MAJOR NETWORK OUTAGES OF 2021

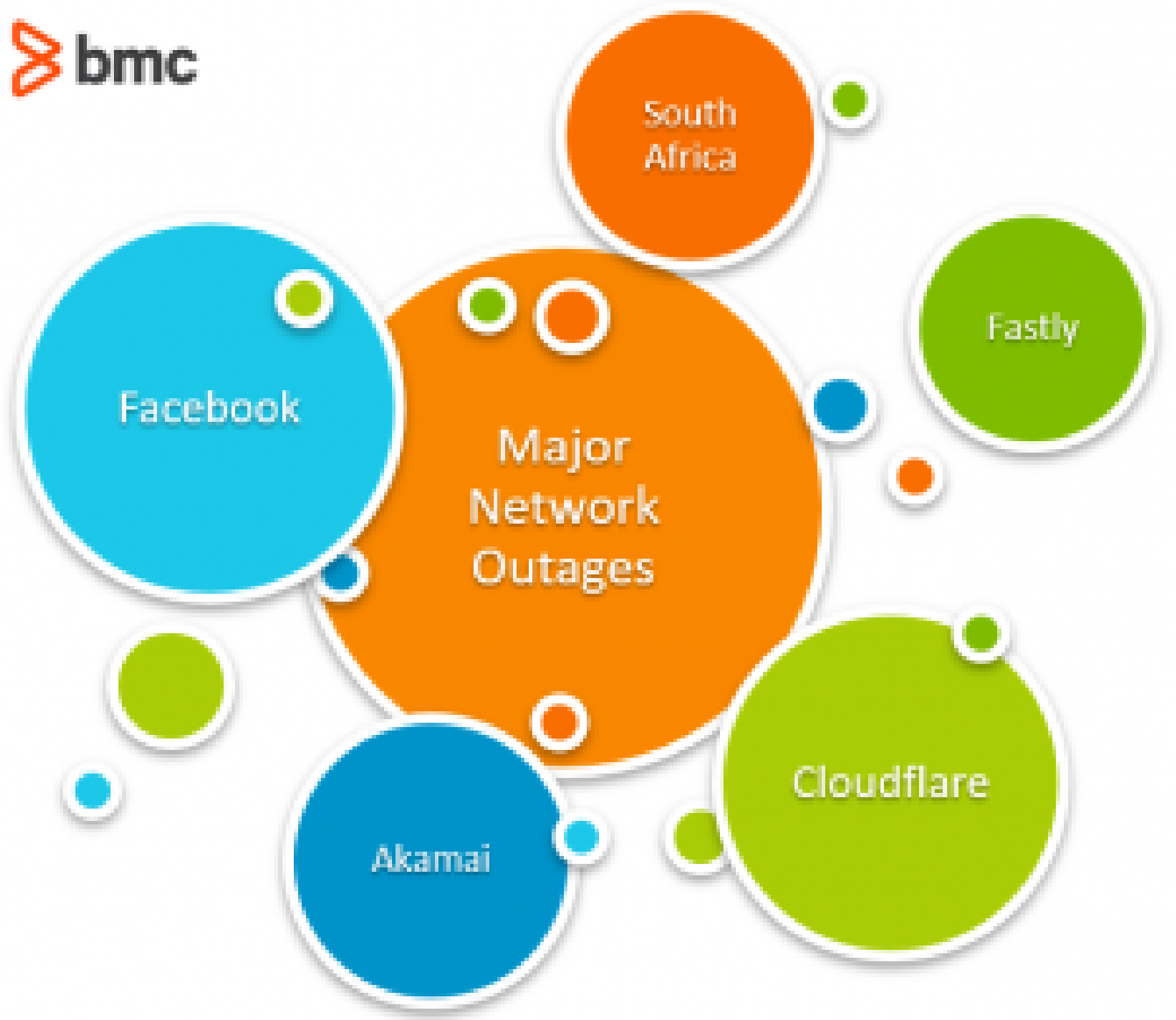
Perhaps the biggest effect of the digital age is that connectivity is a basic need for all. There is little wonder that enterprise risk management considers network outages as a top tier risk.

- 83% of respondents from an Open Gear survey reported that network resilience was their number one concern
- 92% reported financial loss from network outages.

Despite significant efforts to limit the impact of network unavailability through redundancy and other means, providing 100% uptime still remains a major challenge, mainly due to unforeseen factors.

So, let's take a look at some recent outages that have significantly impacted users around the globe.

(Understand the impact of redundancy on availability.)



Facebook's social gaffes

On Monday, October 4th, 2021, some form of online world peace was experienced for approximately six hours following a network outage on Facebook together with its associated services WhatsApp and Instagram.

In a detailed post, their Infrastructure VP explained how a configuration change took down all the connections in their backbone network, effectively disconnecting their data centers from the rest of the internet. This then resulted in a second problem where their DNS servers disabled the BGP advertisements due to inability to reach the data centers, causing all DNS queries to their services to go unanswered.

Unfortunately, due to security measures which depended on the network to work, data center engineers faced challenges while attempting to physically access the backbone network routers to reconfigure them manually.

Summarizing this outage, CloudFlare called the episode:

> "A gentle reminder that the internet is a very complex and interdependent system of millions of systems and protocols working together."

This was the second major outage affecting the social media giant in 2021, with the first occurring on 19th March for 45 minutes, affecting the same services. A Facebook spokesperson later said that the outage was due to a technical issue that had since been resolved.

Fastly goes slow after network bug

On June 8th, 2021, Fastly had an outage that lasted almost an hour, causing major websites such as Amazon, eBay, Reddit, Spotify, Twitch, The Guardian, The New York Times, and even the UK government's websites to be unreachable.

The company is one of the world's leading Content Delivery Networks, and as a CDN it runs an edge cloud network which brings web content closer to users, thereby reducing latency, while also facilitating handling of traffic spikes and offering protection from DDoS attacks.

Fastly explained that the previous month, a software deployment introduced a latent bug into their network. This bug was then triggered by a configuration change pushed by a customer, resulting in their network returning errors in 85% of routing requests. Users reported getting 503 errors, meaning there was a temporary problem accessing the web hosting servers.

The team at Fastly were quick to isolate the cause and disable the configuration, before turning their attention to deploying a bug fix and carry out a postmortem on preventive and corrective measures to prevent recurrence.

Cloudflare & Akamai's bottlenecks

In recent times, both Cloudflare and Akamai experienced network outages, resulting in service unavailability for many of their customers' end users.

Cloudflare, which handles approximately 18% of all web traffic, experienced a network outage that impacted 50% of its traffic resulting in major websites being unreachable for around 27 minutes. Websites impacted included Shopify, Discord, and AWS.

The incident on 17th July 2020 was a result of a configuration change made on their backbone network to alleviate congestion. Unfortunately, an error routed all the BGP traffic to another backbone router in Atlanta which became overwhelmed, resulting in congestion and subsequent errors. To resolve the issues, the Atlanta router was dropped from the network and traffic rerouted to other routers.

On the other hand, Akamai's edge DNS had an issue that impacted quite a number of websites globally on 22nd July 2021 for about an hour. Given that the company boasts of having 85% of the world's Internet users being within a single "network hop" of an Akamai CDN server, downtime would be felt significantly across the world.

Services affected included PlayStation Network, Airbnb, FedEx, and UPS. In a series of tweets, Akamai reported that a software configuration update triggered a bug in the DNS system, resulting in the incident.

Rolling back the update addressed the issue, but the damage had already been done.

Freak case: South Africa's slow internet

In January 2020, a freak occurrence of two undersea internet cables suffering breakdowns at the same time resulted in slow internet speeds for South Africa and nearby countries.

The South Atlantic 3/West Africa (SAT-3/Wasc) submarine cable which links Portugal and Spain to South Africa, and the West Africa Cable System (Wacs) which links SA with the UK, both suffered breakdowns near Gabon and Congo respectively. A second cut on the Wacs cable near the UK was later discovered, compounding the problem, according to reports.

Traffic was rerouted to other undersea cables, while repair ships were marshalled to restore the connectivity. Unfortunately, delays were experienced due to the time it took to prepare for such an operation, as well as high winds in the Atlantic Ocean.

It took several weeks for services to be completely restored on the two cables.

A future with no outages?

The internet powers today's economy. Customers want faster access to the data they need, whether for business or personal use.

The rise of edge computing to supplement the cloud cannot be ignored as it addresses the needs for low latency and high resilience, through CDNs and other technologies. However, implementing redundancy at the distributed level, as well as providing onsite support in case of emergencies will most likely result in increased risk of outages.

Configuration changes as a source of major network outages is also evident as some of the examples have demonstrated. It is likely that as more complexity is introduced, chances of random bugs being introduced that cannot be spotted by existing test scenarios will increase.

So, what's the key takeaway? The focus for service providers will be to:

- Build more layers of resilience through redundancy
- Limit impact through distributed networks and faster restoration mechanisms

Related reading

- BMC IT Operations Blog
- BMC Business of IT Blog
- Incident Management: The Complete Guide
- AI Cyberattacks & How They Work, Explained
- What Is a Cyber Resilience Strategy?
- N-Modular Redundancy Explained: N, N+1, N+2, 2N, 2N+1, 2N+2, 3N/2