# Detecting Internet Routing Outages with Topology and Service analysis

Pei ZHANG, Xiaohong HUANG, Yan MA
School of Computer Science
Beijing University of Posts and Telecommunications

北京邮电大学

BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

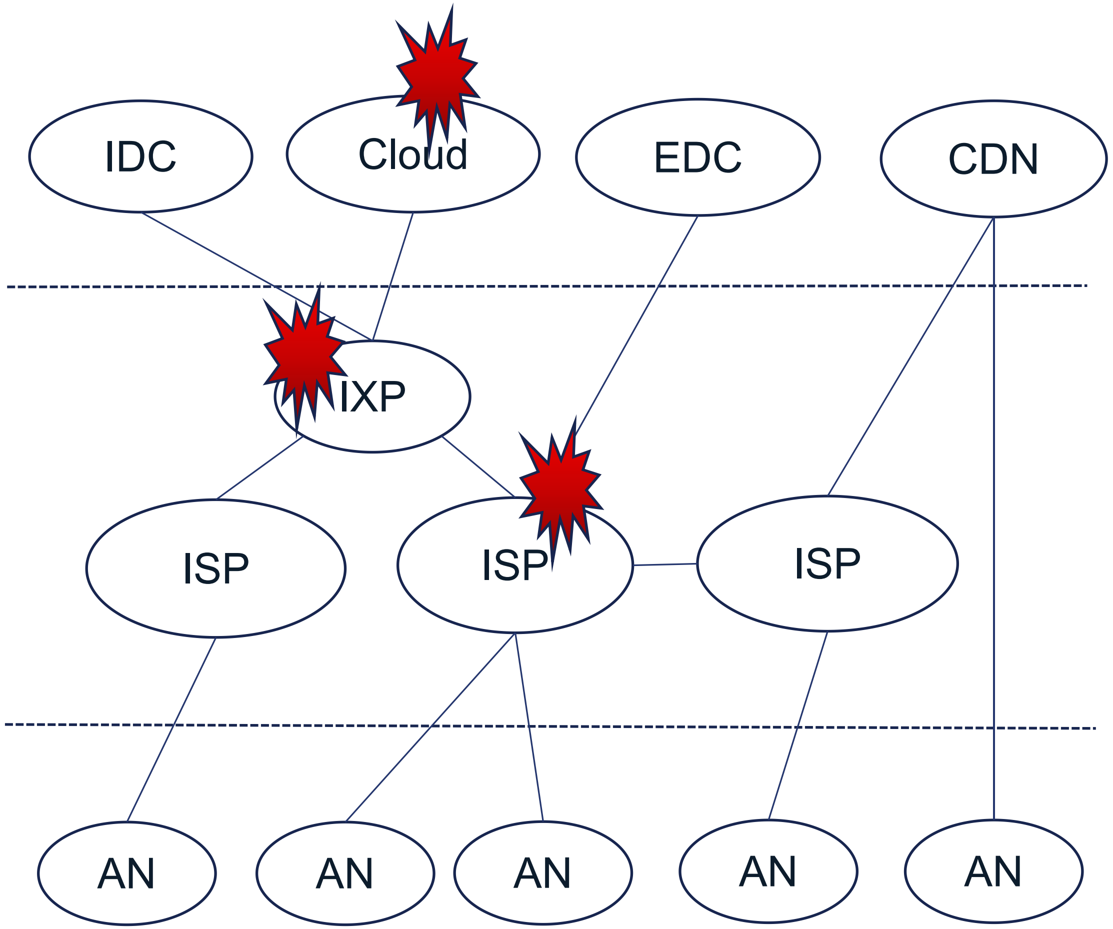
# Routing Outages Cause Internet Problems Worldwide

## The Internet is interdependent

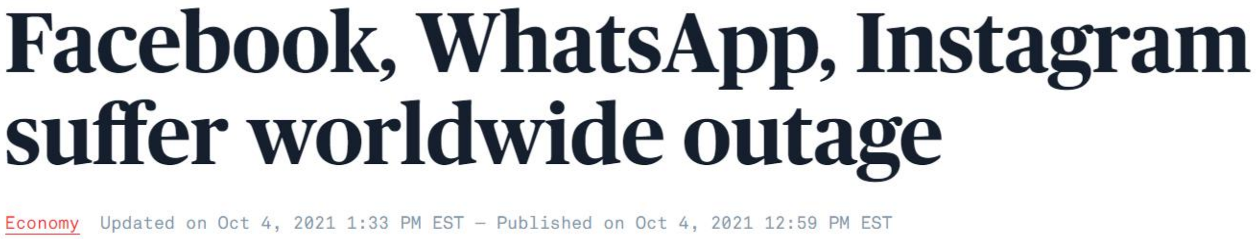
- Application delivery is dependent on many Internet Service Providers.
- CDN, DNS, public cloud work together to provide exceptional digital experiences.

## Outages can happen at any time, anywhere

- IXP outage, cloud outage, transit key point outage.
- Natural disasters, misconfiguration, network attacks, router overloads can lead to outage.
- Affect people's normal life,Organization lost revenue, reputational damage, even take entire network offline.

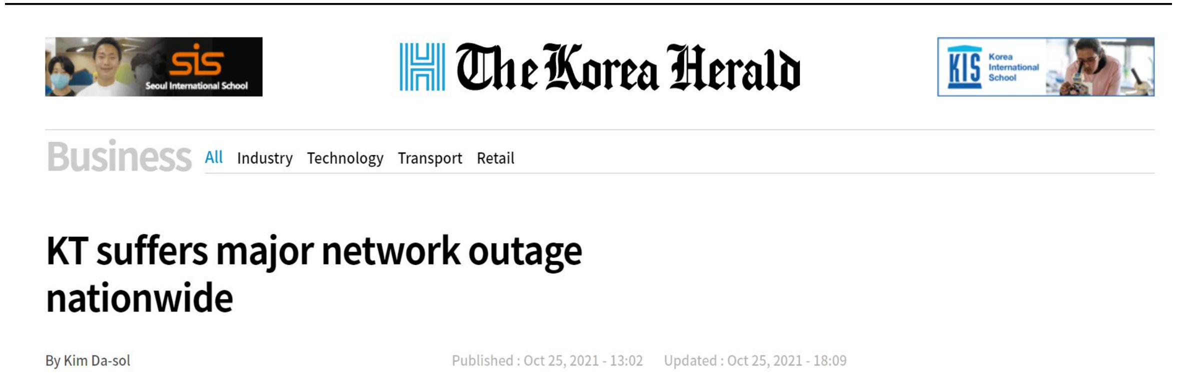


# Internet Routing Outages Incidents are Increasing



## Facebook, WhatsApp, Instagram suffer worldwide outage

Economy Updated on Oct 4, 2021 1:33 PM EST — Published on Oct 4, 2021 12:59 PM EST



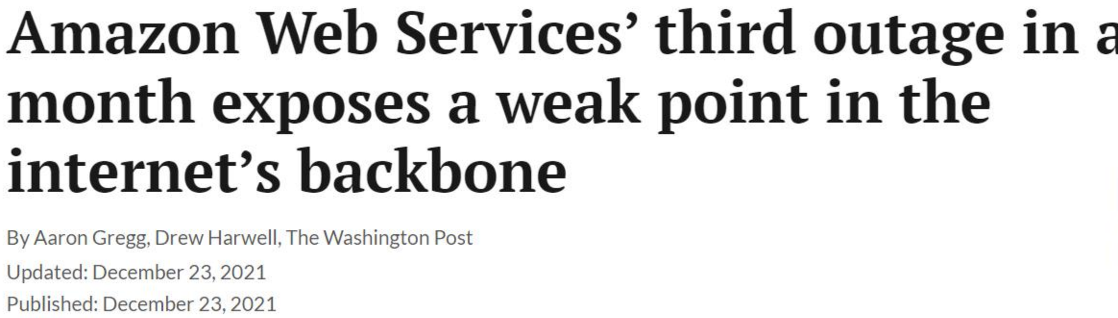
The Korea Herald

Business All Industry Technology Transport Retail

## KT suffers major network outage nationwide

By Kim Da-sol

Published : Oct 25, 2021 - 13:02 Updated : Oct 25, 2021 - 18:09

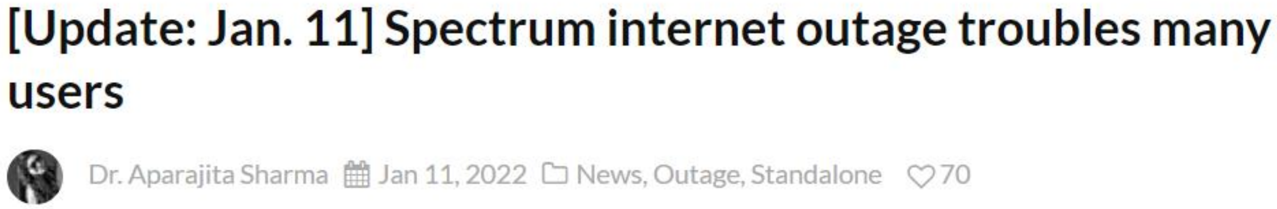


## Amazon Web Services' third outage in a month exposes a weak point in the internet's backbone

By Aaron Gregg, Drew Harwell, The Washington Post

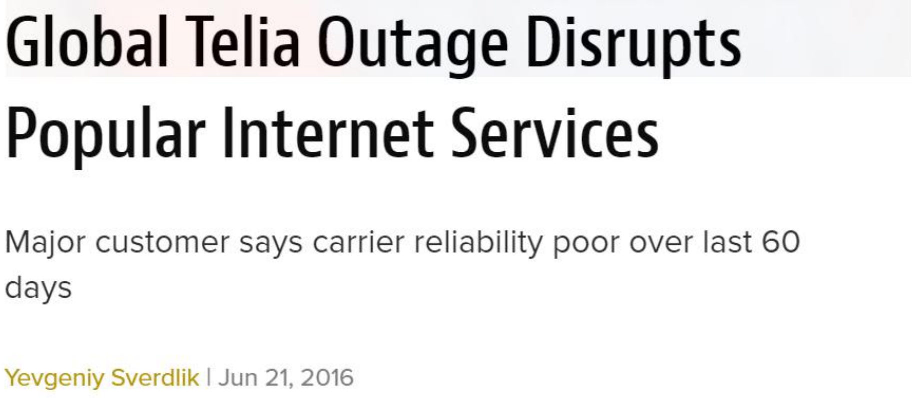
Updated: December 23, 2021

Published: December 23, 2021



## [Update: Jan. 11] Spectrum internet outage troubles many users

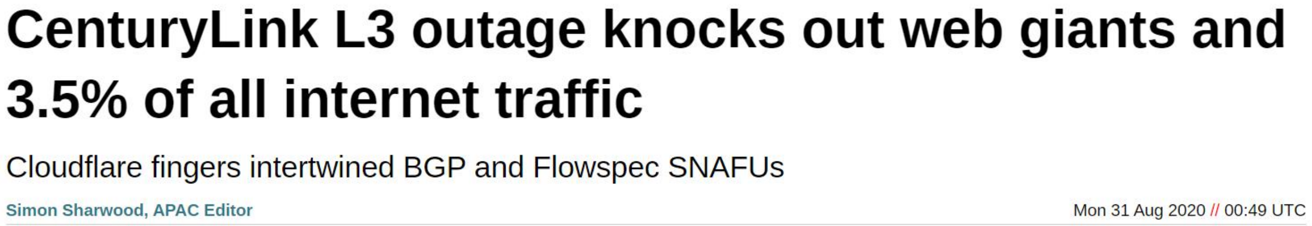
Dr. Aparajita Sharma Jan 11, 2022 News, Outage, Standalone ♡70



## Global Telia Outage Disrupts Popular Internet Services

Major customer says carrier reliability poor over last 60 days

Yevgeniy Sverdlik | Jun 21, 2016



## CenturyLink L3 outage knocks out web giants and 3.5% of all internet traffic

Cloudflare fingers intertwined BGP and Flowspec SNAFUs

Simon Sharwood, APAC Editor Mon 31 Aug 2020 // 00:49 UTC

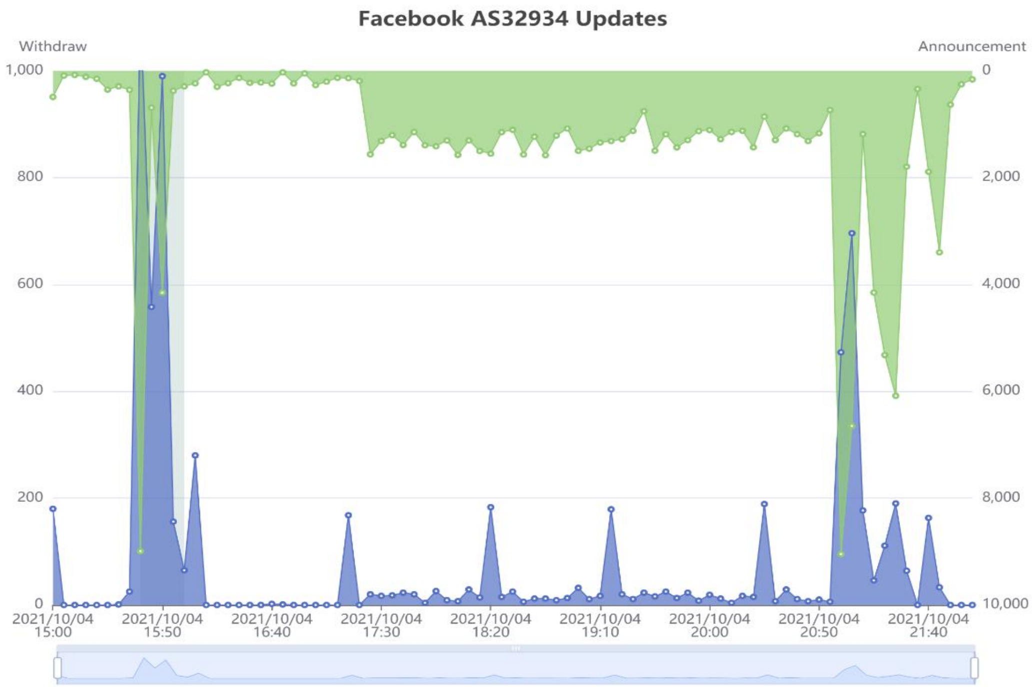
# Three Large-scale Internet Routing Outages Events

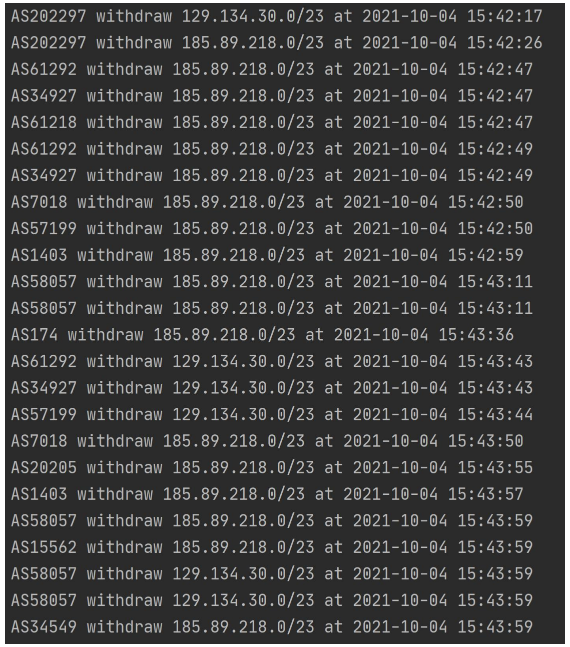
| Event | Time and Duration | Root cause | Impacts |
|---|---|---|---|
| **Facebook Outage** | October 4, 2021, between 15:40 and 22:45 UTC for more than seven hours. | Routine maintenance rendered its DNS servers unusable, cutting off Facebook's entire backbone network from its data centers. | Facebook and its other platforms, including Instagram, WhatsApp and Messenger, went down globally for close to six hours. |
| **KT Outage** | October 25, 2021, between 2:16 and 2:56 UTC for approximately 40 minutes. | In a statement, the telco said it initially suspected a DDoS attack due to traffic overload but after it scrutinised the matter it found that the cause was a routing error. | The telco's subscribers were unable to use their credit cards, trade stocks, or access apps, while some large commercial websites were also shut down during that period. |
| **CenturyLink Outage** | August 30, 2020, between 10:04 and 15:30 UTC for approximately five and a half hours. | Misconfiguration,the outage was caused by an offending Flowspec announcement that prevented BGP from correctly establishing. | Takes down Cloudflare, Reddit, Hulu, AWS, Blizzard, Steam, Xbox Live, Discord, and dozens more. A 3.5% drop in global web traffic. |

# What’s Happening during the Facebook Outage Event？

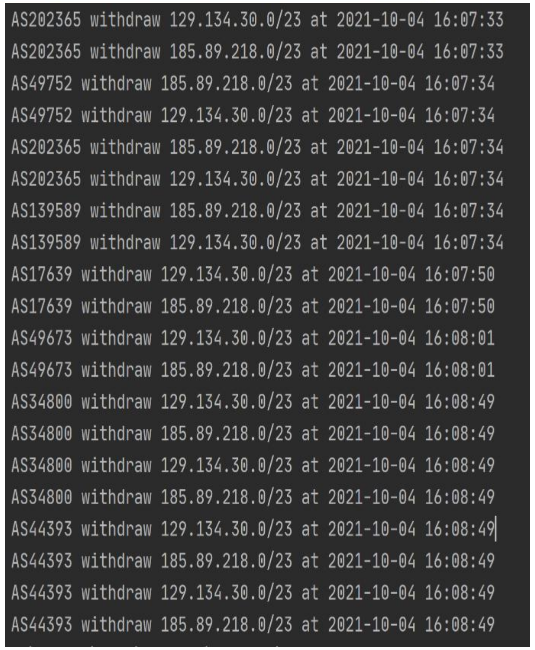
Important applications and DNS authoritative resolution service are centralized in AS32934!

- AS32934 BGP Withdraw and Announcement updates surged.
- Faecbook’s DNS Authoritative server prefixes were withdrawed by many ASes.
- Some other important applications went down.
- The whole process lasted 20 minutes.
- It took six hours to recover.



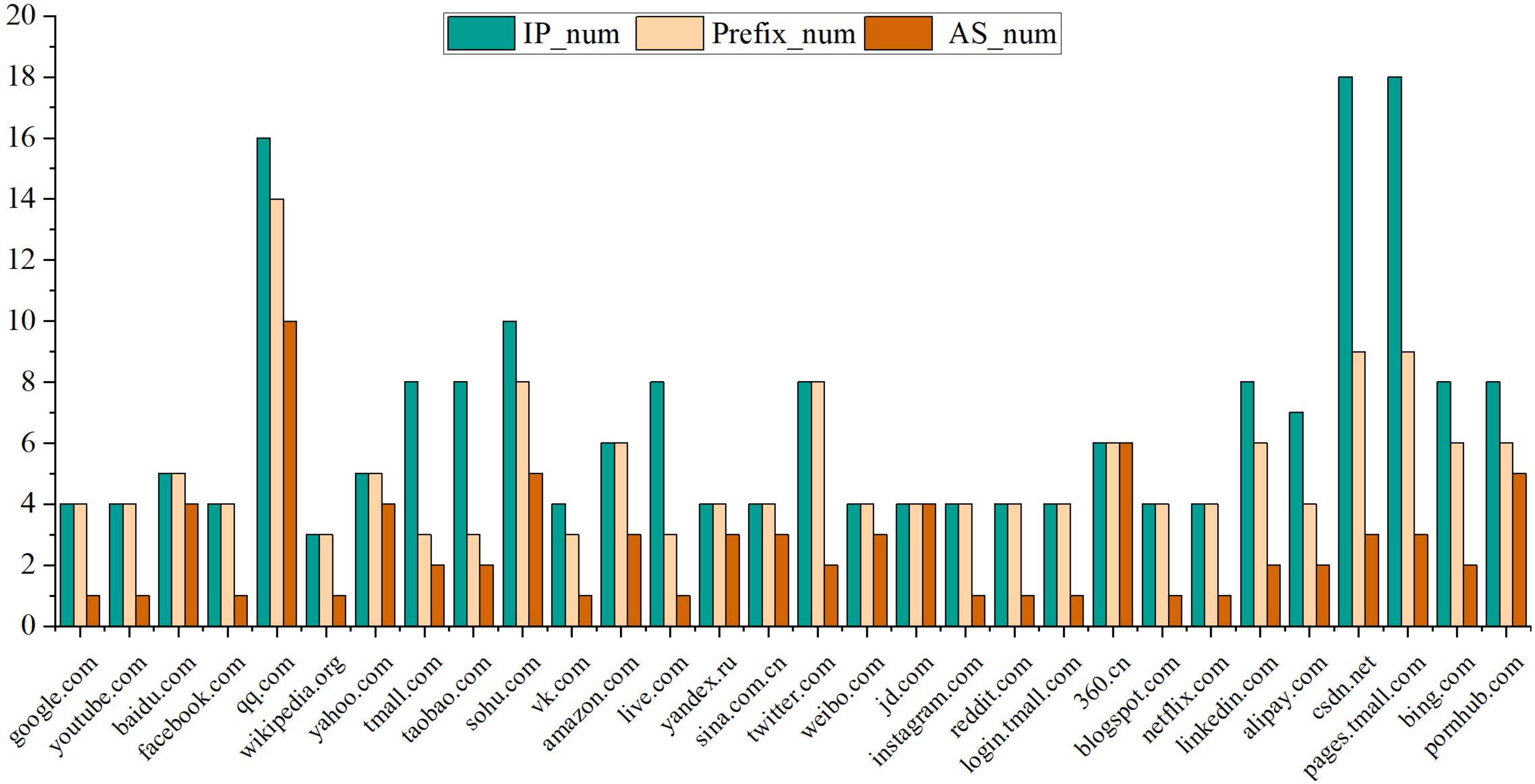


```
AS202297 withdraw 129.134.30.0/23 at 2021-10-04 15:42:17
AS202297 withdraw 185.89.218.0/23 at 2021-10-04 15:42:26
AS61292 withdraw 185.89.218.0/23 at 2021-10-04 15:42:47
AS34927 withdraw 185.89.218.0/23 at 2021-10-04 15:42:47
AS61218 withdraw 185.89.218.0/23 at 2021-10-04 15:42:47
AS61292 withdraw 185.89.218.0/23 at 2021-10-04 15:42:49
AS34927 withdraw 185.89.218.0/23 at 2021-10-04 15:42:49
AS7018 withdraw 185.89.218.0/23 at 2021-10-04 15:42:50
AS57199 withdraw 185.89.218.0/23 at 2021-10-04 15:42:50
AS1403 withdraw 185.89.218.0/23 at 2021-10-04 15:42:59
AS58057 withdraw 185.89.218.0/23 at 2021-10-04 15:43:11
AS58057 withdraw 185.89.218.0/23 at 2021-10-04 15:43:11
AS174 withdraw 185.89.218.0/23 at 2021-10-04 15:43:36
AS61292 withdraw 129.134.30.0/23 at 2021-10-04 15:43:43
AS34927 withdraw 129.134.30.0/23 at 2021-10-04 15:43:43
AS57199 withdraw 129.134.30.0/23 at 2021-10-04 15:43:44
AS7018 withdraw 185.89.218.0/23 at 2021-10-04 15:43:50
AS20205 withdraw 185.89.218.0/23 at 2021-10-04 15:43:55
AS1403 withdraw 185.89.218.0/23 at 2021-10-04 15:43:57
AS58057 withdraw 185.89.218.0/23 at 2021-10-04 15:43:59
AS15562 withdraw 185.89.218.0/23 at 2021-10-04 15:43:59
AS58057 withdraw 129.134.30.0/23 at 2021-10-04 15:43:59
AS58057 withdraw 129.134.30.0/23 at 2021-10-04 15:43:59
AS34549 withdraw 185.89.218.0/23 at 2021-10-04 15:43:59
```



```
AS202365 withdraw 129.134.30.0/23 at 2021-10-04 16:07:33
AS202365 withdraw 185.89.218.0/23 at 2021-10-04 16:07:33
AS49752 withdraw 185.89.218.0/23 at 2021-10-04 16:07:34
AS49752 withdraw 129.134.30.0/23 at 2021-10-04 16:07:34
AS202365 withdraw 185.89.218.0/23 at 2021-10-04 16:07:34
AS202365 withdraw 129.134.30.0/23 at 2021-10-04 16:07:34
AS139589 withdraw 185.89.218.0/23 at 2021-10-04 16:07:34
AS139589 withdraw 129.134.30.0/23 at 2021-10-04 16:07:34
AS17639 withdraw 129.134.30.0/23 at 2021-10-04 16:07:50
AS17639 withdraw 185.89.218.0/23 at 2021-10-04 16:07:50
AS49673 withdraw 129.134.30.0/23 at 2021-10-04 16:08:01
AS49673 withdraw 185.89.218.0/23 at 2021-10-04 16:08:01
AS34800 withdraw 129.134.30.0/23 at 2021-10-04 16:08:49
AS34800 withdraw 185.89.218.0/23 at 2021-10-04 16:08:49
AS34800 withdraw 129.134.30.0/23 at 2021-10-04 16:08:49
AS34800 withdraw 185.89.218.0/23 at 2021-10-04 16:08:49
AS44393 withdraw 129.134.30.0/23 at 2021-10-04 16:08:49
AS44393 withdraw 185.89.218.0/23 at 2021-10-04 16:08:49
AS44393 withdraw 129.134.30.0/23 at 2021-10-04 16:08:49
AS44393 withdraw 185.89.218.0/23 at 2021-10-04 16:08:49
```

# IP of Alexa Top 30 Websites' Authoritative DNS Servers



(The servers' IP measured from five servers worldwide on October 10, 2021, and aggregated by prefix, AS)

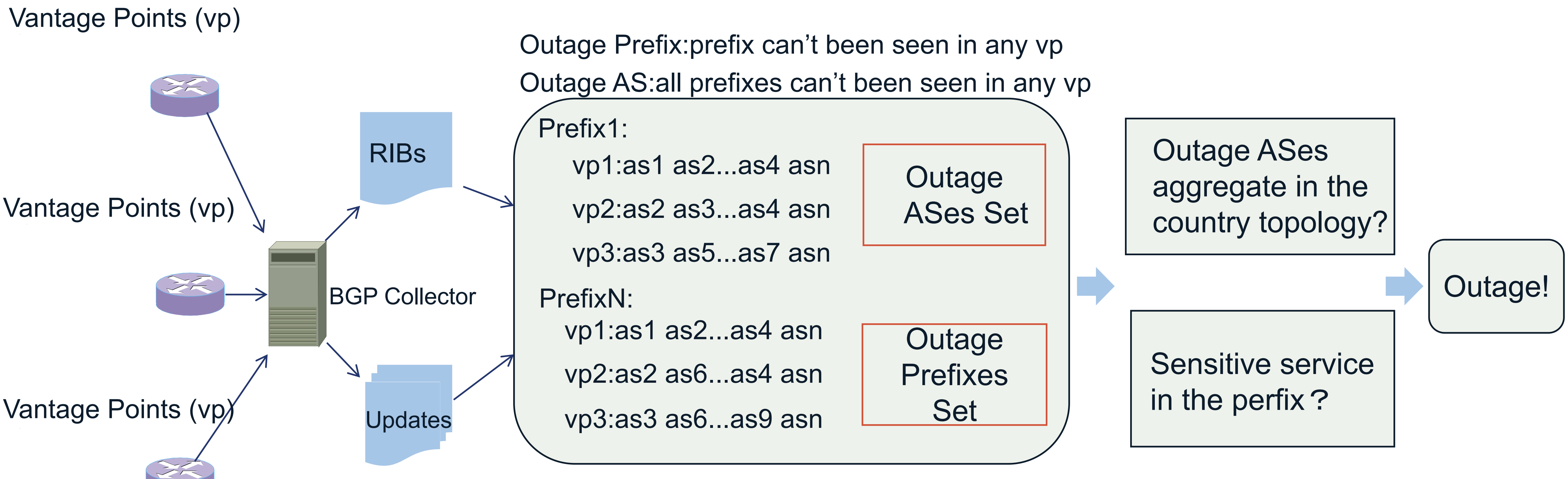
# What We Learned from these Outage Events?

BGP and DNS are critical infrastructure of the network. Any configuration operations should be strictly audited and validated. Multi-dimensional IP database is very necessary for route filtering.

Critical network infrastructure such as DNS authority servers and critical services should have redundant backup mechanisms and should not all be placed in a single prefix or AS .

The BGP anomaly monitoring system should not only focus on the false positive rate and false negative rate, but also on the sensitivity of prefixes and AS. When a anomaly detected, we should know whether the prefix or AS contains important services.

# BGP Outage Detection Architecture



Vantage Points (vp)

Vantage Points (vp)

Vantage Points (vp)

BGP Collector

RIBs

Updates

Outage Prefix:prefix can’t been seen in any vp

Outage AS:all prefixes can’t been seen in any vp

Prefix1:

vp1:as1 as2...as4 asn

vp2:as2 as3...as4 asn

vp3:as3 as5...as7 asn

Outage ASes Set

PrefixN:

vp1:as1 as2...as4 asn

vp2:as2 as6...as4 asn

vp3:as3 as6...as9 asn

Outage Prefixes Set

Outage ASes aggregate in the country topology?

Sensitive service in the perfix？

Outage!

Maintain a real-time global topology in memory

A real-time global topology is maintained in memory and checking the visibility of prefixes and AS in vantage points’ routing table, then observe whether these outage prefixes contain sensitive services and whether outage ASes have aggregation in the country’s topology.

# What IP Address and AS are Sensitive？

## IP Address

- Country’s top websites
- DNS server, PoP router
- Industrial system
- Finance, banking, energy, government services

Alexa

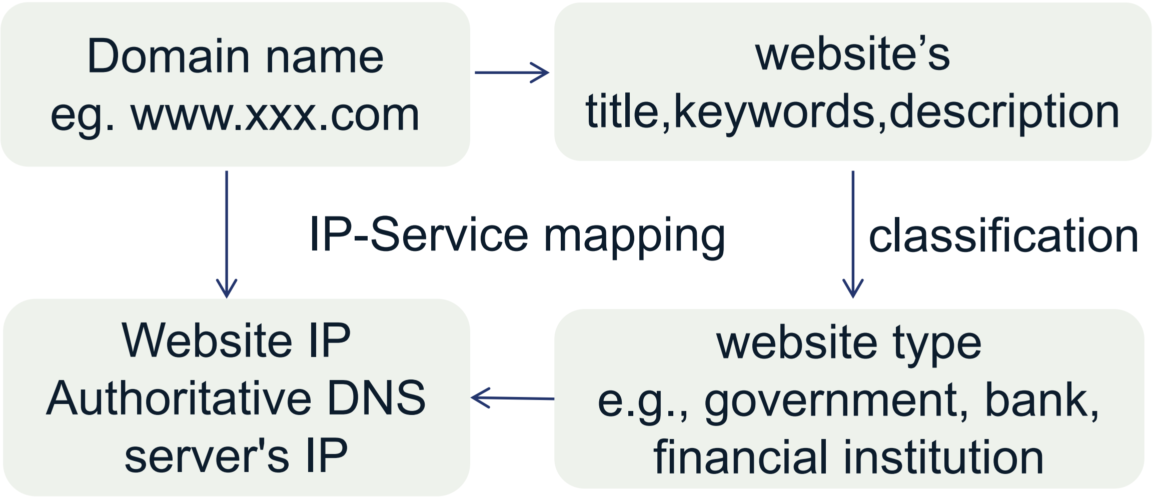
## AS

- IDC
- Cloud
- IXP
- .....

# How to Build the Database？

## Crawling, probing and analysing

- Crawl important sites, get their IP addresses and content, and then analyse the type of site based on the content (e.g., government, bank, financial institution) .
- Probe and get the authoritative DNS server's IP addresses of important web sites from different locations.
- Analyze common service ports in passive network traffic or scan the  whole IPv4 address space and get the common service ports.
- Analyse the type of AS from the textual semantics of the WHOIS database.



Domain name
eg. www.xxx.com

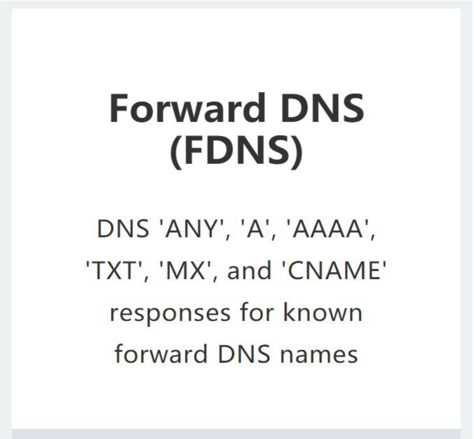
website's
title,keywords,description

IP-Service mapping

classification

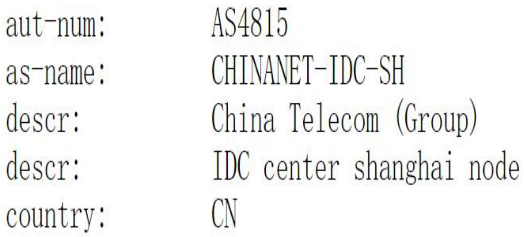
Website IP
Authoritative DNS
server's IP

website type
e.g., government, bank,
financial institution

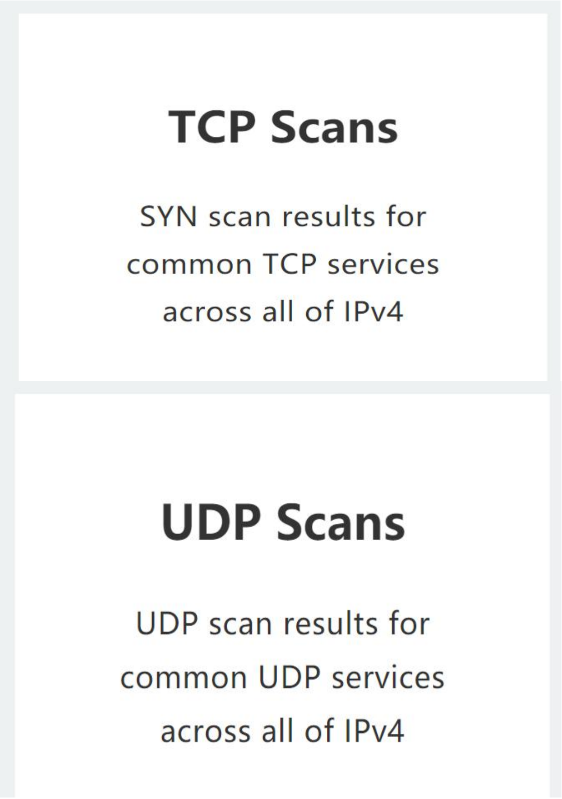


**Forward DNS (FDNS)**

DNS 'ANY', 'A', 'AAAA', 'TXT', 'MX', and 'CNAME' responses for known forward DNS names



```
aut-num:        AS4815
as-name:        CHINANET-IDC-SH
descr:          China Telecom (Group)
descr:          IDC center shanghai node
country:        CN
```



**TCP Scans**

SYN scan results for common TCP services across all of IPv4

**UDP Scans**

UDP scan results for common UDP services across all of IPv4

Thank you！