean Sea on

[1] Gary Anthes, The Internet is Down – Now What?, Computing SA, http://mybroadband.co.xa/news/print/2674.html; January 28, 2008.

January 30, 2008, cutting off Internet service from North Africa, India, and the Middle East to the rest of the world. The outage lasted for several days and for several weeks in some cases. Coincidentally, two days later, another cable was cut by an anchor north of Dubai, disrupting service between the Middle East and parts of Asia.

This was not the first time that such a global Internet disaster had happened. In December, 2006, a magnitude 7.1 earthquake severed nine cables between Taiwan and the Philippines, cutting Internet and other communication services between southeast Asia and the rest of the world for seven weeks.

95% of all transoceanic communications are carried by submarine cables, the rest by satellite. Submarine cables carry the majority of Internet traffic between the Americas, Europe, the Middle East, and Asia. When a submarine cable breaks, it wrecks havoc on the operations of thousands of companies large and small. Would your company survive such an outage?

February 22, 2008 – Pakistan Blocks YouTube Around the Globe

The Internet is a highly structured set of interconnected networks. It comprises a network of *autonomous systems* (AS). An AS is a collection of networks controlled by a single entity, such as an ISP, a country, or a large corporation. Because of a capability of the Border Gateway Protocol (BGP) that is used to route global traffic between ASs, it is possible for a nefarious AS to hijack traffic to one or more web sites. It can do this by modifying routing tables in edge routers to redirect all traffic destined for a specific web site to a different "black hole" web site. This rerouting will be rapidly propagated through the global Internet, thus blocking all traffic to that site.[2]

This, in fact, happened to YouTube quite accidentally on February 22, 2008. Pakistan decided to redirect Pakistani YouTube traffic to a "black hole" via BGP hijacking because of what it perceived to be a blasphemous video clip. However, a simple mistake by an engineer at Pakistan Telecommunications Authority caused the redirection to be propagated throughout the entire Internet. YouTube was globally inaccessible for about two hours before the error was reported and corrected.

Other countries that have temporarily blocked access to YouTube include Turkey and Thailand. It could happen to you, accidentally or on purpose.

Wide-Area Outages

Global outages may be few and far between, but outages affecting large areas of a country are far more common. Following are some recent examples that show the variety of mishaps that can befall the Internet. They include a construction mishap, a power failure, and vandalism.

December 11, 2008 – Embarq and Verizon Customers Cut Off by Cable Cut in Southern Nevada

60,000 Embarq and Verizon customers throughout southern Nevada lost Internet and other communication services for up to two days when a construction equipment operator mistakenly cut through underground cables while digging a new sanitary sewage line. The backhoe broke through plastic and concrete conduit carrying copper wire and fiber cables. The accident interrupted Internet service, long-distance land-line service, and mobile service.

[2] Eavesdropping on the Internet, *Availability Digest*; March 2009.

February 1, 2009 – Major ISP Customers in Melbourne Downed by Power Failure

A Primus data center - a primary hub for several major ISPs serving customers in the Melbourne area and south to Tasmania - lost power due to a CitiPower substation fault. Though its battery UPS carried it for several minutes, its backup diesel generator failed to start. Hundreds of thousands of customers lost Internet services for sixteen hours.

Primus had a second backup site in Melbourne, but they elected not to transfer operations there because they felt that it would take longer to make the move than it would to restore power.

April 9, 2009 – Vandals Take Out Much of Silicon Valley

Thousands of businesses and individual users in Silicon Valley and the San Francisco area were without Internet, phone, and wireless services for more than twelve hours when vandals cut communication cables used by AT&T, Verizon, and Sprint. Cables were cut in two locations within a two-hour period. It turned out to be an easy operation. All the vandals had to do was to lift a manhole cover, climb down a ladder, and cut the cables.

Many configurations used by communication providers use a ring topology so that if a cable is cut, communication simply continues in the opposite direction. Evidently, these vandalized cables were either point-to-point, or the ring was otherwise disabled for maintenance. Though the perpetrators have yet to be caught, it is suspected that they may have been disgruntled employees since they seemed to have direct knowledge of which cables to cut.

Metropolitan Outages

February 18, 2009 - Router Takes Down London Network

A major network fault the morning of February 18th took thousands of customers offline for two hours. It was reported to be a router failure that precluded an alternate route from being established. Users were reduced to using modems over telephone lines.

The pain that was felt was well expressed by one blogger: “This is absolutely killing our sales office in London. We currently have an entire sales team crowded round a laptop fighting over access to a Vodafone dongle!”

April 6, 2009 – Could the London Olympics Be Next?

London is set to host the Summer Olympics in 2012. BT (British Telecom) is the official communication services provider for the Games, and it is determined to have a flawless operation during the Olympics. It predicts a data rate of six gigabytes per second. Even a few seconds of downtime could deprive the world of seeing a new record set.

On March 1, speaking at a conference in London, Stuart Hill, BT’s VP and director of BT 2012, said, “This is the most complex logistical peacetime challenge I think we’ve had to face. We have one spin of the circle … to make sure we’ve got it right.”

Good luck, Mr. Hill. A month after his talk, on Saturday afternoon, April 6th, contractors working on the Olympic site sent a large-thrust borer right through a deep BT tunnel, severing multiple fiber cables and shutting down Internet and other communication services for tens of thousands of customers.[3]

[3] Thanks to our reader, Rob Wickes, for pointing us to this story.

The cable tunnel was 32 meters (about 100 feet) below street level. The tunnel was completely blocked and unsafe. Its depth made it very difficult to repair the cables. They had to be pulled to the surface, repaired, and then routed through a new conduit.

BT was able to restore service to about 70% of the downed customers in two days, but 30% of the affected customers were still without Internet access for several more days.

Terrorism – Sometime in the Future?

Experts on communication security have pointed out that the most vulnerable point in a communication network is the central office. It is a hub and a single point of failure for a mass of communication links. If a terrorist were able to damage or destroy, for instance, Verizon's central office in lower Manhattan, communication service to the Wall Street area could be taken out for days or even weeks.[4]

For this reason, these facilities are heavily protected by security. We trust that we will not be reporting on such a disaster in the *Availability Digest*.

Summary

We ask again – could your company survive such an Internet outage? Are the procedures for such an outage incorporated into your business recovery plan? If not, now is the time to decide what you are going to do – not after the outage strikes.

As seen by the above examples, you could lose Internet access for hours, for days, even for weeks. Recovery planning could take several forms.

At the very least, to protect yourself against local outages, you should be connected to at least two points-of-presence (POPs) that are independent and separately routed. You should make sure that they do not use some common third-party carrier whose failure could affect both of your POPs.

You should make sure that your POPs are fault-tolerant, either because they are on a ring network or on a mesh network. You should insist on seeing a physical diagram of the providers' network paths to ensure that there are no single points of failure. No one should accept a failure due to point-to-point connections.

Another concern is network latency. If you are on the Internet, you have already accepted response times that are measured often in seconds. However, if your carrier can reroute around an outage and continue service, that rerouting could seriously increase your response times. When the Mediterranean Sea cables were cut, Internet access from North Africa to Europe was rerouted through the Middle East and Asia, across the Pacific Ocean and North America, across the Atlantic Ocean, and finally to Europe. Can you tolerate very slow response times? Will your applications time out and crash?

But what about wide-area or global Internet outages that cannot be restored by rerouting or for which rerouting causes such congestion that the Internet is useless to you? As we suggested in our What? No Internet? article, previously referenced, the first line of defense is a contingency plan to get reconnected to the Internet. One contemporary possibility is a satellite backup channel. The hours following a massive Internet failure is no time to try to negotiate backup channel capacity – there might not be any. There are several companies that offer satellite backup services, such as VSAT Systems (www.vsat-systems.com). Another is the FailSafe

[4] How secure is the U.S, communications network?, CNET News; April 13, 2009.

service from Ground Control (www.groundcontrol.com) that covers the contiguous 48 states in the U.S. via the Galileo geostationary satellite.

As a leading consultant said, "Our increasing dependence on the first 'w' in 'www' can undermine 'the best laid plans of mice and men,' to borrow a line that Robert Burns wrote in 1785."[5] Plan carefully and thoroughly to mitigate the problems that a major Internet outage will create for you.

Acknowledgements

In addition to references already given, material for this article was taken from the following sources:

Pakistan lifts the ban on YouTube, *BBC News*; February 26, 2008.
Construction mishap disrupts phones, *Las Vegas Review-Journal*; December 11, 2008.
Who's Really to Blame for 60,000 Lost Connections?, *American Fiber Systems*; December 11, 2008.
Melbourne blackout cripples Internet nationally, *APC Magazine*; February 1, 2009.
Sky network downed in London, *The Register*; February 18, 2009.
BT's Panic over 2012 London Olympics, *Business Week*; March 2, 2009.
Broadband outage hits tens of thousands in East London, *IT Pro*; April 6, 2009.
BT does Italian Job on London traffic lights, *The Register*; April 6, 2009.
Vandals Blamed for phone and Internet outage, *CNET News*; April 9, 2009.

[5] Marcia Gulesian, When the Internet Fails: Application Availability, SLAs, and Disaster Recovery Planning, *Enterprise IT Planet*; September 24, 2008.