Michael Takeuchi

Cyber Security in ISP Level

19 February 2022, Online
Archonlabs CyberFest #10 Webinar

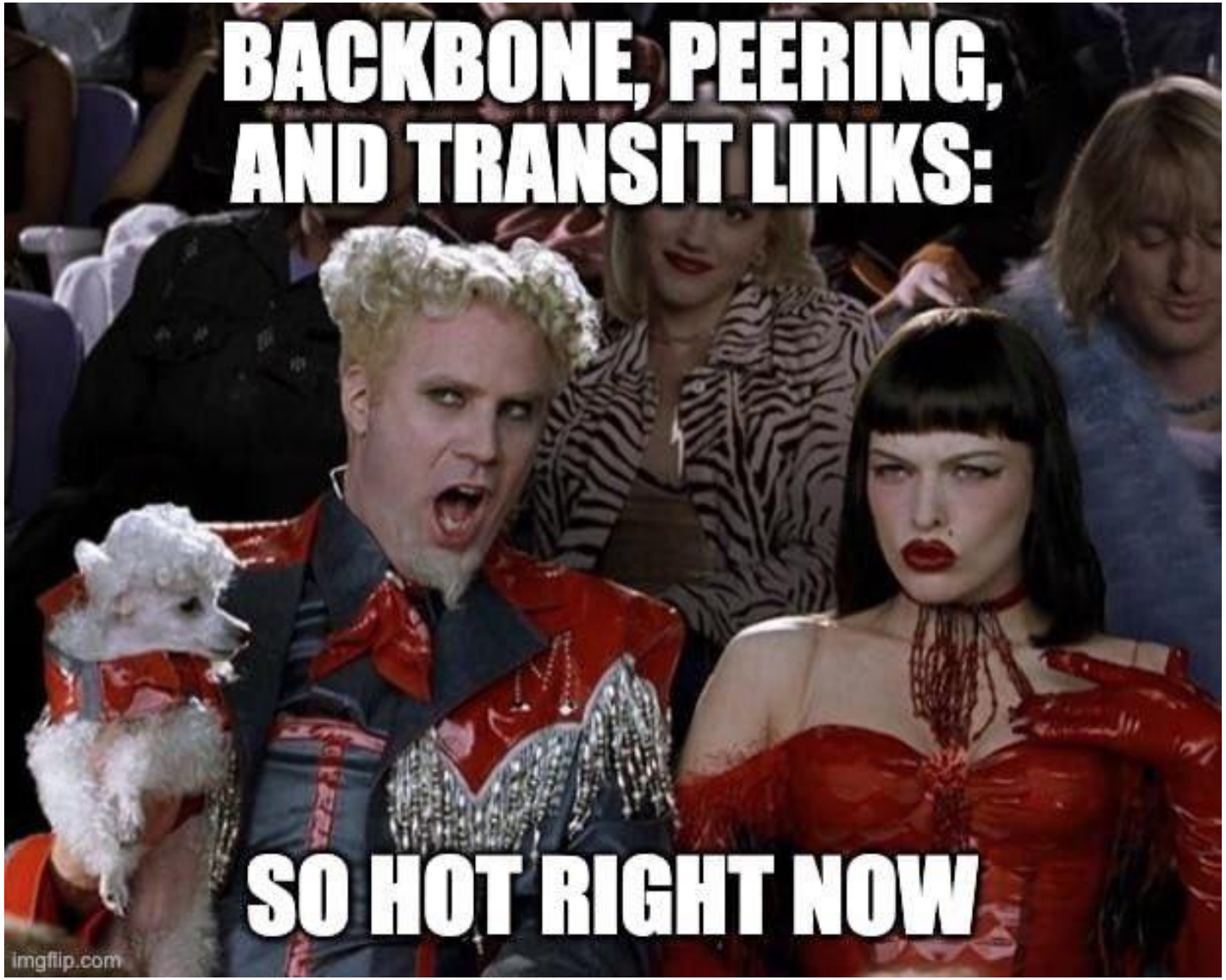
Hello, I am **Michael Takeuchi**

- Cisco Certfied CCNA & CCNP
- EC-Council Certified CEI, CEH, CND, CSA, ECIH, CTIA
- Fortinet Certified Network Security Architect (NSE 7)
- MikroTik Certified Consulant & Engineer
  (MTCNA, MTCRE, MTCINE, MTCUME, MTCTCE, MTCWE, MTCIPv6E, MTCSE)
- Juniper Certfied JNCIA-Junos, JNCDA, JNCIA-Sec, JNCIA-Cloud, JNCIA-DevOps, JNCIS-ENT, JNCIS-SP, JNCIP-DC, JNCIP-ENT, JNCIP-SP
- Managed more than 20+ Networks (ISP & non-ISP) in APAC & EMEA
- Connected to NiCE/OpenIXP, IIX, neuCentrIX, INIX, CDIX, DCI-IX, cloudXchange, Amsterdam AMS-IX, Frankfurt DE-CIX, Singapore SGIX, Equinix EIE, MegaIX & a Few Other Private Internet Exchange
- Based in Jakarta and Own ISP in Central Java 🇮🇩

https://www.linkedin.com/in/michael-takeuchi
https://www.facebook.com/mict404
https://www.takeuchi.id
michael@takeuchi.id

Cyber Security?
Internet Service Provider?


BRACE YOURSELF
PROBLEM ARE COMING


BACKBONE, PEERING,
AND TRANSIT LINKS:
SO HOT RIGHT NOW
imgflip.com


WELCOME TO THE INTERNET
I'll be your guide
motifake.com

Cyber Security Issue in Enterprise

- Computer Virus
- Data Protection
- Host Protection
- Application Security
- Policy, Regulations, Legal
- Work from Home Setup :P
- Pirated Software
- Insider Threats

Cyber Security Issue in ISP

- Flooding & DDoS Attack
- Route Leak
- BGP Hijacking
- Improper Routing Configuration in Internet Exchange
- Broadcast in Internet Exchange
- IP Address Reputation
- Policy, Regulations, Legal
- Physical Issue (FO Cable Cut, Electrical, Unintentional Issue in NER & MMR)

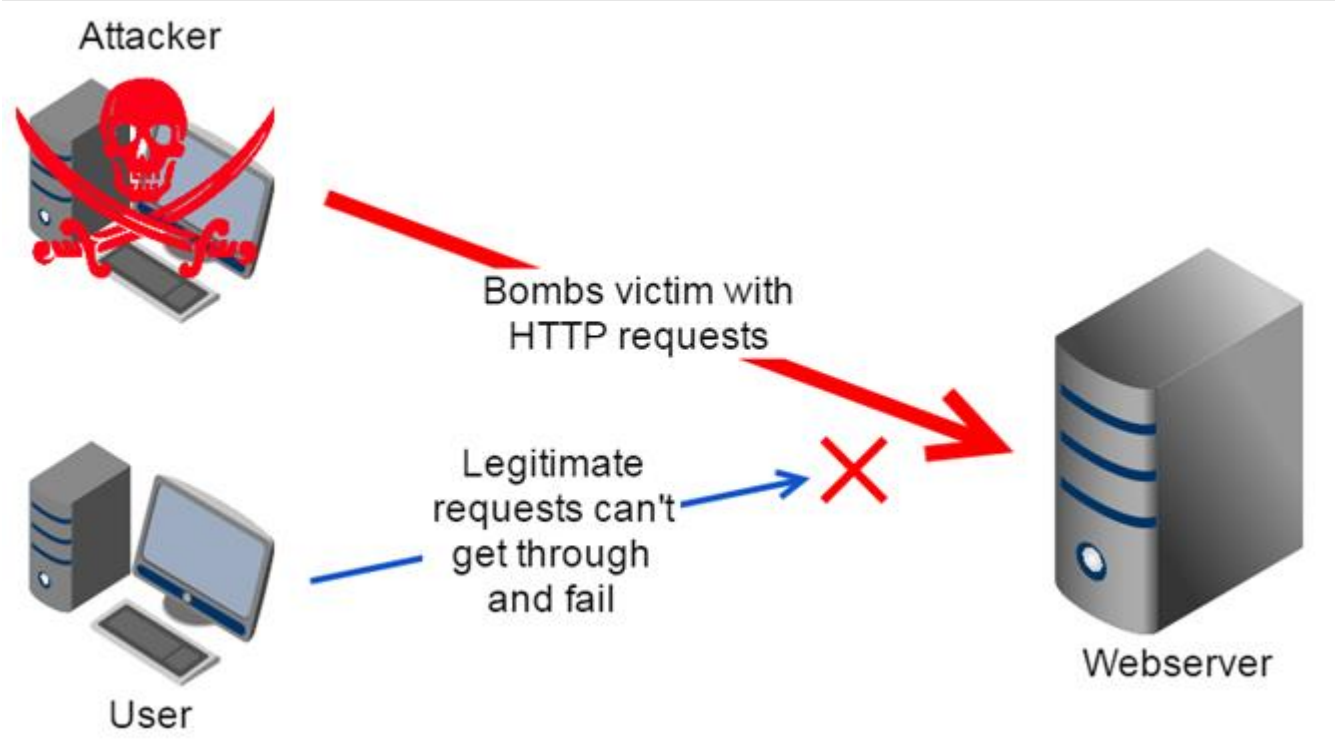
Flooding

- Imagine when 1 Little House got 1000 Guest
- In computer networking let's say, you have a router and your internet bandwidth capacity is 10Mbps but you got attack and make your link capacity is full

Request > Capacity

(more than)

Denial of Services &
Distributed Denial of Services



Images was taken from about31.net

Denial of Services *VS* Distributed Denial of Services

- DOS attacks are simultaneously launched from one sources destinated to the same target
- DDoS attacks are simultaneously launched from several sources destinated to the same target

DOS	DDoS
One Attacker to One Target	Many Attacker to One Target

Route Leak

- The Internet Engineering Task Force (IETF) in **RFC 7908** provides a working definition of a BGP Route Leak as "the propagation of routing announcement(s) beyond their intended scope.
- That is, an announcement from an Autonomous System (AS) of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, and/or one of the ASes along the preceding AS path."

Route Leak Example #1

```
Path/Ogn
 7717 179[redacted] 4800 6939 63199i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 7473 12322 20940?
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 20940i
 7717 179[redacted] 4800 6453 20940 21342i
 7717 179[redacted] 4800 6939 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 20940i
 7717 179[redacted] 4800 3741 37150 30997 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 174 12322 12322 12322 12322 20940?
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 174 6762 20940 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 6939 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 174 20940i
 7717 179[redacted] 4800 2914 20940i
 7717 179[redacted] 4800 2914 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 6939 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 6453 20940 20940i
 7717 179[redacted] 4800 174 6762 20940 20940i
 7717 179[redacted] 4800 174 6762 20940 20940i
 7717 179[redacted] 4800 6453 32787 20940 20940i
 7717 179[redacted] 4800 2914 32787 20940 20940i
 7717 179[redacted] 4800 2914 32787 20940 20940i
 7717 179[redacted] 4800 6453 32787 20940 20940i
 7717 179[redacted] 4800 1299 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 174 3257 20940 20940i
 7717 179[redacted] 4800 2914 20940i
```

- AS7717 = Internet Exchange (NiCE/OpenIXP)
- AS179** = Route Leaker
- AS4800 = AS179** Upstream
- After AS4800 = Tier 1 Networks

In Summary, AS179** was advertise some prefix that beyond their intended scope (in this case, they advertise Internet Prefix)

Route Leak Example #2

```
Path/Ogn
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859 2.4305i
    7717 638   18059 6453 21859 2.4305i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 56258 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 4788 3257 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 7473 3462 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 7473 3462 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 6453 21859i
    7717 638   18059 56258 21859i
    7717 638   18059 56258 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 4788 21859i
    7717 638   18059 4788 21859i
    7717 638   23947 3257 21859i
    7717 638   18059 6453 3356 21859 2.4305i
    7717 638   23947 6939 21859i
    7717 638   18059 6453 21859i
    7717 638   23947 6939 21859i
    7717 638   18059 56258 21859i
    7717 638   18059 7473 3462 21859i
    7717 638   18059 58463 1299 8781 21859i
    7717 638   18059 4788 6774 21859i
    7717 638   18059 4788 21859i
```

- Similar Issue, can you guess the answer?

Internet Exchange = ???

Route Leaker = ???

Route Leaker Upstream = ???

What They Leak = ???

BGP Hijacking

- So? What's the problem?

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE FORUMS

THE POWER OF FALSE ADVERTISING —

How an Indonesian ISP took down the mighty Google for 30 minutes

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

Declan McCullagh Feb. 25, 2008 4:28 p.m. PT

Yesterday morning we posted a tweet (below) that Amazon's authoritative DNS service had been impacted by a routing (BGP) hijack. Little did we know this was part of an elaborate scheme to use the inherent security weaknesses of DNS and BGP to pilfer crypto currency, but that remarkable scenario appears to have taken place.

InternetIntelligence
@InternetIntel

BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today:
205.251.192.0/24
205.251.193.0/24
205.251.195.0/24
205.251.197.0/24
205.251.199.0/24

245 9:52 PM - Apr 24, 2018

275 people are talking about this

CLOUDFLARE The Cloudflare Blog

Contact Sales: +1 (888) 274-3482

Thanks for being here, come back soon. Get notified of new posts:

Email Address Subscribe

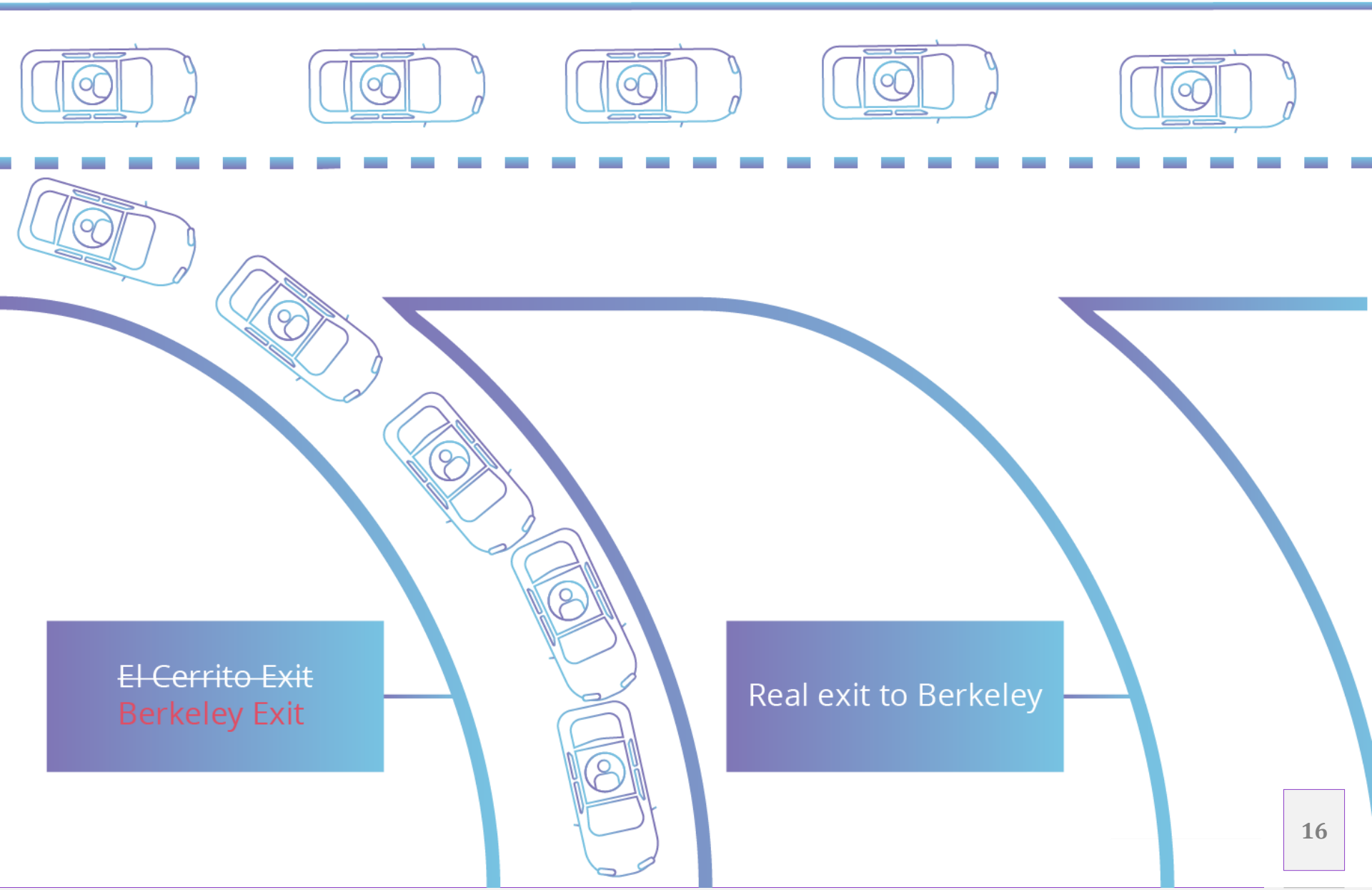
Product News | Speed & Reliability | Security | Serverless | Cloudflare Network | Developers | Deep Dive | Life @Cloudflare

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today

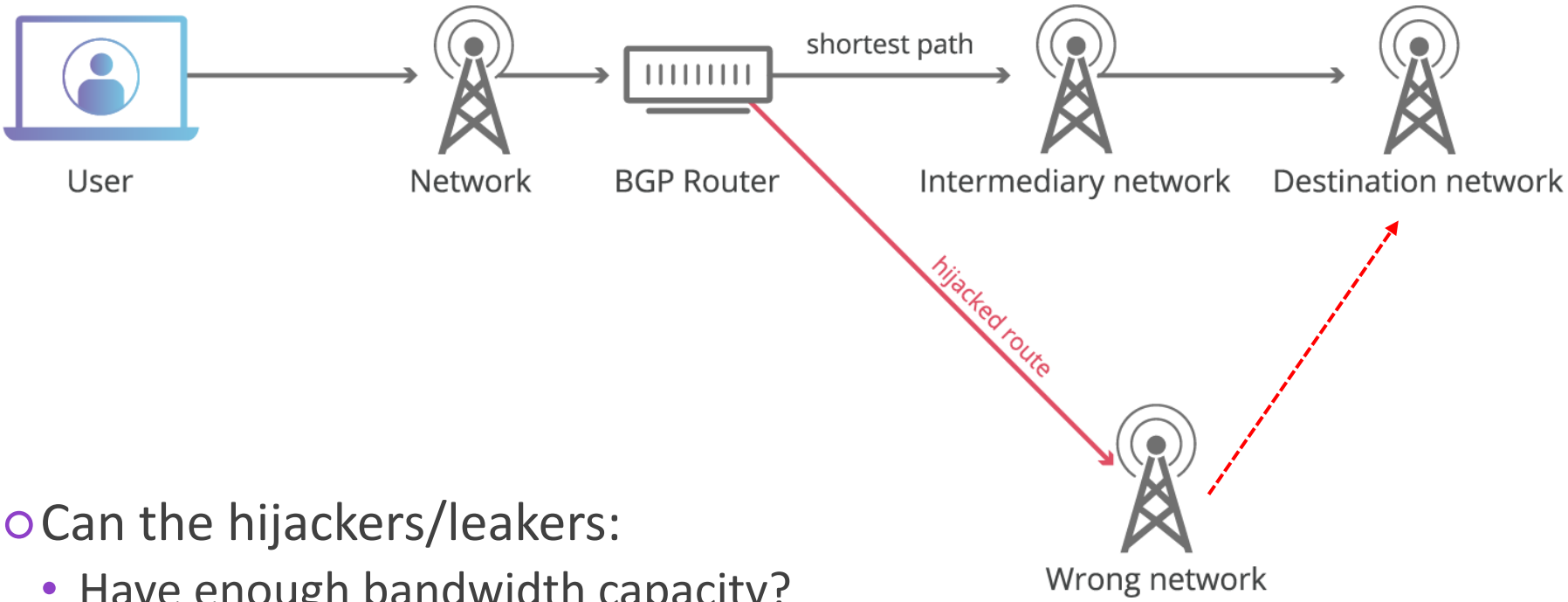
June 25, 2019 2:58 AM

https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

BGP Hijacking



BGP Hijacking



- Can the hijackers/leakers:
  - Have enough bandwidth capacity?
  - Keep our network quality of services good?
  - Leading us to the right server or content that we want?

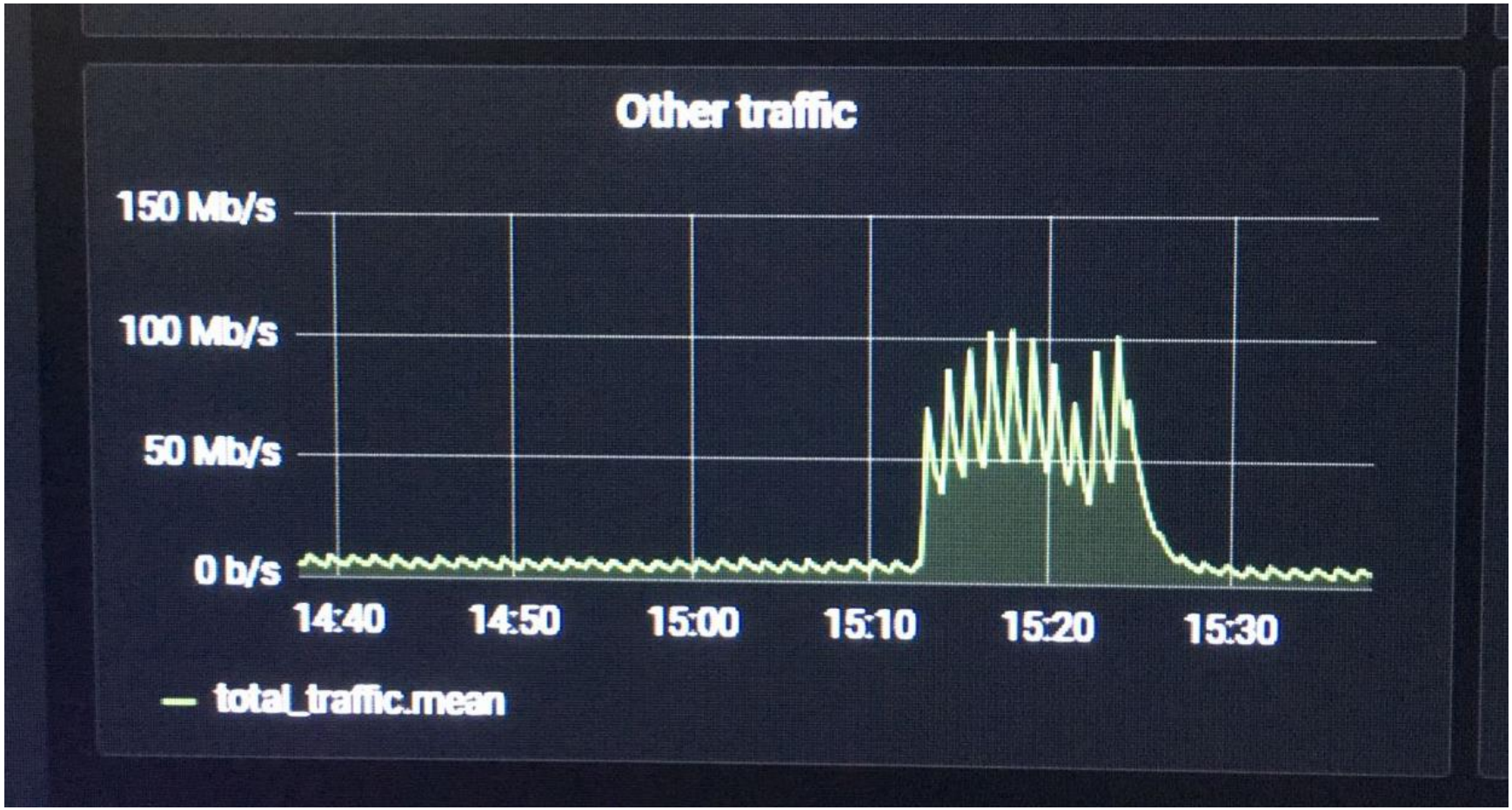
https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

Improper Routing Configuration in Internet Exchange

Improper Routing Configuration in Internet Exchange

```
103.28.74.129          7597     107544      76479       0       0 3w3d 5:05:14 Establ
  inet.0: 2192/15012/9984/0
103.28.74.222          7597       9625       3366       0       1  1d 1:34:42 Establ
  inet.0: 1374/7280/6770/0
103.28.74.255          7597     115132      76478       0       0 3w3d 5:05:10 Establ
  inet.0: 2311/15007/10007/0
103.28.75.222          7597       9936       3367       0       2  1d 1:35:05 Establ
  inet.0: 5277/7320/6810/0

{master}
[redacted]> show route advertising-protocol bgp 103.28.74.222

{master}
[redacted]> show route advertising-protocol bgp 103.28.75.222

{master}
[redacted]> show route advertising-protocol bgp 103.28.74.129

{master}
[redacted]> show route advertising-protocol bgp 103.28.74.255

{master}
[redacted]>
```

Improper Routing Configuration in Internet Exchange



Improper Routing Configuration in Internet Exchange

#GerakanAntiStaticRouting

#BukanHasilStaticRouting

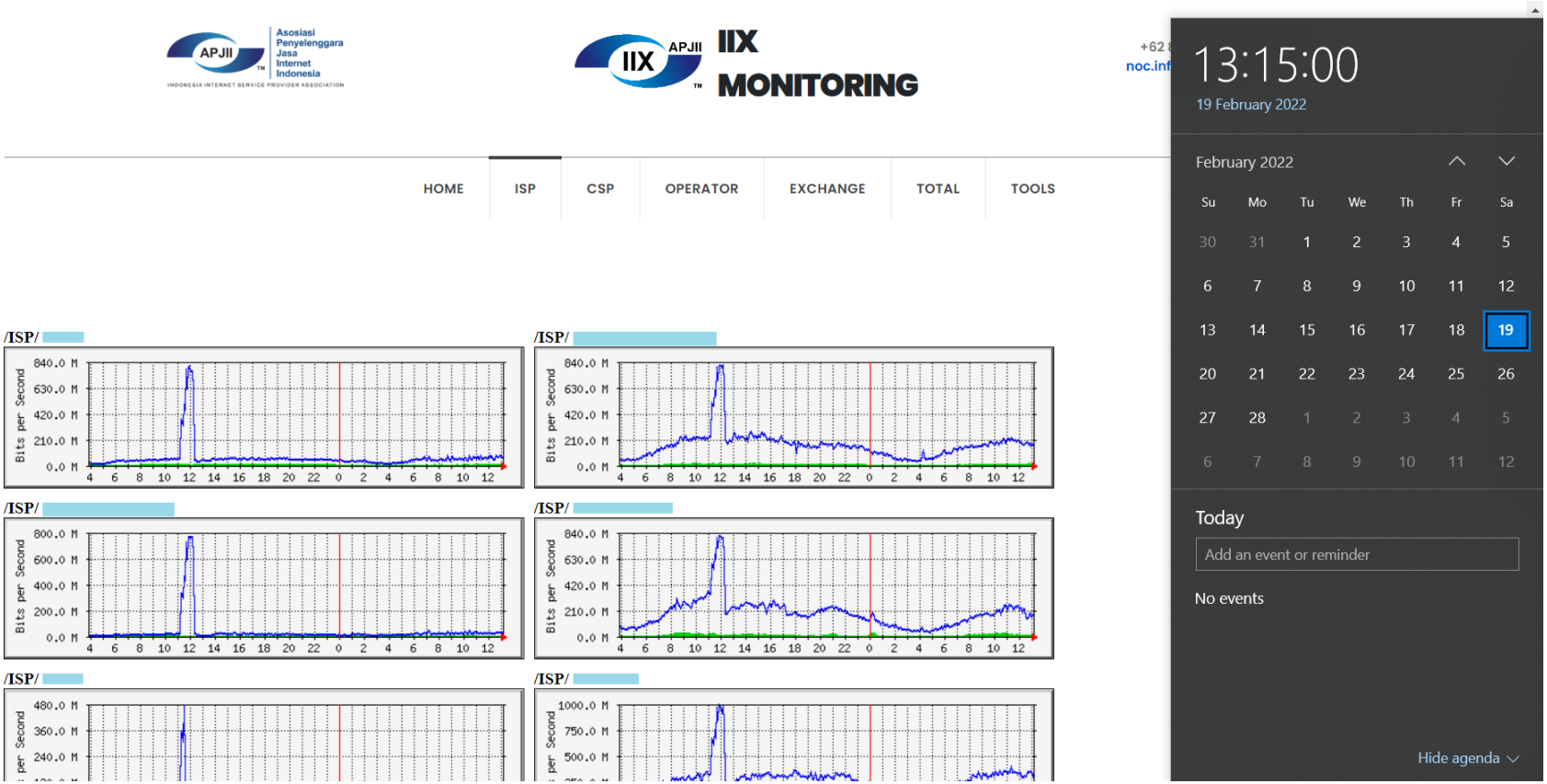
Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

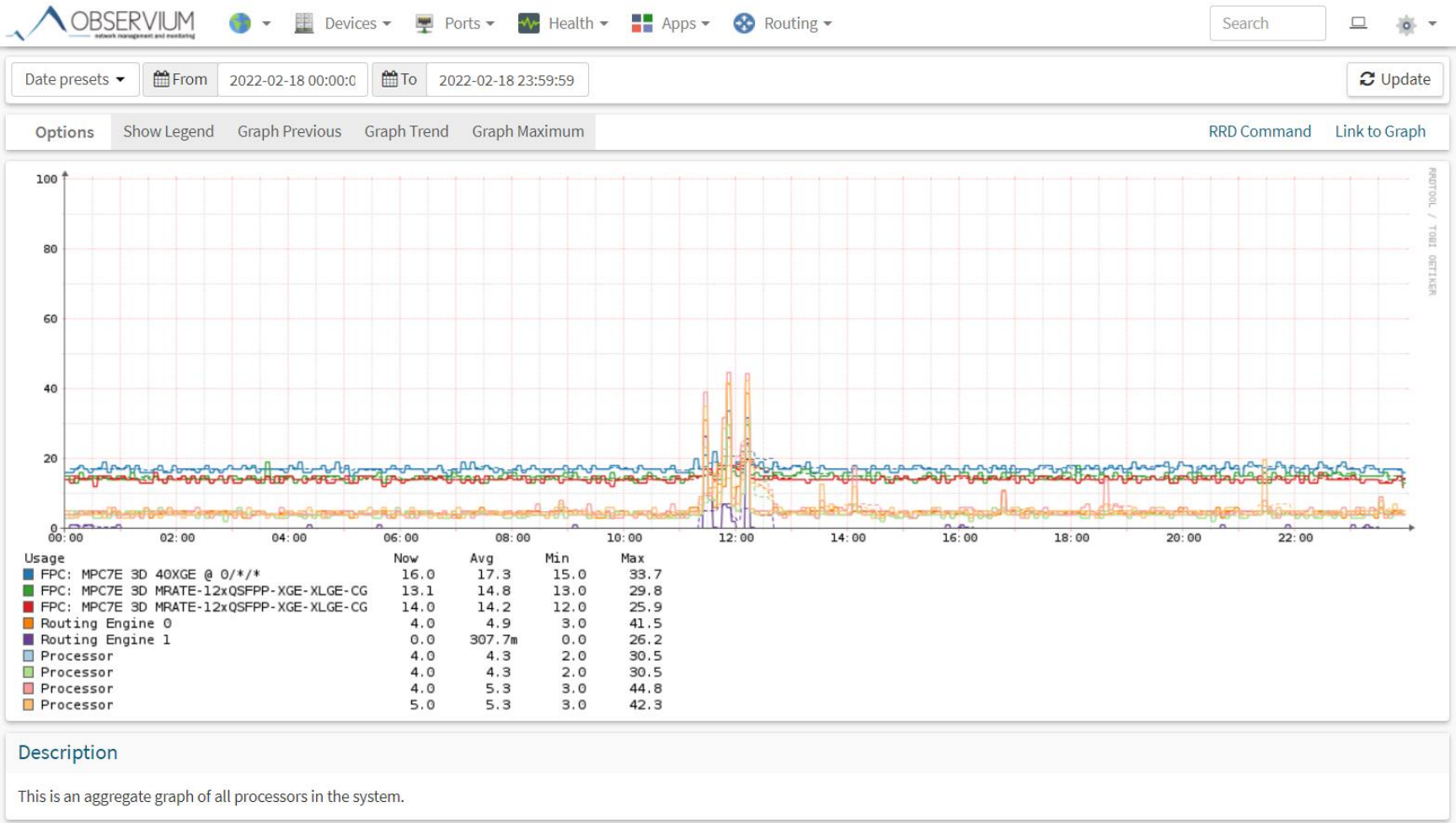
Reset Counters | Reset All Counters

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface
0	accept	prerouting						ether5-IIX
1	accept	prerouting						ether5-IIX
2	accept	prerouting						ether5-IIX
3	accept	prerouting						ether5-IIX
4	accept	prerouting						ether5-IIX
5	accept	prerouting		103.136				ether5-IIX
6	accept	prerouting		103.141				ether5-IIX
7	accept	prerouting		103.241				ether5-IIX
8	accept	prerouting						ether5-IIX
9	accept	prerouting						
10	drop	prerouting						ether5-IIX

Broadcast in Internet Exchange



Broadcast in Internet Exchange



IP Reputation

- Reputation that we know is an opinion about that entity, typically as a result of social evaluation on a set of criteria. And this one also applicable on Computer Networking
- If we see reputation by person, in Computer Networking we see reputation by IP Address

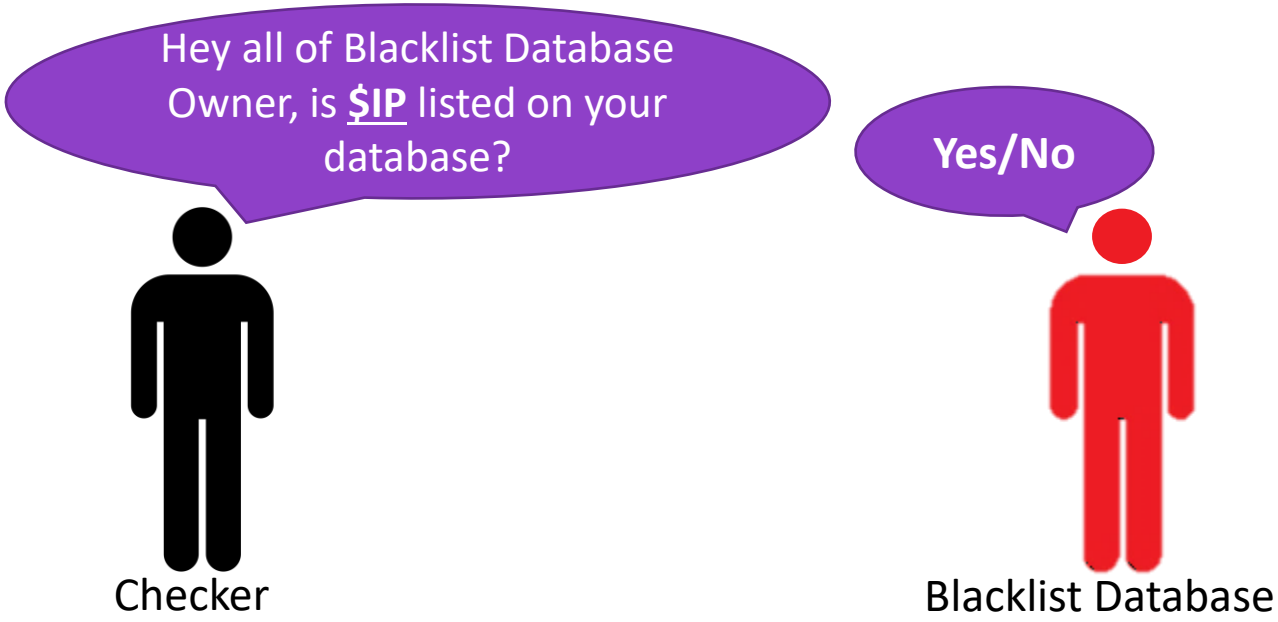
Reputation Check
(Online Reputation Checker)

- https://bgp.he.net
- https://mxtoolbox.com/blacklists.aspx
- https://www.dnsbl.info

etc.

Reputation Check (How it works?)

How it works?



Reputation Check (Blacklist Database)

IP Info | Whois | DNS | RBL

Failed 0 out of 105 tests.

access.redhawk.org	PASS
all.spamblock.unit.liu.se	PASS
b.barracudacentral.org	PASS
bl.deadbeef.com	PASS
bl.emailbasura.org	PASS
bl.spamcannibal.org	PASS
bl.spamcop.net	PASS
blackholes.five-ten-sg.com	PASS
blackholes.mail-abuse.org	PASS
blacklist.sci.kun.nl	PASS
blacklist.woody.ch	PASS
bogons.cymru.com	PASS
bsb.spamlookup.net	PASS
cbl.abuseat.org	PASS
cbl.anti-spam.org.cn	PASS
cblless.anti-spam.org.cn	PASS
cblplus.anti-spam.org.cn	PASS
cdl.anti-spam.org.cn	PASS
combined.njabl.org	PASS

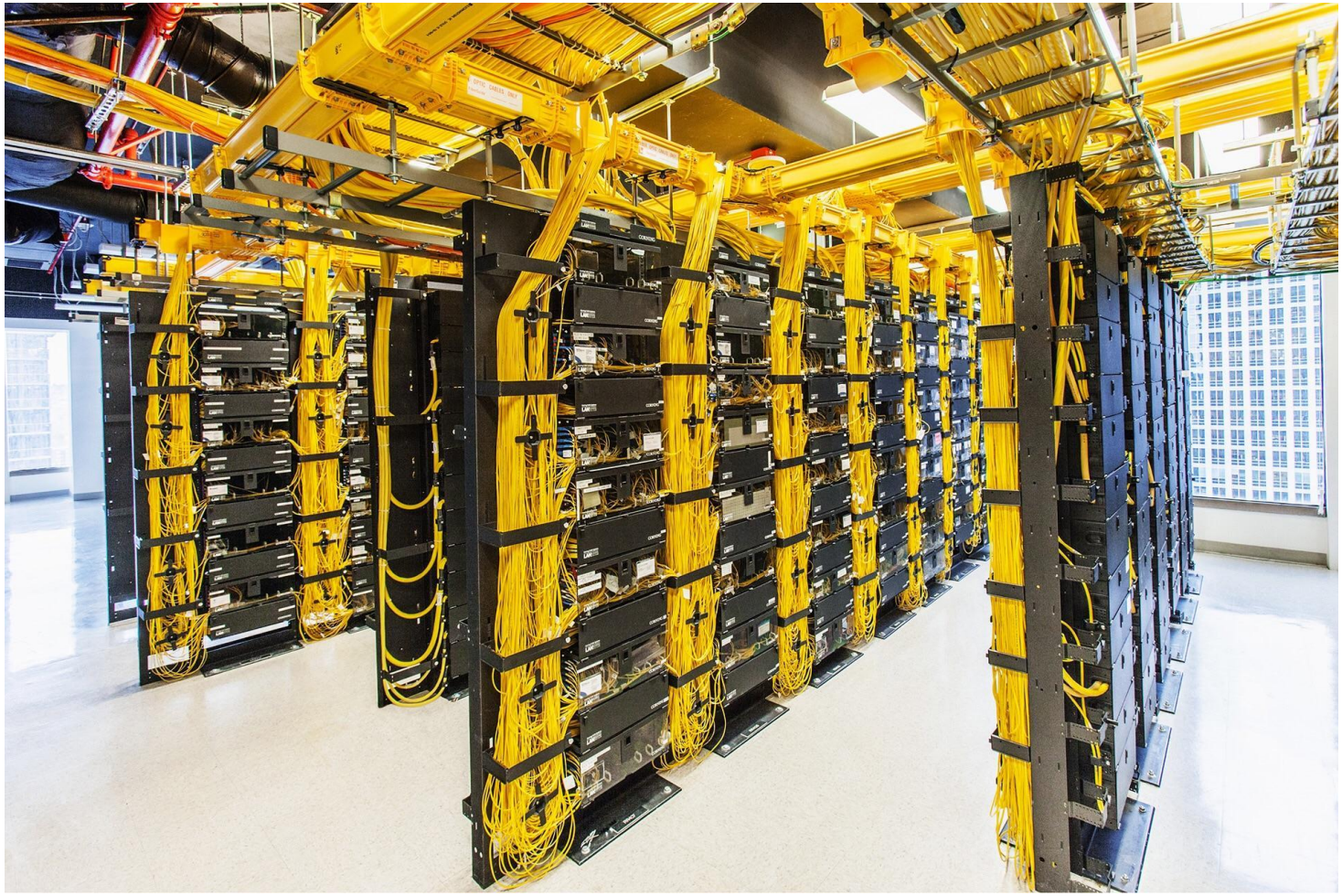
This is only few of many Blacklist Database from bgp.het.net online reputation checker

Policy, Regulations, Legal

Physical Issue – FO Cable Cut

Physical Issue – Electrical

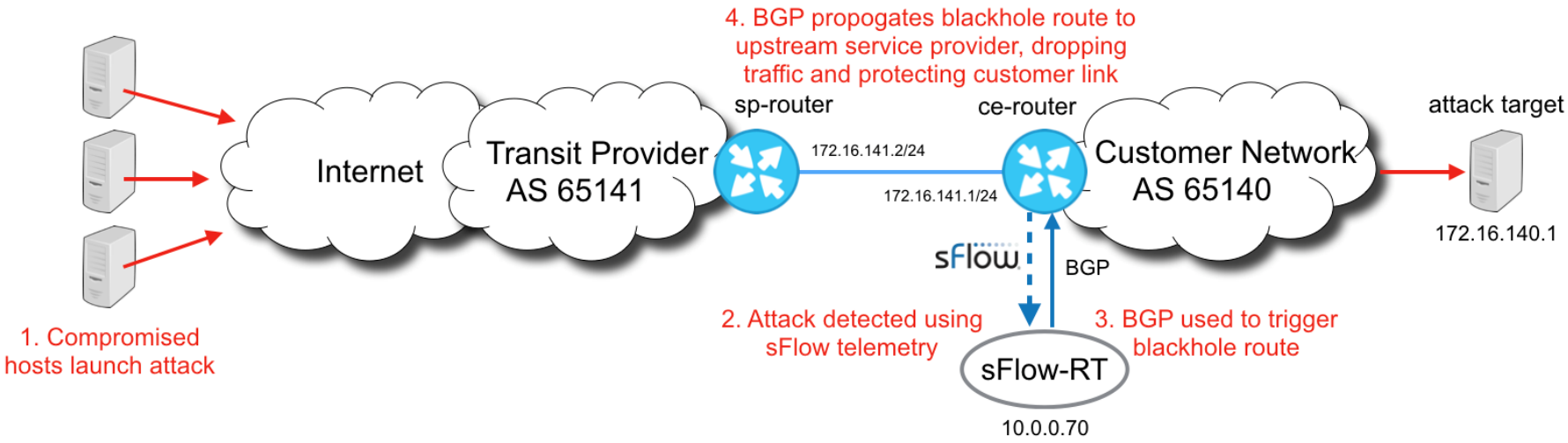
Physical Issue – Unintentional Issue in NER & MMR



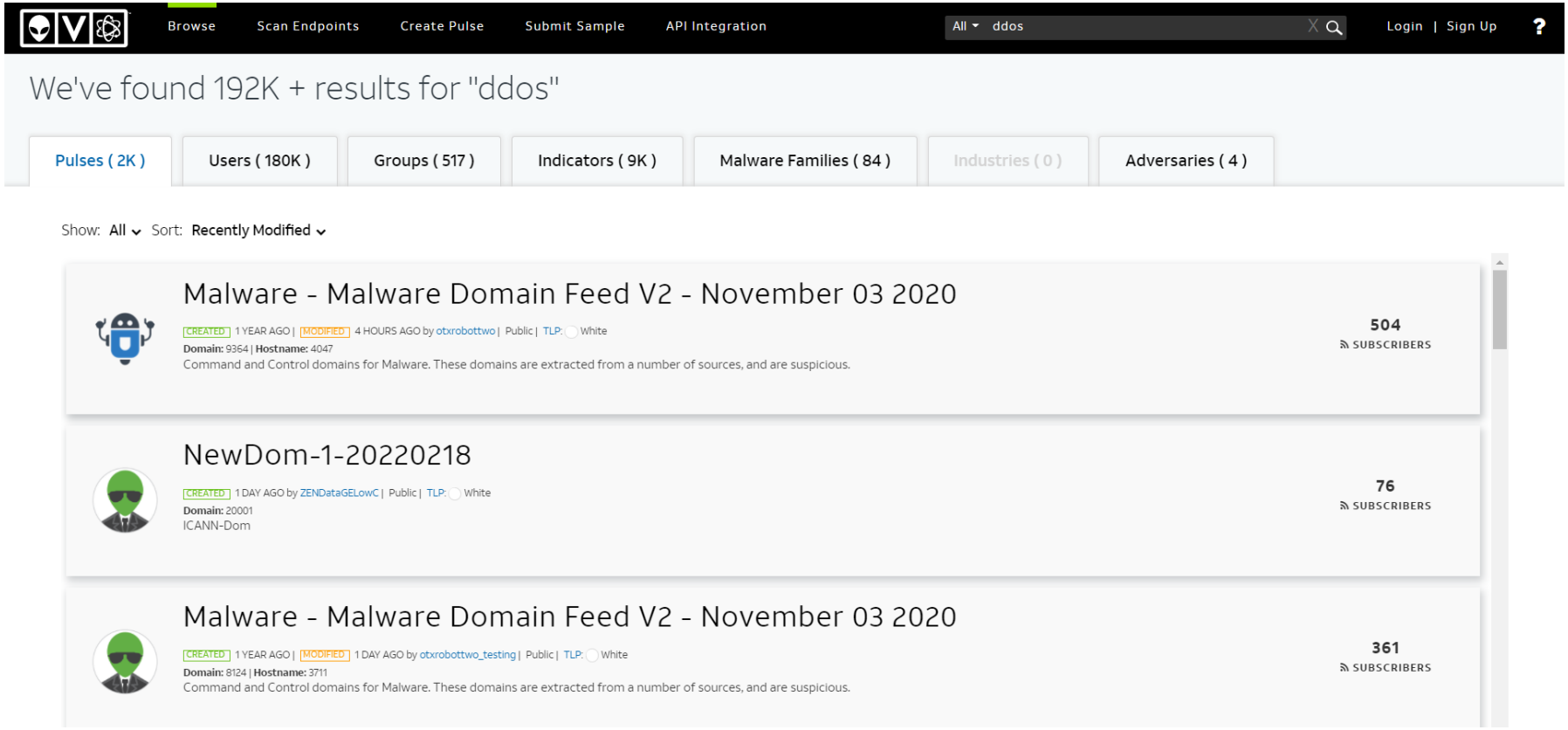
Solution?

- Just like diapers that can mitigate “problem” come out
- We need to have something like diapers in our network :)

Solution #1 – Flooding & DDoS Attack



Solution #1 – Flooding & DDoS Attack



Solution #2 – Route Leak, BGP Hijacking & Improper Config

MANRS

Mutually **A**greed **N**orms for **R**outing **S**ecurity

Solution #2 – Route Leak, BGP Hijacking & Improper Config

How MANRS can resolve the problem: MANRS outlines four simple but concrete actions that network operators should take:

- **Filtering** – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity
- **Anti-spoofing** – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure
- **Coordination** – Maintain globally accessible up-to-date contact information. Also, we should use PeeringDB to update the peering information.
- **Global Validation** – Publish your data, so others can validate routing information on a global scale. You can validate your route using IRR and RPKI.

Solution #3 – IP Reputation

Bad IP Reputation has a few root cause, you need to identify your network and monitor your IP RBL (Realtime Blackhole List) and always check your abuse contact mailbox here is some root cause that makes your IP have a bad reputation

- Malicious/Anomalies Traffic
  - Botnet
  - Flooding
  - Spamming
  - Denial of Services/Distributed Denial of Services
- Bruteforce Login
- Copyright Infringement

etc.

Solution #4 – Broadcast in Internet Exchange

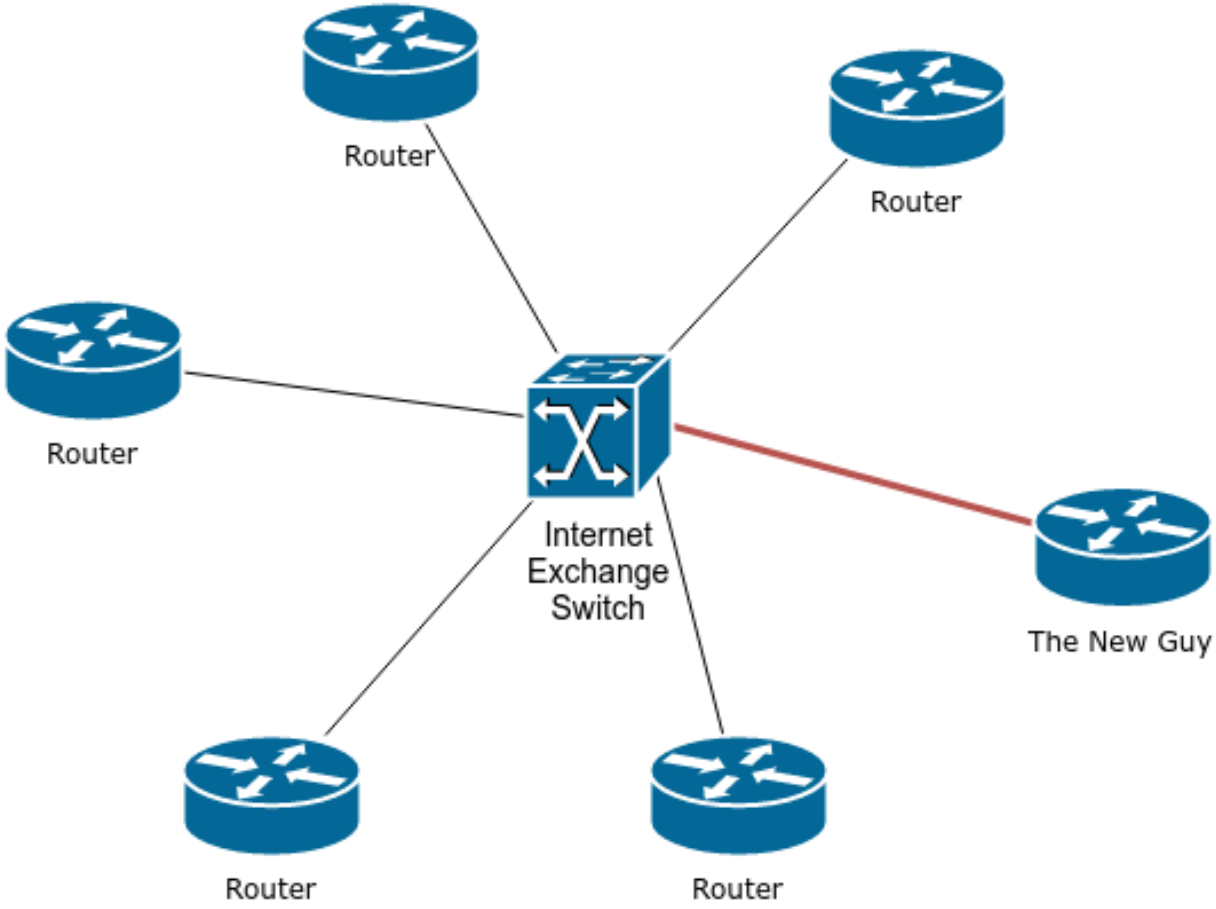
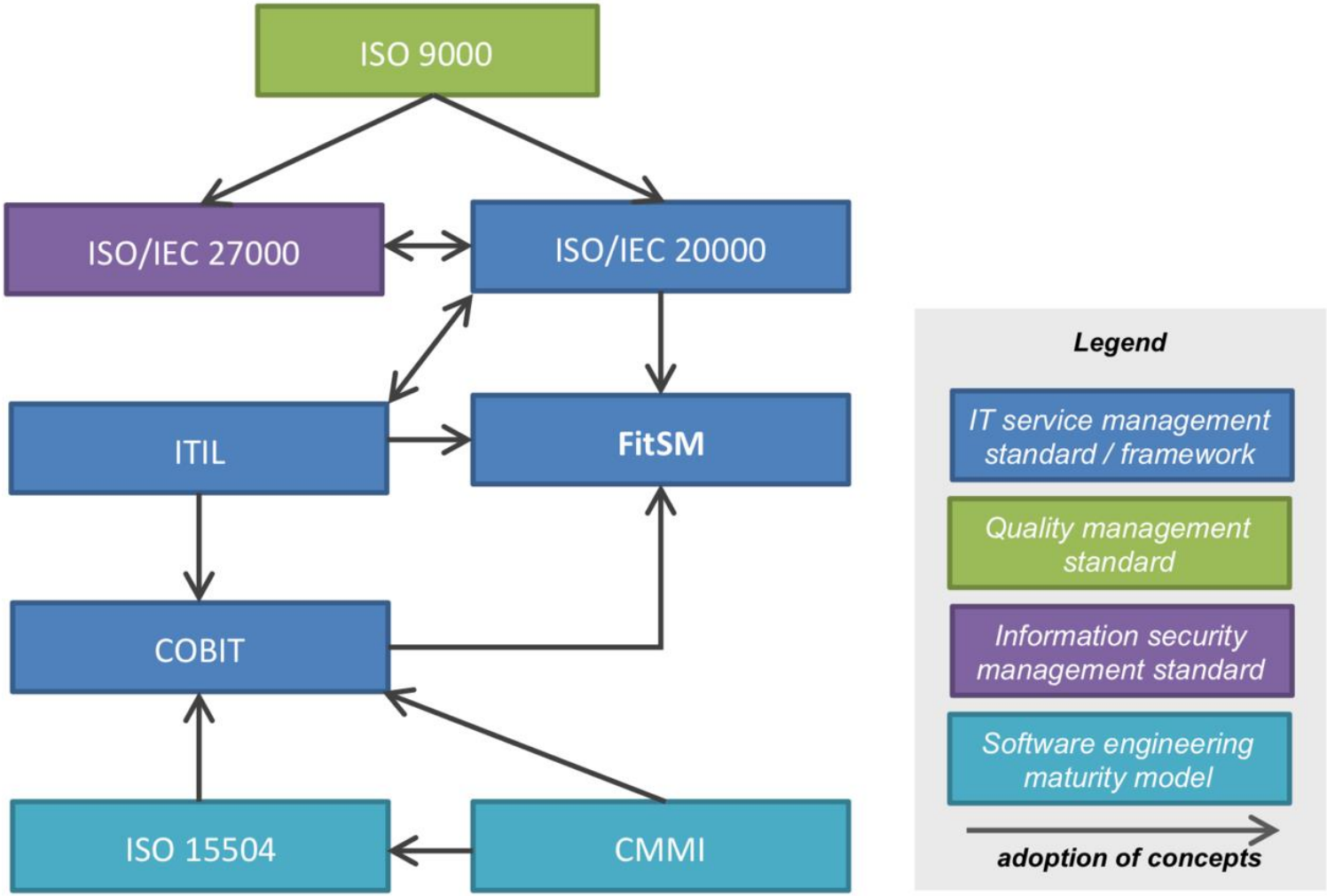


Image was taken from blog.thelifeofkenneth.com

Solution #5 – Policy, Regulations, Legal



Solution #6 – Physical Issue

- Fiber Cable Cut
  - Have more than 1 link for redundancy
- Electrical
  - Have dual source electrical & PSU
  - Provide UPS (Uninterruptible Power Supply)
  - Proper Data Center
  - DRC Data Center
- Unintentional Issue in NER & MMR
  - Proper Data Center Policy
  - Well-trained Technician
  - Good Cable Management

Question & Answer


Thank you