the Availability Digest

www.availabilitydigest.com
@availabilitydig

Don't Let Your Network Crash

October 2017

There is nothing that can ruin your day more than to have your network crash. Imagine being without the Internet for hours at a time. Most of us would be unable to accomplish much during that period.

Fortunately, our networks are quite robust. The TCP/IP protocol now in common use guarantees the proper error-free delivery of messages. And our networks have many paths so that messages can be routed around failed network segments and still reach their recipients.

However, networks have not always been so robust. In 1990, a software bug propagated through the ATT network and took down the entire ATT system for hours. A decade earlier, a similar bug collapsed the ARPANET. The ARPANET was one of the earliest networks and through its failure history paved the way for today's ultra-reliable networks.

The ARPANET

The Advanced Research Projects Agency Network (ARPANET) was an early packet-switching network. The ARPANET established its first computer-to-computer link on October 29, 1969.

As the ARPANET project progressed, protocols for internetworking were developed so that multiple separate networks could be joined into a network of networks. 1n 1982, the Internet Protocol Suite (TCP/IP) was introduced as the standard networking protocol on the ARPANET. These technologies became the technical foundation for the Internet.

The ARPANET was decommissioned in 1990.

The First Major Network Crash – the ARPANET

The ARPANET initially linked four sites in California and Utah. It later was expanded to cover research centers across the country.

The ARPANET was the granddaddy of network crashes. On October 27, 1980, it experienced its first network crash. The network failure resulted from a redundant single-error detecting code that was used for transmission but not storage, and a garbage-collection algorithm for removing old messages that was not resistant to the simultaneous existence of one message with several different time stamps. The combination of the events took the network down for four hours.

The Amadeus Network Disruption

On September 28, 2017, a passenger management system used by dozens of airlines went offline. A technical problem described as a 'network issue' forced crowded airports to issue manual boarding passes, creating long queues and worldwide flight delays. Disruptions to check-in service were reported from London's Heathrow Airport (LHR) to Singapore's Changi (SIN) and even in the US at airports such as Washington, DC's Reagan Airport (DCA).

The disruption was caused by an internal issue with IT firm Amadeus. The company's Altea software is used by more than 100 airlines around the world. Passengers traveling with a number of airlines, such as British Airways, Air France, KLM, Southwest, Lufthansa and more, reported the delays when checking in. The program that caused the delays was a passenger management system. It was used to manage booking and check-in systems, allowing airlines to check who's meant to be on each flight.

Amadeus confirmed that its network had a disruption and that it was working to resolve it.
"Amadeus confirms that during the morning, we experienced a network issue that caused disruption to some of our systems," an Amadeus spokesperson said. "As a result of the incident, customers experienced disruption to certain services."

The company said that services were gradually being restored, and its technical teams were working to identify the cause and restore services as quickly as possible. A spokesperson for London's Heathrow Airport confirmed that the airport had faced disruptions as a result of the outage.

"A small number of airlines are currently experiencing intermittent issues with their check-in systems at airports around the world — including at Heathrow," the spokesperson said. "Passengers will still be able to check-in for their flight, although the process may take slightly longer than usual. We are working closely with our airlines to help resolve the issue as quickly as possible."

The outage was unusual because of the scale of the problem. Usually, a technical incident is limited to a single airline or airport. Yesterday, passengers in London, Australia, Singapore and France, among many others, were forced to wait when a software package used by over 130 different airlines experienced a brief spell of technical problems.

The DarkNet

The DarkNet is a private network in which connections are made only between trusted peers. It is structured to maintain the anonymity of its users. A person can only access a Darknet web site if he has been approved by the other members of the web site. For instance, if you want to get onto a hacker's web site, you have to prove to the current members that you are a legitimate hacker.

The DarkNet actually originated quite legally under the auspices of ARPANET, the predecessor to the Internet. Launched in 2002, a project called Tor was set up by the U.S. Naval Research Laboratory with the purpose of protecting U.S. intelligence communications. It allowed groups of people using the Internet to maintain complete anonymity.

Tor is an acronym for The Onion Ring project because of its many layers of protection. Tor directs Internet traffic through a worldwide, volunteer network of more than 5,000 relays to conceal a user's location and usage from anyone conducting network surveillance. Tor is currently supported by the nonprofit Tor Project (www.torproject.com) and is heavily used legitimately by groups of people who need to keep their communications absolutely private.

IPv4 and IPv6

IPv4 was the fourth version of the Internet Protocol and was introduced in 1981. Growing out of the ARPANET (Advanced Research Projects Agency Network), a joint venture of the U.S. Department of Defense and several universities and laboratories, the primary use of the Internet was expected to be for the exchange of scientific papers and studies for academia.

However, the Internet's use expanded beyond the wildest expectations. It was almost doomed to failure by its use of IPv4 to assign addresses to Internet hosts. The 32-bit addressing space of IPv4 could provide addressing to about four billion hosts, and it was about to run out, which would doom the Internet to almost certain failure.

Thus, IPv6 was born. With its 128-bit address space, there is no concern of running out of host addresses. IPv6 can provide 10^{38} host addresses.

Will the Cloud Be Able To Handle IoT?

Devices carrying the IoT label are inherently sensors that collect data and send it to be processed, usually via multiple mathematical components. Consider a smart car sending fuel economy data back to its manufacturer via its IoT devices. Not only is each car's raw data being sent, but also factors like road surface, tire quality, outside temperature and average speed. All this data is uploaded to the cloud where the car manufacturer's business intelligence tools perform computations and analysis, then produce massive data sets. These data sets are then downloaded to the car manufacturer for analysis.

The IoT device plays little more than the role of the messenger here. the IoT device and the cloud are highly sophisticated machines; but it is the cloud that is doing almost all of the heavy lifting, which can leave it showing considerable strain for its efforts.

Despite like-minded technologies at their cores, IoT and cloud computing have several properties that conflict with one another that are factors in this strain.

In general, cloud computing resources are fairly inexpensive in terms of availability, can perform tasks rapidly and are quite flexible in meeting the needs of each user they serve. User location is irrelevant to using the cloud; as long as you have the Internet, you can connect.

Conversely, IoT devices are more expensive (in terms of development and deployment), they are not nearly as flexible, and they are generally stuck in one location.

The number of IoT devices is expected to skyrocket over the next several years, to be numbered in the billions. Can our clouds handle this computational workload? Will IoT devices cause some of our clouds to fail?

Hacking on the Internet

The worst network crash would be that of the Internet. Yet the Internet is susceptible to being crashed by hackers.

In November, 1988, the news broke that a dangerous computer worm – the first to spread widely – was slithering across the Internet. As the attack raged, crashing thousands of machines and causing millions of dollars in damage, it became clear that the failure went beyond a single flaw in the Internet. The worm was using the Internet's essential nature — fast, open and frictionless — to deliver malicious code along computer lines designed to carry harmless files or e-mails.

Decades later, after hundreds of billions of dollars spent on computer security, the threat posed by the Internet seems to grow worse each year. Where hackers once attacked only computers, the penchant for destruction has now leapt beyond the virtual realm to threaten banks, retailers, government agencies, and, experts worry, critical mechanical systems in dams, power plants and aircraft.

Summary

Fortunately, once we got past the ARPANET days, network crashes have become a rarity. But with the openness of the Internet and its widespread importance to billions of people, we are once again faced with the possibility of a major network failure. It is important for every corporation, and in fact every person, to consider the consequences of an extended Internet outage and how they will carry on during that time.

Acknowledgements

Information for this article was taken from the following sources:

The IPV4 Doomsday, *The Availability Digest*; August 2009.
http://www.availabilitydigest.com/public_articles/0408/ipv4_doomsday.pdf
With 100% Uptime, Do I Need a Business Continuity Plan? *The Availability Digest*; October 2006.
http://www.availabilitydigest.com/public_articles/0101/do_i_need_a_bcp.pdf
The DarkNet, *Availability Digest*; September 2014.
http://www.availabilitydigest.com/public_articles/0909/darknet.pdf
A Flaw in the Design, *The Washington Post*; May 30, 2015.
'Network Issue' Causes Check-In Systems to Crash Worldwide; Passengers Report Massive Delays, *The The Points Guy*; September 28, 2017.
How will the cloud be able to handle the emergence of IoT, *Network World;* October 3, 2017.
Bug in software used by 130 airlines creates check-in chaos, *Digital Journal*; September 29, 2017.
A Day in History: October 27, *Computer History Museum*.
ARPANET, *Wikipedia*.