



Cloudflare outage on July 17, 2020

07/17/2020



John Graham-Cumming

4 min read

Today a configuration error in our backbone network caused an outage for Internet properties and Cloudflare services that lasted 27 minutes. We saw traffic drop by about 50% across our network. Because of the architecture of our backbone this outage didn't affect the entire Cloudflare network and was localized to certain geographies.

The outage occurred because, while working on an unrelated issue with a segment of the backbone from Newark to Chicago, our network engineering team updated the configuration on a router in Atlanta to alleviate congestion. This configuration contained an error that caused all traffic across our backbone to be sent to Atlanta. This quickly overwhelmed the Atlanta router and caused Cloudflare network locations connected to the backbone to fail.

The affected locations were San Jose, Dallas, Seattle, Los Angeles, Chicago, Washington, DC, Richmond, Newark, Atlanta, London, Amsterdam, Frankfurt, Paris, Stockholm, Moscow, St. Petersburg, São Paulo, Curitiba, and Porto Alegre. Other locations continued to operate normally.

For the avoidance of doubt: this was not caused by an attack or breach of any kind.

We are sorry for this outage and have already made a global change to the backbone configuration that will prevent it from being able to occur again.

The Cloudflare Backbone



Cloudflare operates a *backbone* between many of our data centers around the world. The backbone is a series of private lines between our data centers that we use for faster and more reliable paths between them. These links allow us to carry traffic between different data centers, without going over the public Internet.

We use this, for example, to reach a website origin server sitting in New York, carrying requests over our private backbone to both San Jose, California, as far as Frankfurt or São Paulo. This additional option to avoid the public Internet allows a higher quality of service, as the private network can be used to avoid Internet congestion points. With the backbone, we have far greater control over where and how to route Internet requests and traffic than the public Internet provides.

Timeline

All timestamps are UTC.

First, an issue occurred on the backbone link between Newark and Chicago which led to backbone congestion in between Atlanta and Washington, DC.

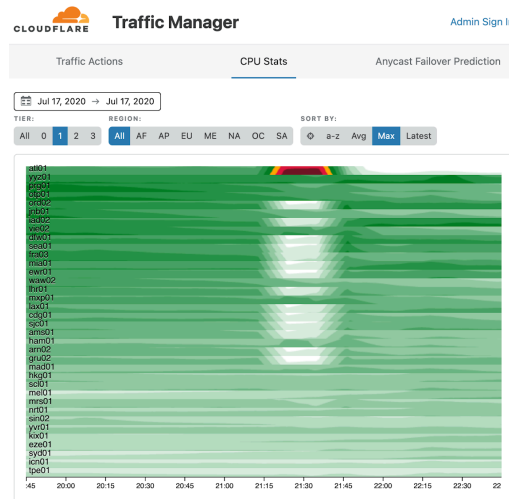
In responding to that issue, a configuration change was made in Atlanta. That change started the outage at 21:12. Once the outage was understood, the Atlanta router was disabled and traffic began flowing normally again at 21:39.

Shortly after, we saw congestion at one of our core data centers that processes logs and metrics, causing some logs to be dropped. During this period the edge network continued to operate normally.

- 20:25: Loss of backbone link between EWR and ORD
- 20:25: Backbone between ATL and IAD is congesting
- 21:12 to 21:39: ATL attracted traffic from across the backbone
- 21:39 to 21:47: ATL dropped from the backbone, service restored
- 21:47 to 22:10: Core congestion caused some logs to drop, edge continues operating
- 22:10: Full recovery, including logs and metrics

Here's a view of the impact from Cloudflare's internal traffic manager tool. The red and orange region at the top shows CPU utilization in Atlanta reaching overload, and the white regions show affected data centers seeing CPU drop to near zero as they were no longer handling traffic. This is the period of the outage.

Other, unaffected data centers show no change in their CPU utilization during the incident. That's indicated by the fact that the green color does not change during the incident for those data centers.



What happened and what we're doing about it

As there was backbone congestion in Atlanta, the team had decided to remove some of Atlanta's backbone traffic. But instead of removing the Atlanta routes from the backbone, a one line change started leaking all BGP routes into the backbone.

```
(master) (edit)
[edit policy-options policy-statement 6-BBONE-OUT term 6-SITE-LOCAL from]
!
  inactive: prefix-list 6-SITE-LOCAL { ... }
```

The complete term looks like this:

```
from {
  prefix-list 6-SITE-LOCAL;
}
then {
  local-preference 200;
  community add SITE-LOCAL-ROUTE;
  community add ATL01;
  community add NORTH-AMERICA;
  accept;
}
```

This term sets the local-preference, adds some communities, and accepts the routes that match the prefix-list. Local-preference is a transitive property on iBGP sessions (it will be transferred to the next BGP peer).

The correct change would have been to deactivate the term instead of the prefix-list.

By removing the prefix-list condition, the router was instructed to send all its BGP routes to all other backbone routers, with an increased local-preference of 200. Unfortunately at the time, local routes that the edge routers received from our compute nodes had a local-preference of 100. As the higher local-preference wins, all the traffic meant for local compute nodes went to Atlanta compute nodes instead.

With the routes sent out, Atlanta started attracting traffic from across the backbone.

We are making the following changes:

- Introduce a maximum-prefix limit on our backbone BGP sessions - this would have shut down the backbone in Atlanta, but our network is built to function properly without a backbone. This change will be deployed on Monday, July 20.
- Change the BGP local-preference for local server routes. This change will prevent a single location from attracting other locations' traffic similarly. This change has been deployed following the incident.

Conclusion

We've never experienced an outage on our backbone and our team responded quickly to restore service in the affected locations, but this was a very painful period for everyone involved. We are sorry for the disruption to our customers and to all the users who were unable to access Internet properties while the outage was happening.

We've already made changes to the backbone configuration to make sure that this cannot happen again, and further changes will resume on Monday.

We protect [entire corporate networks](#), help customers build [Internet-scale applications efficiently](#), accelerate any [website or Internet application](#), [ward off DDoS attacks](#), keep [hackers at bay](#), and can help you on [your journey to Zero Trust](#).

Visit [1.1.1.1](#) from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, [start here](#). If you're looking for a new career direction, check out [our open positions](#).

[Discuss on Hacker News](#)

ON AIR | **CLOUDFLARE TV**

Infrastructure and Sustainability

Tune In



[Post Mortem](#) [Outage](#)

Follow on X

Cloudflare | [@cloudflare](#)

RELATED POSTS

April 29, 2024 6:00 AM

Q1 2024 Internet disruption summary

The first quarter of 2024 kicked off with quite a few Internet disruptions. Perhaps most interestingly, RPKI, DNS, and DNSSEC issues were among the technical problems that disrupted connectivity for subscribers across multiple network providers...

By **David Belson**

[Cloudflare Radar](#), [Internet Traffic](#), [Outage](#), [Internet Shutdown](#), [Internet Quality](#)

April 08, 2024 6:00 AM

Major data center power failure (again): Cloudflare Code Orange tested

Just four months after a complete power outage at a critical data center we were hit with the exact same scenario. Here's how we did this time, and what's next...

By **Matthew Prince**, **John Graham-Cumming**, **Jeremy Hartman**

[Post Mortem](#), [Outage](#)

March 14, 2024 11:03 AM

Undersea cable failures cause Internet disruptions for multiple African countries

Internet connectivity in several African countries was disrupted on March 14, 2024, beginning at approximately 05:00 UTC. Based on published reports and social media posts from impacted network providers, the disruption is believed to be due to multiple undersea cable failures in the region...

By **João Tomé**, **David Belson**

[Cloudflare Radar](#), [Outage](#), [Internet Traffic](#), [Trends](#)

January 22, 2024 6:00 AM

Q4 2023 Internet disruption summary

In this post, we review selected Internet disruptions observed by Cloudflare during the fourth quarter of 2023, supported by traffic graphs from Cloudflare Radar and other internal Cloudflare tools, and grouped by associated cause or common geography...

By **David Belson**

[Cloudflare Radar](#), [Internet Traffic](#), [Outage](#), [Internet Shutdown](#), [Internet Quality](#)

