the Availability Digest

What? No Internet?

February 2008

On Wednesday, January 30, 2008, North Africa, the Middle East, and India experienced a massive Internet outage that was destined to last for several days or even weeks.[1] How did this happen? How did companies cope? Could it happen in other areas such as Europe or the United States?

The Failure

The bulk of data traffic from North Africa, from the Middle Eastern countries, and from India and Pakistan is routed through North Africa. There, it is carried by a set of three submarine cables that lie under the Mediterranean Sea. The cables link Alexandria, Egypt, with Palermo, Italy, where the traffic then moves on to Europe, the UK, and the Eastern United States.

On January 30, 2008, two of these three cables were severed. It is not yet known why, but the predominant theory is that the cables were severed by the anchor of a huge freighter. Heavy storms had hit the area the previous day and forced Egyptian authorities to close the northern entrance to the Suez Canal at Alexandria. As a result, ships had to anchor offshore in the Mediterranean Sea, dropping their anchors to ride out the storm. It is suspected that one of the freighters dropped its anchor on top of the cables.

Reportedly, the two severed cables were a kilometer apart. The storm may have dragged the freighter's anchor across the sea bed, thus taking out both cables.

The result of this catastrophe was that 75% of channel capacity was lost from the Mideast to Europe and beyond.

Coincidentally, on the same day, Telecom Egypt and France's Alcatel-Lucent signed a deal to lay a new $125 million submarine cable connecting Africa to Europe – a real-life case of too little too late.

Is Cable Really That Important to the Internet?

It certainly is when it comes to intercontinental communications. More than 95% of transoceanic telecommunications and data traffic is carried by submarine cables. The rest is carried by satellite. Submarine cables account for the majority of communications between Europe and the Middle East.

[1] USA Today; February 1, 2008.
Africa Reuters; January 31, 2008.
cnn.com; February 1, 2008.
Newsvine; January 31, 2008.
Gulf Times; February 1, 2008.

A single cable is no thicker than a human thumb but can carry an incredible amount of traffic. A single pair of fiber cables can carry the equivalent of 150 million phone calls. Therefore, only a few of these very expensive cables are needed to carry all of the traffic from a technically accomplished region. Three cables did the trick for communications traffic between the Mideast and Europe.

The Impact

The severed cables carried not only Internet traffic but also international telephone and television traffic to the affected regions. The outage affected countries through a wide swath of the Middle East and beyond, including Egypt, Saudi Arabia, The United Arab Emirates, Yemen, Qatar, Bahrain, Kuwait, India, and Pakistan.

About 70% of Egyptian users were affected. The Egyptian financial markets were disrupted. Egypt's call-center industry saw its productivity reduced by 70%. Egypt's Telecom Ministry requested users not to overload the backup system with hefty downloads and file-sharing applications. An Egyptian blogger sarcastically predicted complete social breakdown in Cairo's upscale districts as thousands of users would find it impossible to update their Facebook status.

Betelco, the Bahraini communications company, also requested users not to overload the back-up communication links with downloads and file-sharing applications. People downloading music and films were going to affect businesses, which have more important things to do, Betelco said.

Saudi Telecom reported the loss of more than 50% of its international lines, and Qatar reported a 40% loss.

Perhaps the hardest hit in the region was Dubai, Bahrain's major city. Dubai is, in the view of many, the rising star in the Middle East crown of high technology and is responsible for billions of dollars worth of transactions daily.

Information-technology companies, software companies, and call centers that provide online service to the UK, to Europe, and to the U.S. East Coast were the worst affected. India's $11-billion outsourcing industry provides services ranging from answering customer queries to analyzing equity markets. These services are provided to global clients that seek to cut costs by outsourcing work. India's outsourcing industry employs 700,000 people working for 1,250 companies in 30 cities.

Among these companies, the hardest hit were those in the call-center industry. Call centers were impacted not only by the loss of most of their Internet capacity but also by the degradation in voice quality as telecommunications links were rerouted to longer cable runs across the Pacific and to satellite channels.

India was also concerned that the outage could affect the trading patterns on its two major stock exchanges, the National Stock Exchange in Delhi and the SENSEX exchange in Bombay.

Extending beyond India in the area, Bangladesh reported running at 25% of its usual capacity, with ISPs and call centers being affected. Sri Lanka experienced a drastic drop in service quality, and Pakistan was affected.

To add to the area's woes, millions of South Asians work to send money home to their families that live in the Mideast. The next day was Friday, the first day of the month. It was on this day that these foreign workers would descend on the Internet to send money home to their families.

Recovery and Restoration

When communication was lost over the severed cables, all traffic was rerouted to the third surviving cable. This cable is an older cable with less capacity than the two newer cables that were now failed. As a result, the third cable became seriously overloaded, making the Internet almost useless and voice traffic barely intelligible.

Once the magnitude of the outage was realized, backup plans (to the extent that they existed) were put into place. Traffic from the Mideast and Africa had to be rerouted eastward through Pacific cables around most of the globe or over satellite channels. These longer channels caused serious degradation in voice traffic and longer delays in Internet interactions than was normally experienced but with at least acceptable quality.

Fortunately, many companies and some countries had contingency plans in place. Several large companies had redundant routes over the Atlantic and Pacific oceans. Israel, Lebanon, and Iraq (of all places) had backup satellite channels and switched over immediately with little if any impact on users.

As of this writing, conjecture was that it would take one or two weeks, perhaps more, to repair the two cables. Efforts to get to the cables were thwarted by the continuing bad weather.

In order to repair the cables, the location of the break has to be determined; and then the cables have to be dragged to the surface and the severed sections replaced with new lengths of cable. The location of the break can be determined by sending down the cable a signal that will then be reflected back to its source. By measuring the time delay of the reflection, the location of the cable break can be determined.

Once ships arrive at the break location, the repair technique depends upon the depth of the cable at that point:

- If the severed section is less than 4,000 feet below the surface, a submersible robot can be sent. The robot finds the severed section, cuts it out, and drags the cable ends back up to the repair ship.

- If the cable break is deeper than 4,000 feet, the cable technicians use a “grapnel” to cut and hold the cable as it is being dragged to the surface.

- Once the cable ends have been brought to the surface, a skilled technician splices the glass fibers and uses adhesives to attach the new section of cable.

- The repaired cable is then lowered on ropes back to the seabed.

Could Such a Massive Internet Failure Have Been Foreseen?

It seems so, and there is little excuse for not having a tested contingency plan in place.

There is a significant precedent for such a failure. One of the biggest interruptions of international telecommunication services occurred in December, 2006, when a magnitude 7.1 earthquake broke nine submarine cables between Taiwan and the Philippines and cut connections between southeast Asia and the rest of the world. Internet links were down in China, Hong Kong, Japan, Singapore, Taiwan, and the Philippines, disrupting banks, airlines, and email services. It took 49 days to restore full capacity.

Why would anyone think that this couldn't happen again, or happen to them? Indeed, a recent report by the Business Roundtable,[2] 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. This outage certainly beat their timetable. They suggest that this breakdown could be brought about by malicious code, coding error, natural disasters, or attacks by terrorists or other adversaries. How about man-made disasters, like a dragging ship anchor?

They point out that business executives often fail to realize how dependent they have become on the Internet for email, collaboration, ecommerce, public interfaces, and internal web sites. These executives fail to take into account in their disaster recovery and business continuity plans the threat of an Internet disruption to their companies or to their suppliers. After all, in all of the decades of the Internet, this has never happened to them or to their peers.

But as this incident shows, it can happen. After the recent cable break, a Dubai analyst noted that when it comes to great technology, it's not about building it, it's how to protect it.

Lessons Learned

If your company depends upon the Internet for its day-to-day well-being, it is incumbent on you for the sake of your company, your suppliers, your customers, and your shareholders to ensure that your business can continue should you lose your primary Internet infrastructure. This is all the more important if you are a supplier of web services such as web hosting or software-as-a-service.

The first line of defense is a contingency plan to get reconnected to the Internet. The hours following a massive channel 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 service from Ground Control (www.groundcontrol.com) that covers the contiguous 48 states in the U.S. via the Galileo stationary satellite.

Beyond the first line of defense must be a deeper contingency plan. A solid knowledge of network topology is essential in order to arrange additional meaningful contingency agreements with alternate ISPs. Furthermore, contingency plans are meaningless without live testing in which you really pull the plug and switch over to your contingency path.

Finally, for the company that is truly serious about continuous uptime, the primary data center must be replicated to a remote facility with rapid failover. This is where active/active system technology can play a major role, reducing failover time from hours or days to seconds.[3]

Postscript

Two days later, on February 1, another cable in the Persian Gulf 35 miles north of Dubai was severed, causing disruptions between the Middle East and parts of Asia. This one was caused by a 5 ½ ton abandoned anchor.

Yes, massive Internet interruptions can occur!

[2] Gary Anthes, The Internet is Down – Now What?, Computing SA, http://mybroadband.co.xa/news/print/2674.html; January 28, 2008.
[3] What Is Active/Active?, *Availability Digest*; October, 2006.