BGP and Attacks on BGP

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Learning Internet Structure from Traceroute

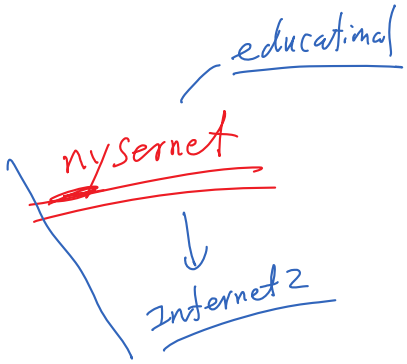
```
$ tracert www.syr.edu

Tracing route to syr.edu [128.230.171.184]
over a maximum of 30 hops:

  1     5 ms     4 ms     5 ms  192.168.0.1
  2     8 ms    14 ms     9 ms  142.254.213.97
  3    14 ms    21 ms    21 ms  tge0-0-3.fyvlnyhe01h.northeast.rr.com [24.24.16.81]
  4   143 ms     6 ms    10 ms  24.58.52.164
  5    16 ms    23 ms    15 ms  be27.albynyyf01r.northeast.rr.com [24.58.32.80]
  6    29 ms    36 ms    24 ms  bu-ether46.nycmny837aw-bcr00.tbone.rr.com [107.14.19.102]
  7    23 ms    28 ms    34 ms  0.ae2.pr0.nyc20.tbone.rr.com [107.14.19.147]
  8    25 ms    23 ms    24 ms  be7843.ccr21.jfk10.atlas.cogentco.com [154.54.10.137]
  9    25 ms    27 ms    26 ms  be2056.ccr41.jfk02.atlas.cogentco.com [154.54.44.217]
 10   201 ms   208 ms   204 ms  be2106.ccr21.alb02.atlas.cogentco.com [154.54.3.50]
 11    31 ms    30 ms    30 ms  be2770.rcr11.syr01.atlas.cogentco.com [154.54.41.133]
 12    30 ms    30 ms    32 ms  38.122.120.10
 13    35 ms    31 ms    33 ms  core1-bb-87-41.syr.edu [128.230.87.41]
 14    35 ms    30 ms    31 ms  g7000-061-018.syr.edu [128.230.61.18]
 15    33 ms    37 ms    30 ms  syr.edu [128.230.171.184]
```

Case Study: Traceroute From SU

```
helios 1: traceroute www.uci.edu
traceroute to www.uci.edu (128.195.188.232), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  0.892 ms  0.778 ms  0.656 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  0.471 ms  0.356 ms  0.376 ms
 3  128.230.61.113 (128.230.61.113)  0.481 ms  0.420 ms  0.379 ms
 4  syr-9208-syru.nysernet.net (199.109.9.5)  0.487 ms  0.391 ms  0.383 ms
 5  buf-9208-syr-9208.nysernet.net (199.109.7.194)  3.716 ms  3.617 ms  3.623 ms
 6  I2-CHIC-buf-9208.nysernet.net (199.109.11.38)  17.934 ms  17.823 ms  17.937 ms
 7  et-10-0-0.106.rtr.kans.net.internet2.edu (198.71.45.15)  28.873 ms  33.293 ms  29.035 ms
 8  et-1-0-0.109.rtr.hous.net.internet2.edu (198.71.45.16)  43.343 ms  43.516 ms  43.531 ms
 9  et-5-0-0.111.rtr.losa.net.internet2.edu (198.71.45.21)  75.942 ms  75.855 ms  75.854 ms
10  137.164.26.200 (137.164.26.200)  75.956 ms  75.861 ms  75.862 ms
11  hpr-uci-uci1--lax-hpr2-egm.cenic.net (137.164.27.42)  109.379 ms  77.887 ms  79.609 ms
12  * * *
13  * * *
```




```
helios 2: traceroute www.google.com
traceroute to www.google.com (172.217.4.68), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  1.101 ms  1.221 ms  0.656 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  10.585 ms  198.110 ms  0.619 ms
 3  te0-0-1-3.rcr11.syr01.atlas.cogentco.com (38.122.120.9)  0.910 ms  1.352 ms  0.946 ms
 4  be2770.ccr21.alb02.atlas.cogentco.com (154.54.41.134)  4.139 ms  3.900 ms  4.045 ms
 5  be2106.ccr41.jfk02.atlas.cogentco.com (154.54.3.49)  7.225 ms  7.142 ms  7.113 ms
 6  be2060.ccr21.jfk05.atlas.cogentco.com (154.54.31.10)  7.371 ms  7.422 ms  7.536 ms
 7  tata.jfk05.atlas.cogentco.com (154.54.12.18)  7.089 ms  7.136 ms  6.980 ms
 8  if-ae-12-2.tcore1.N75-New-York.as6453.net (66.110.96.5)  10.172 ms  7.274 ms  7.274 ms
 9  72.14.195.232 (72.14.195.232)  7.770 ms 72.14.214.68 (72.14.214.68)  7.300 ms  7.303 ms
10  209.85.248.242 (209.85.248.242)  7.909 ms 216.239.50.106 (216.239.50.106)  7.874 ms  7.870 ms
11  209.85.240.113 (209.85.240.113)  8.066 ms  8.150 ms  7.982 ms
12  lga15s47-in-f4.1e100.net (172.217.4.68)  7.624 ms  7.711 ms  7.547 ms
```

```
helios 3: traceroute www.washington.edu
traceroute: Warning: www.washington.edu has multiple addresses; using 128.95.155.134
traceroute to www.washington.edu (128.95.155.134), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  0.924 ms  8.933 ms  0.807 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  77.346 ms  1.178 ms  200.802 ms
 3  128.230.61.113 (128.230.61.113)  0.468 ms  0.417 ms  0.375 ms
 4  syr-9208-syru.nysernet.net (199.109.9.5)  0.483 ms  0.362 ms  0.385 ms
 5  buf-9208-syr-9208.nysernet.net (199.109.7.194)  3.703 ms  3.724 ms  3.610 ms
 6  I2-CHIC-buf-9208.nysernet.net (199.109.11.38)  17.921 ms  17.785 ms  17.949 ms
 7  et-10-0-0.106.rtr.kans.net.internet2.edu (198.71.45.15)  29.152 ms  29.027 ms  29.047 ms
 8  et-4-0-0.110.rtr.salt.net.internet2.edu (198.71.45.19)  49.110 ms  49.010 ms  49.148 ms
 9  et-5-0-0.113.rtr.seat.net.internet2.edu (198.71.45.25)  64.993 ms  64.761 ms  64.886 ms
10  64.57.28.54 (64.57.28.54)  64.990 ms  65.269 ms  65.010 ms
11  ae0--4002.icar-sttl1-1.infra.pnw-gigapop.net (209.124.181.132)  65.133 ms  65.177 ms  65.161 ms
12  ae0--4002.uwbr-ads-1.infra.washington.edu (209.124.181.133)  65.271 ms  65.322 ms  65.315 ms
13 ^C
```

```
helios 4: traceroute www.microsoft.com
traceroute to www.microsoft.com (104.88.99.161), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  0.896 ms  0.656 ms  0.523 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  0.335 ms  0.337 ms  0.378 ms
 3  te0-0-1-3.rcr11.syr01.atlas.cogentco.com (38.122.120.9)  1.043 ms  0.909 ms  1.084 ms
 4  be2770.ccr21.alb02.atlas.cogentco.com (154.54.41.134)  3.866 ms  3.863 ms  4.045 ms
 5  be2106.ccr41.jfk02.atlas.cogentco.com (154.54.3.49)  7.075 ms  7.254 ms  7.264 ms
 6  be2056.ccr21.jfk10.atlas.cogentco.com (154.54.44.218)  7.510 ms  7.428 ms  7.811 ms
 7  ae-6.r08.nycmny01.us.bb.gin.ntt.net (154.54.12.146)  7.519 ms  7.696 ms  7.279 ms
 8  ae-3.r07.nycmny01.us.bb.gin.ntt.net (129.250.6.176)  7.638 ms  7.546 ms  7.270 ms
 9  * *^C
```

```
helios 5: traceroute www.mit.edu
traceroute to www.mit.edu (104.88.95.69), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  0.738 ms  1.211 ms  0.528 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  0.464 ms  0.341 ms  0.377 ms
 3  te0-0-1-3.rcr11.syr01.atlas.cogentco.com (38.122.120.9)  0.924 ms  0.921 ms  0.798 ms
 4  be2770.ccr21.alb02.atlas.cogentco.com (154.54.41.134)  3.858 ms  3.880 ms  4.171 ms
 5  be2106.ccr41.jfk02.atlas.cogentco.com (154.54.3.49)  7.094 ms  7.399 ms  7.390 ms
 6  be2056.ccr21.jfk10.atlas.cogentco.com (154.54.44.218)  7.361 ms  7.661 ms  7.410 ms
 7  ae-6.r08.nycmny01.us.bb.gin.ntt.net (154.54.12.146)  8.780 ms  7.526 ms  7.397 ms
 8  ae-3.r07.nycmny01.us.bb.gin.ntt.net (129.250.6.176)  7.229 ms  7.393 ms  7.126 ms
 9  * *^C
```

```
helios 6: traceroute www.harvard.edu
traceroute: Warning: www.harvard.edu has multiple addresses; using 54.240.190.74
traceroute to www.harvard.edu (54.240.190.74), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  7.490 ms  1.294 ms  0.929 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  0.311 ms  0.325 ms  0.382 ms
 3  te0-0-1-3.rcr11.syr01.atlas.cogentco.com (38.122.120.9)  0.910 ms  0.916 ms  0.948 ms
 4  be2770.ccr21.alb02.atlas.cogentco.com (154.54.41.134)  4.004 ms  4.010 ms  4.027 ms
 5  be2106.ccr41.jfk02.atlas.cogentco.com (154.54.3.49)  6.949 ms  7.200 ms  7.121 ms
 6  be2324.ccr21.jfk04.atlas.cogentco.com (154.54.47.18)  7.360 ms  7.634 ms  7.670 ms
 7  qwest.jfk04.atlas.cogentco.com (154.54.10.50)  6.930 ms  7.224 ms  6.977 ms
 8  *^C
```

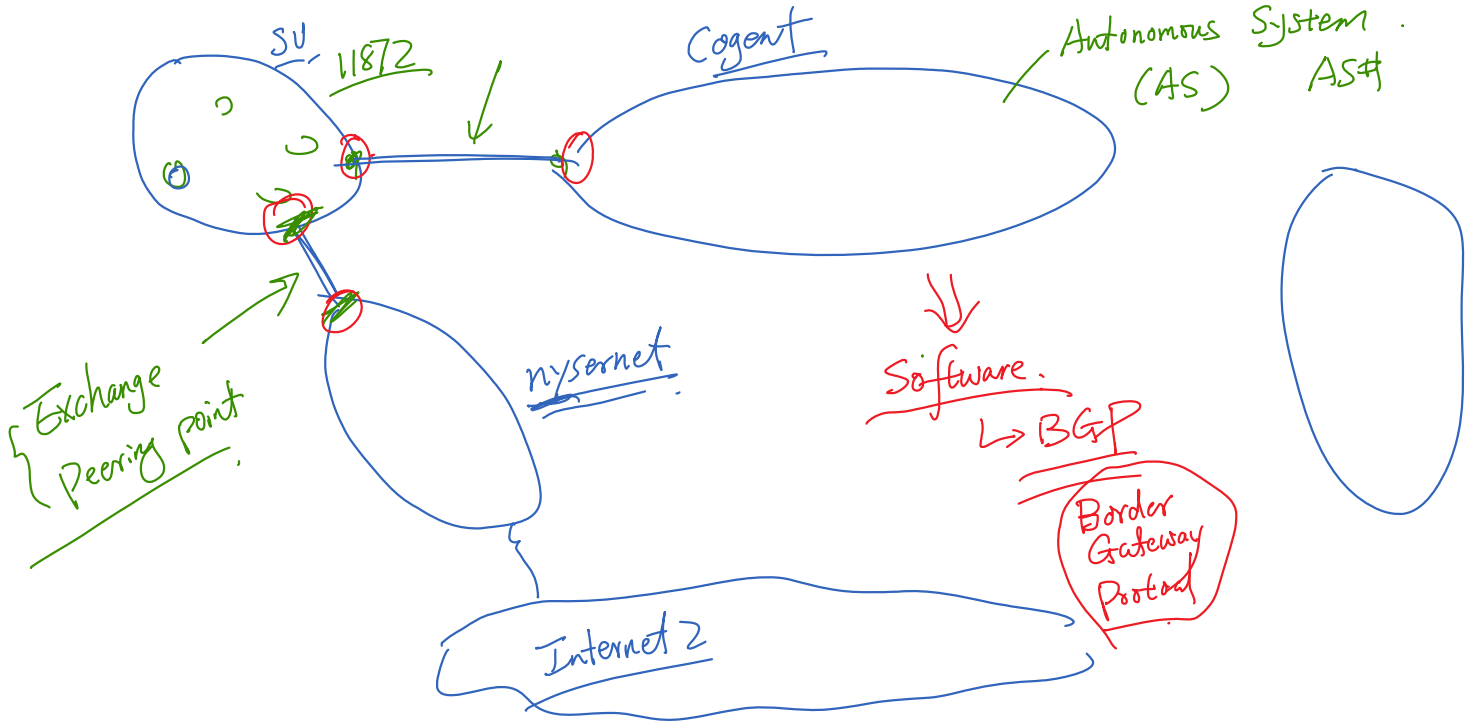
```
helios 7: traceroute www.bu.edu
traceroute: Warning: www.bu.edu has multiple addresses; using 128.197.26.35
traceroute to www.bu.edu (128.197.26.35), 30 hops max, 40 byte packets
 1  128.230.208.2 (128.230.208.2)  1.002 ms  0.620 ms  0.658 ms
 2  backboneb-87-42.syr.edu (128.230.87.42)  0.340 ms  0.341 ms  0.378 ms
 3  128.230.61.113 (128.230.61.113)  0.622 ms  0.416 ms  0.383 ms
 4  syr-9208-syru.nysernet.net (199.109.9.5)  0.475 ms  0.356 ms  0.371 ms
 5  buf-9208-syr-9208.nysernet.net (199.109.7.194)  3.715 ms  3.729 ms  3.759 ms
 6  I2-CLEV-buf-9208.nysernet.net (199.109.11.34)  8.082 ms  8.256 ms  8.111 ms
 7  nox1sumgw1-i2-re.nox.org (192.5.89.17)  21.567 ms  21.475 ms  21.316 ms
 8  192.5.89.21 (192.5.89.21)  16.504 ms  16.585 ms  16.533 ms
 9  bu-re-nox300gw1.nox.org (192.5.89.46)  16.643 ms  16.704 ms  16.824 ms
10  cumm111-core-aca01-gi2-7-comm595-bdr-gw01-gi1-1.bu.edu (128.197.254.117)  16.358 ms  16.261 ms  16.404 ms
11  buic010-dist-aca01-te5-4-cumm111-core-aca01-te3-2.bu.edu (128.197.254.146)  18.046 ms  16.413 ms  16.673 ms
12  www.bu.edu (128.197.26.35)  21.564 ms  21.753 ms  21.459 ms
```

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

How the Internet Is Connected

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

How the Internet Is Connected: High-Level Picture

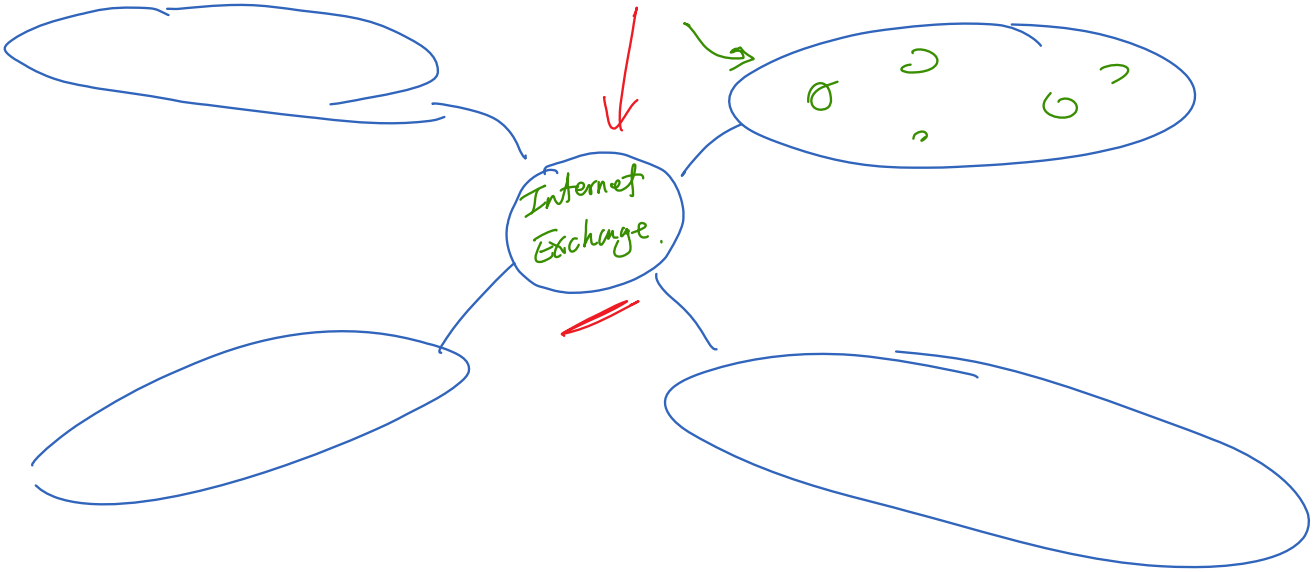


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

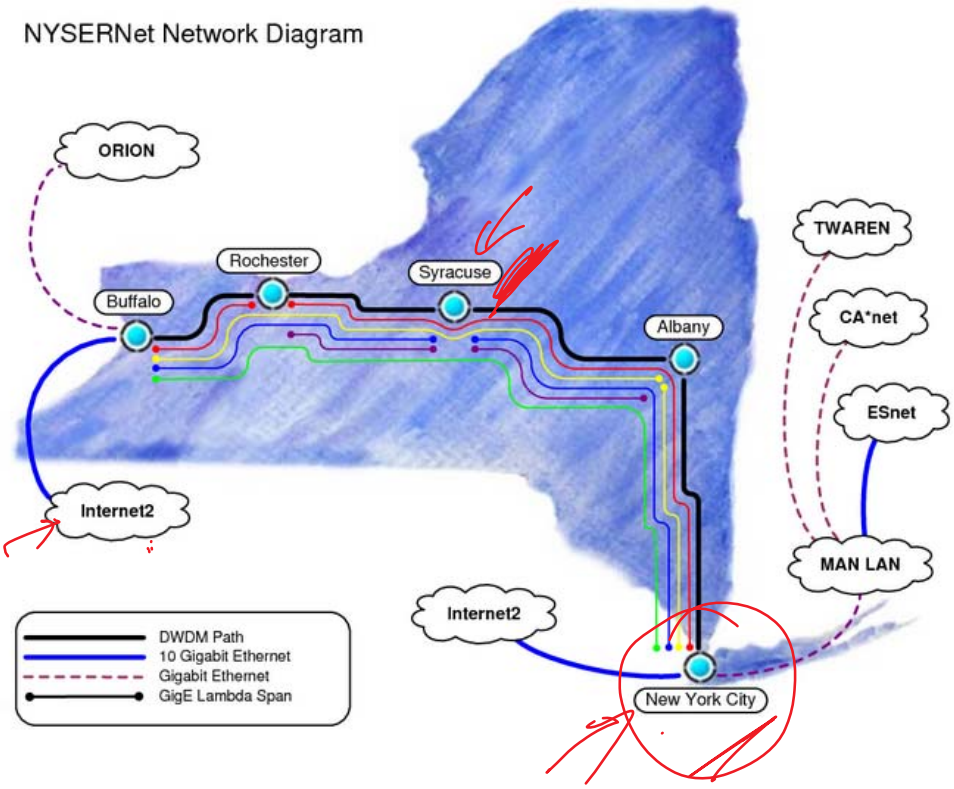
How Backbones Are Connected Physically

Laying Cables

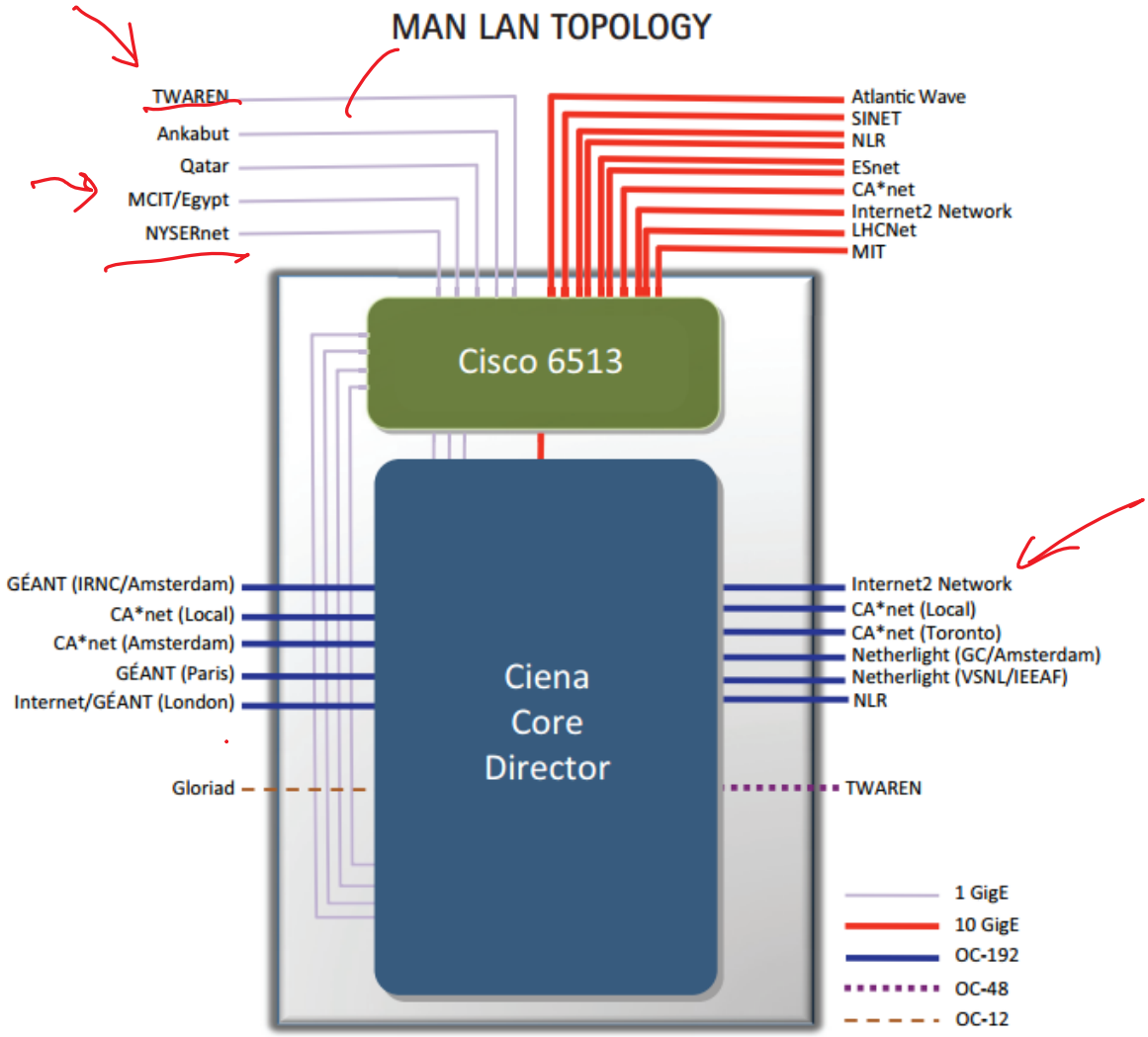
Internet Exchange and Peering



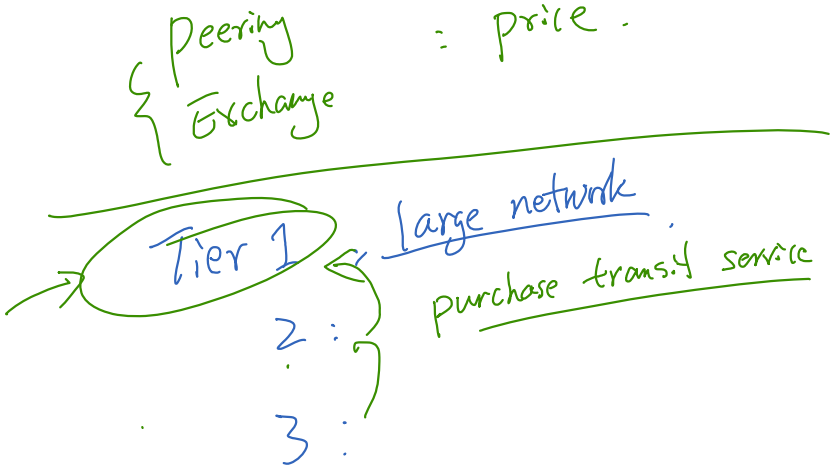
NYSERNet

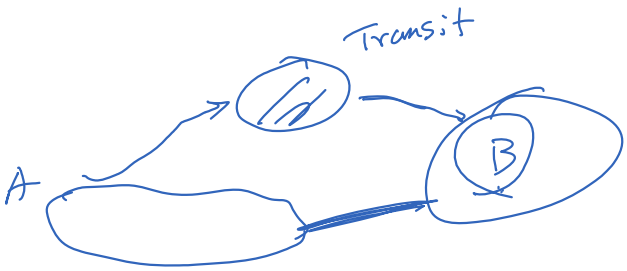

NYSERNet Network Diagram
ORION
Rochester
Buffalo
Syracuse
Albany
TWAREN
CA*net
ESnet
MAN LAN
Internet2
Internet2
New York City
DWDM Path
10 Gigabit Ethernet
Gigabit Ethernet
GigE Lambda Span

Manhattan Landing Exchange Point



Network Tiers





List of Tier-1 Networks

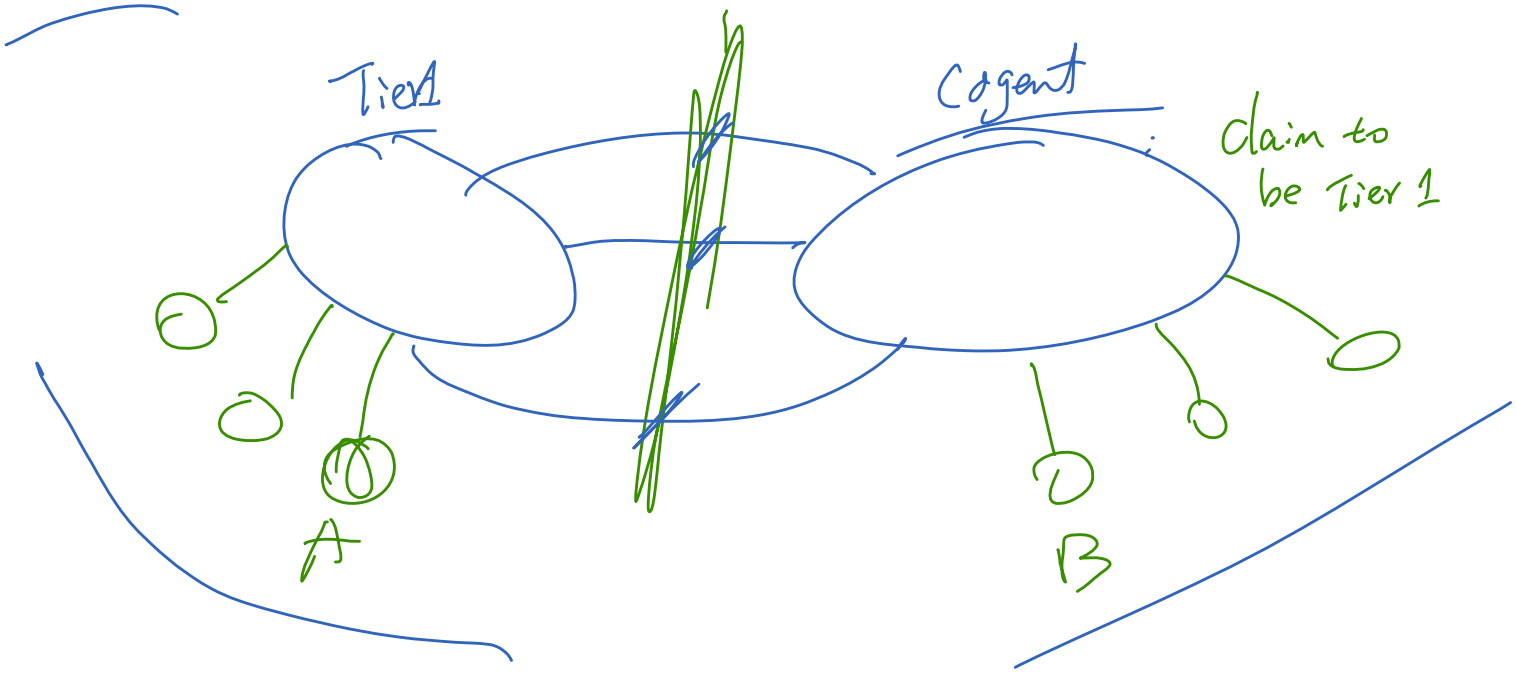
Name	Headquarters	AS number
AT&T Inc.	USA	7018
CenturyLink (formerly Qwest and Savvis)	USA	209 / 3561
Deutsche Telekom AG (now known as International Carrier Sales & Solutions (ICSS))	Germany	3320
XO Communications	USA	2828
Telecom Italia Sparkle (Seabone)	Italy	6762
Inteliquent (formerly Tinet)	USA	3257
Verizon Business (formerly UUNET)	USA	701
Sprint	USA	1239
TeliaSonera International Carrier	Sweden	1299
NTT Communications (formerly Verio)	Japan	2914
Level 3 Communications (formerly Level 3 and Global Crossing)	USA	3356 / 3549 / 1
Tata Communications (formerly Teleglobe)	India	6453
Telefonica	Spain	12956
Zayo Group formerly AboveNet	USA	6461

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Disputes Related to Peering and Connections

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Level 3 vs. Cogent Dispute (2005)



Netflix, Comcast, Level 3, and Verizon Disputes

Netflix pays Verizon for network connection to speed up video

Netflix confirms deal that's similar to agreement with Comcast.

by **Jon Brodkin** - Apr 28 2014, 6:11pm EDT

BROADBAND 65

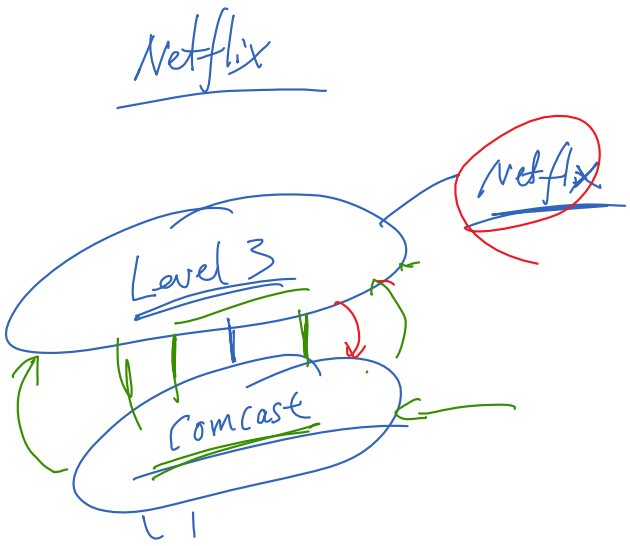
Netflix to Pay Comcast for Smoother Streaming

Deal Ends Standoff, Might Serve as Precedent for Relations With Other Broadband Suppliers

Feb. 23, 2014

In exchange for payment, Netflix will get direct access to Comcast's broadband network.

The deal is a milestone in the history of the Internet, where content providers like Netflix generally have not had to pay for access to the customers of a broadband provider.



Netflix, Level 3, and Comcast

But in November 2010, the two firms became locked in a bitter dispute. Level 3 had just won a contract to deliver content for Netflix, one of the internet's largest video services. Anticipating that Netflix would generate more traffic than the existing links between the Comcast and Level 3 networks could accommodate, Level 3 proposed installing additional links between the networks. Ordinarily, Comcast, as a Level 3 customer, would gladly accept what was essentially a free upgrade. Instead, Comcast refused to accept the new connections unless Level 3 agreed to pay Comcast for the additional traffic. And Level 3, after voicing strong objections, paid up.

More Disputes

Why YouTube buffers: The secret deals that make—and break—online video

When ISPs and video providers fight over money, Internet users suffer.

by **Jon Brodkin** - July 28 2013, 9:00pm EDT

BROADBAND NETWORKING THE WEB 236

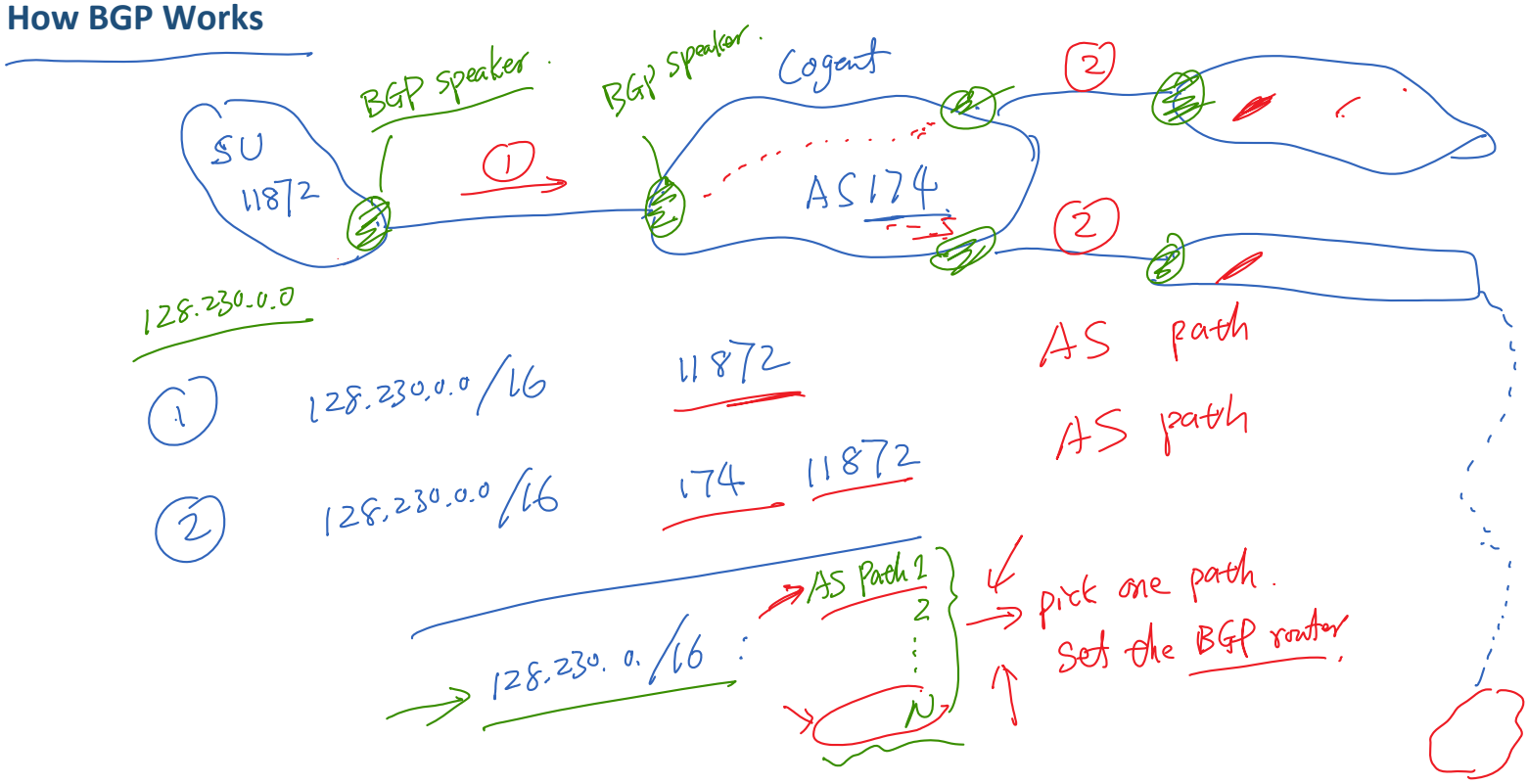
- **November 2010**: After Internet backbone provider Level 3 signs a deal with Netflix to distribute video, Comcast demands money from Level 3 for carrying traffic over the proverbial "last mile" to Comcast subscribers.
- **January 2011**: European ISPs Deutsche Telekom, Orange (formerly France Telecom), Telecom Italia, and Telefónica commission a report saying companies like Netflix and Google's YouTube service should give ISPs a lot more money.
- **August 2011**: Cogent, another Internet backbone provider that handles Netflix traffic, files a complaint in France against Orange, saying the ISP is providing inadequate connection speeds.
- **January 2013**: Free, a French ISP, is accused of slowing down YouTube traffic by failing to upgrade infrastructure (but is later cleared of intentionally degrading YouTube traffic by the French regulator). Free also temporarily blocks ads on YouTube and other video services by sending an update to its modems.
- **January 2013**: Orange and Google have a similar dispute, with Orange CEO Stephane Richard claiming victory. He says that Google is paying Orange to compensate the operator for mobile traffic sent from Google servers.
- **January 2013**: Time Warner refuses Netflix's offer of a free caching service that would provide better performance to Netflix users on Time Warner's network.
- **June 2013**: Cogent accuses Verizon of allowing "ports" between the two providers to fill up, degrading Netflix performance for Verizon customers.
- **July 2013**: The European Commission opens an antitrust probe into whether ISPs abused market positions in negotiations with content providers, and it searches the offices of Orange, Deutsche Telekom, and Telefónica. Separately, the French government demands details of interconnection agreements involving AT&T and Verizon.

In the most extreme cases, large Internet companies stop passing traffic to one another entirely. (This happened in 2005 with France Telecom and Cogent, in 2005 with Cogent and Level 3, and in 2008 with Sprint and Cogent.) But recent disputes have been less likely to lead to a complete severing of ties. "That type of reaction to a policy is becoming less common, possibly because it's so easy to publicize it," Reggie Forster, director of network engineering at XO Communications, told Ars. "They tend to want to keep that quiet."

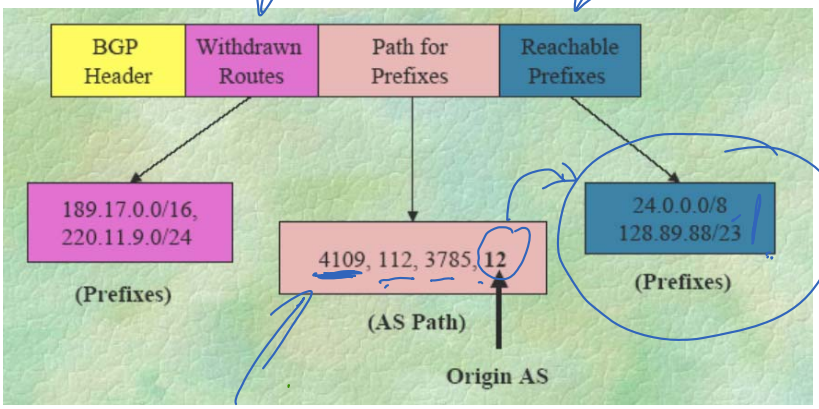
SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

How Networks Are "Glued" Together

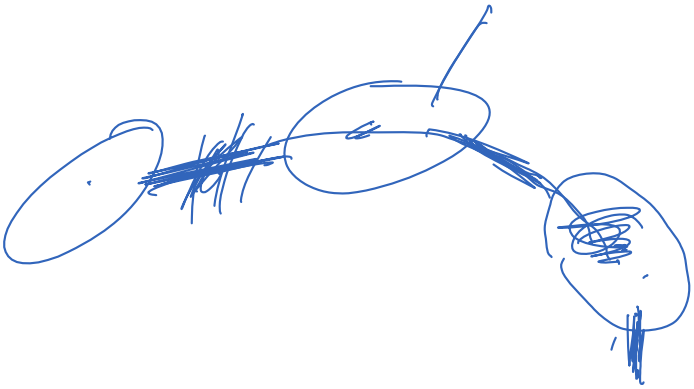
How BGP Works



BGP Update


BGP Header
Withdrawn Routes
Path for Prefixes
Reachable Prefixes
189.17.0.0/16, 220.11.9.0/24
(Prefixes)
4109, 112, 3785, 12
(AS Path)
Origin AS
24.0.0.0/8
128.89.88/23
(Prefixes)


BGP Update.



BGP Prefix Announcement Example

❖ IP prefixes announced by Facebook, Inc.

```
seed@User(10.0.2.18):~$ whois -h whois.radb.net -- '-i origin AS32934' | grep route:
route:          204.15.20.0/22
route:          69.63.176.0/20
route:          66.220.144.0/20
route:          66.220.144.0/21
route:          69.63.184.0/21
route:          69.63.176.0/21
route:          74.119.76.0/22
route:          69.171.255.0/24
route:          173.252.64.0/18
route:          69.171.224.0/19
route:          69.171.224.0/20
route:          103.4.96.0/22
route:          69.63.176.0/24
route:          173.252.64.0/19
route:          173.252.70.0/24
route:          31.13.64.0/18
route:          31.13.78.0/24
route:          31.13.79.0/24
route:          31.13.80.0/24
route:          31.13.82.0/24
route:          31.13.83.0/24
route:          31.13.84.0/24
route:          31.13.85.0/24
route:          31.13.86.0/24
route:          31.13.87.0/24
route:          31.13.88.0/24
route:          31.13.89.0/24
route:          31.13.90.0/24
......
```

66.220.144.0/21	Menlo Park, CA
69.63.176.0/24	San Francisco
103.4.96.0/22	Singapore
31.13.78.0/24	Virginia
31.13.80.0/24	Ontario, Canada
31.13.83.0/24	Madrid, Spain

Find BGP-Related Information

❖ From IP address to AS number

```
seed@User(10.0.2.18):~$ whois -h whois.radb.net 128.230.32.13
route:      128.230.0.0/16
descr:      Proxy-registered route object
origin:     AS11872
mnt-by:     MAINT-AS3491
changed:    jray@pccwglobal.com 20080322  #21:56:51(UTC)
source:     RADB


seed@User(10.0.2.18):~$ whois -h whois.radb.net 149.119.0.0
route:      149.119.0.0/16
descr:      Proxy-registered route object
origin:     AS11872
mnt-by:     MAINT-AS3491
changed:    jray@pccwglobal.com 20080322  #22:38:25(UTC)
source:     RADB


seed@User(10.0.2.18):~$ whois -h whois.radb.net 31.13.78.3
route:      31.13.78.0/24
descr:      Facebook, Inc.
origin:     AS32934
mnt-by:     MAINT-AS32934
changed:    shaw@fb.com 20120423  #20:09:37Z
source:     RADB
```

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

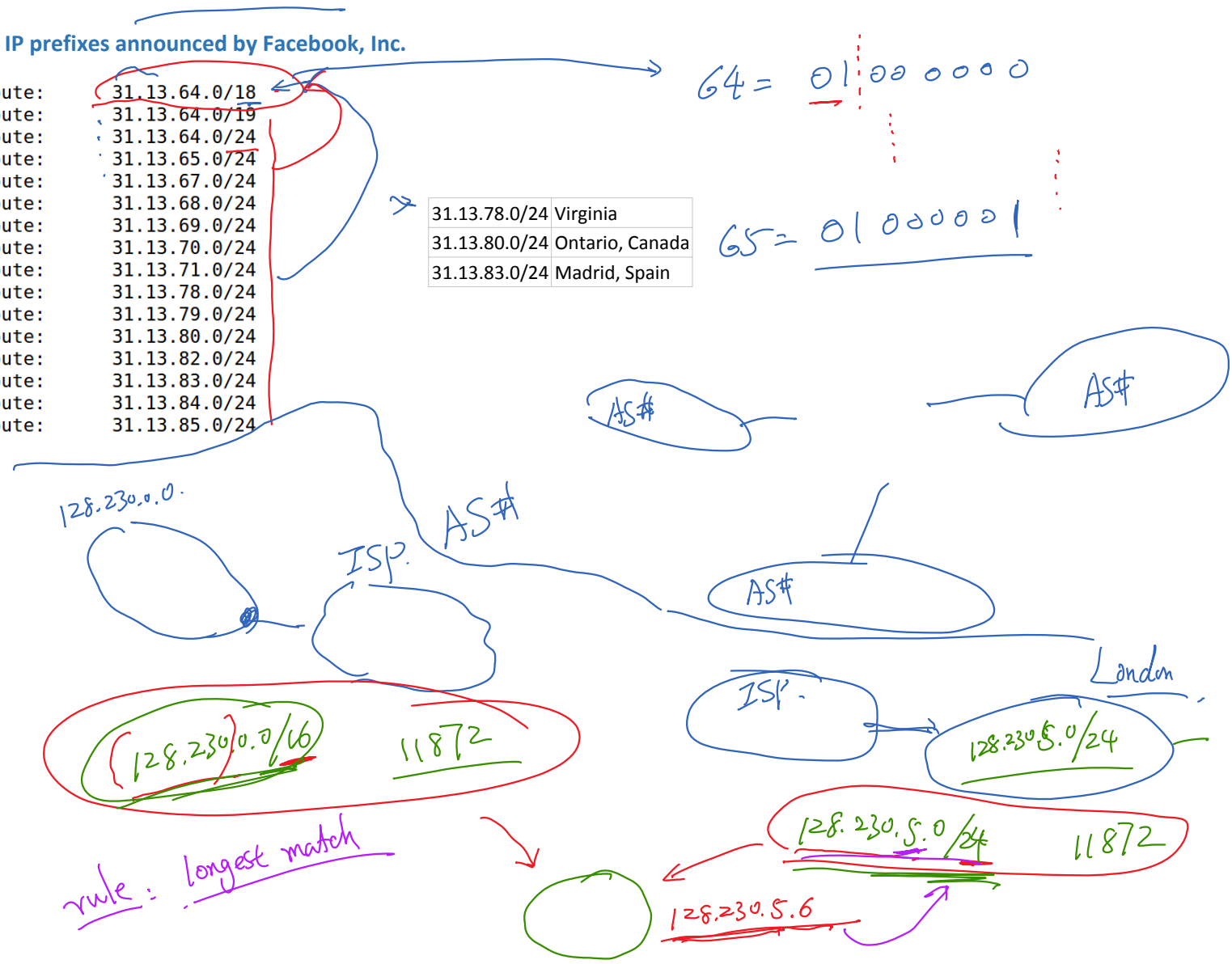
BGP Prefix Deaggregation and Applications

BGP Prefix Deaggregation and Applications

❖ **IP prefixes announced by Facebook, Inc.**

```
route:      31.13.64.0/18
route:      31.13.64.0/19
route:      31.13.64.0/24
route:      31.13.65.0/24
route:      31.13.67.0/24
route:      31.13.68.0/24
route:      31.13.69.0/24
route:      31.13.70.0/24
route:      31.13.71.0/24
route:      31.13.78.0/24
route:      31.13.79.0/24
route:      31.13.80.0/24
route:      31.13.82.0/24
route:      31.13.83.0/24
route:      31.13.84.0/24
route:      31.13.85.0/24
```

31.13.78.0/24	Virginia
31.13.80.0/24	Ontario, Canada
31.13.83.0/24	Madrid, Spain



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

IP Anycast

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

IP Anycast: F-Root Server

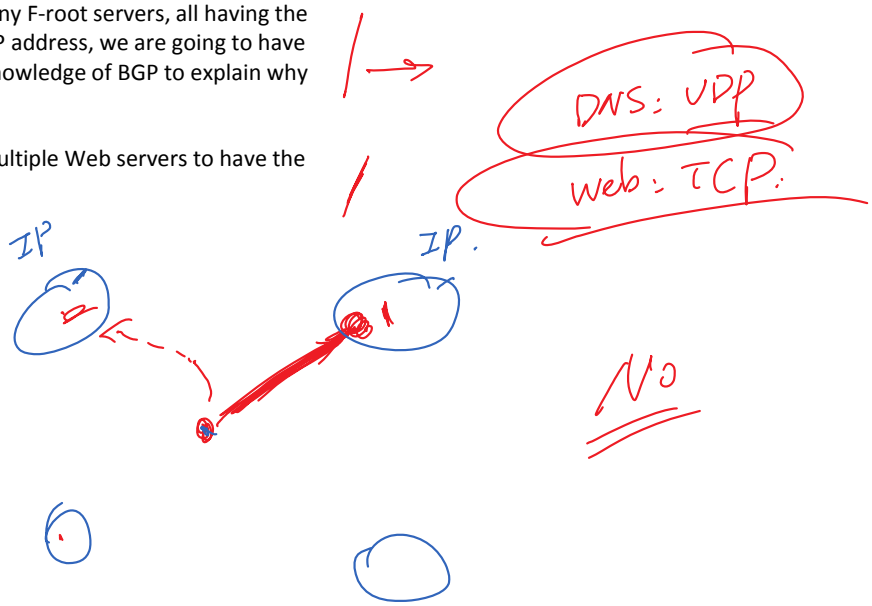
IP Address: **192.5.5.241**

ASN: **AS3557 (Internet Systems Consortium)**

Questions: IP Anycast

- IP Anycast is used by DNS root servers. For example, there are many F-root servers, all having the same IP address. Usually, when multiple machines use the same IP address, we are going to have problems. Why don't we have a problem here? Please use your knowledge of BGP to explain why this is not a problem.

- Can we use the same technology for Web servers, i.e., allowing multiple Web servers to have the same IP address, just like the F-root servers?

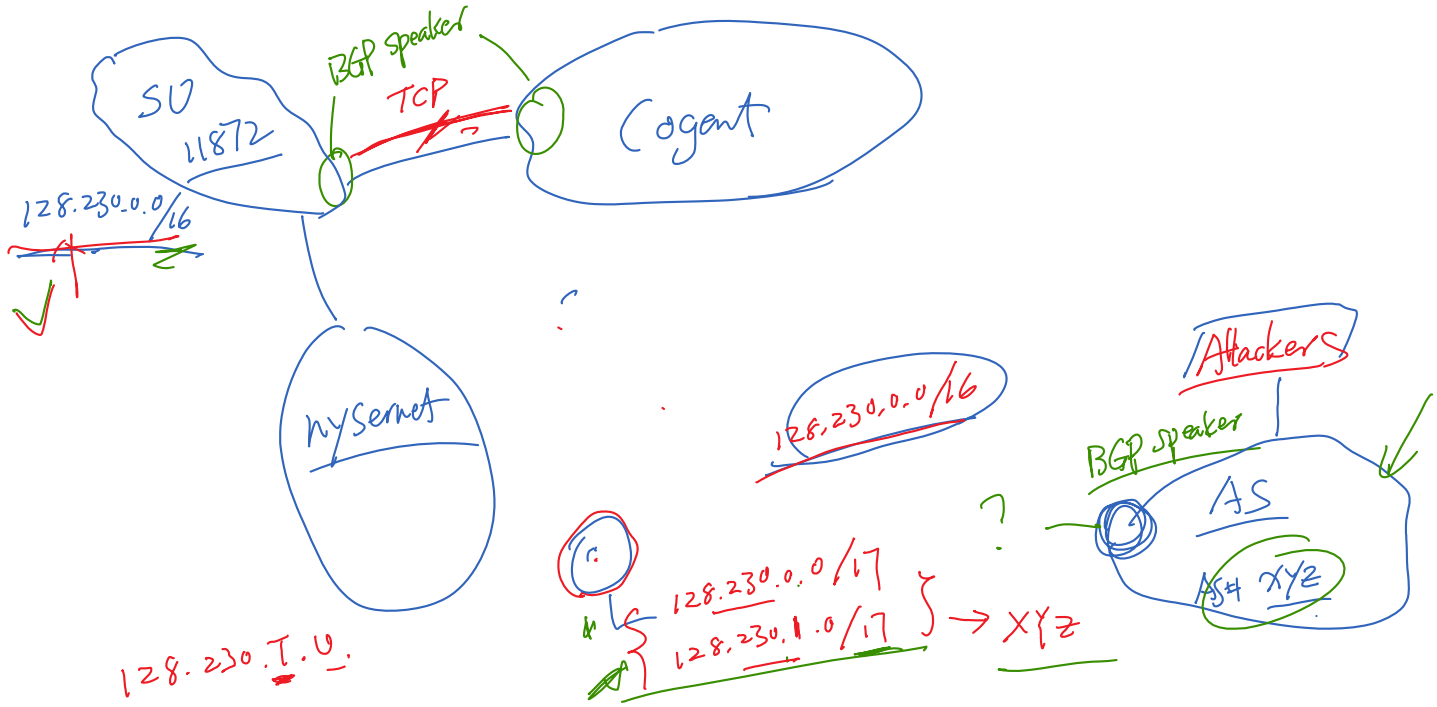


SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Attacks on BGP

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

How to Attack a Network Using BGP



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Case Studies on Attacks

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Pakistan Hijacks YouTube

How Pakistan knocked YouTube offline

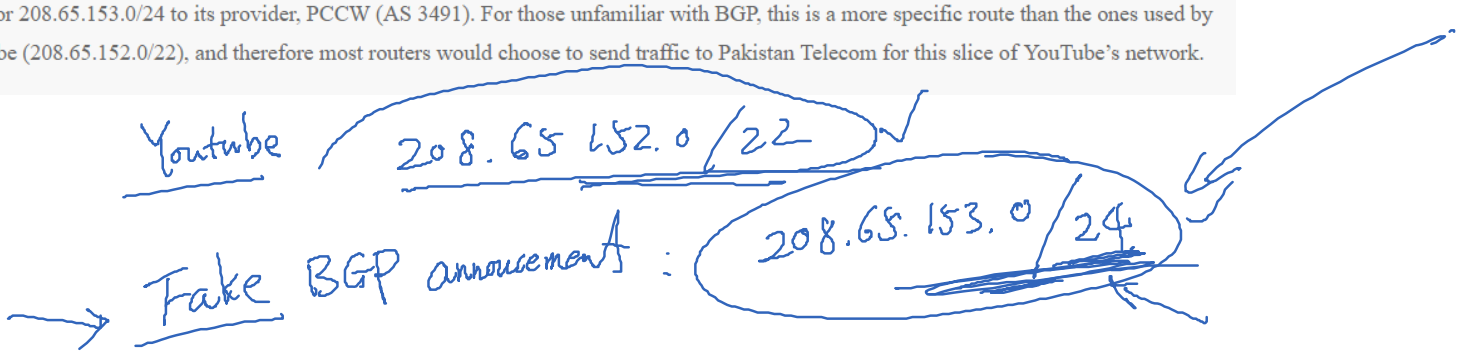
A spokesman for the Pakistani embassy said on Monday that the order to block access to YouTube came from the highest levels of the government. It would have been passed along to Pakistan's Electronic Media Regulatory Authority and then to Pakistan's telecom authority, the spokesman said, which in turn would have issued the formal order to the Internet providers.

Pakistan Telecom responded by broadcasting the false claim that it was the correct route for 256 addresses in YouTube's 208.65.153.0 network space. Because that was a more specific destination than the true broadcast from YouTube saying it was home to 1,024 computers, within a few minutes traffic started flowing to the wrong place.

Pakistan hijacks YouTube

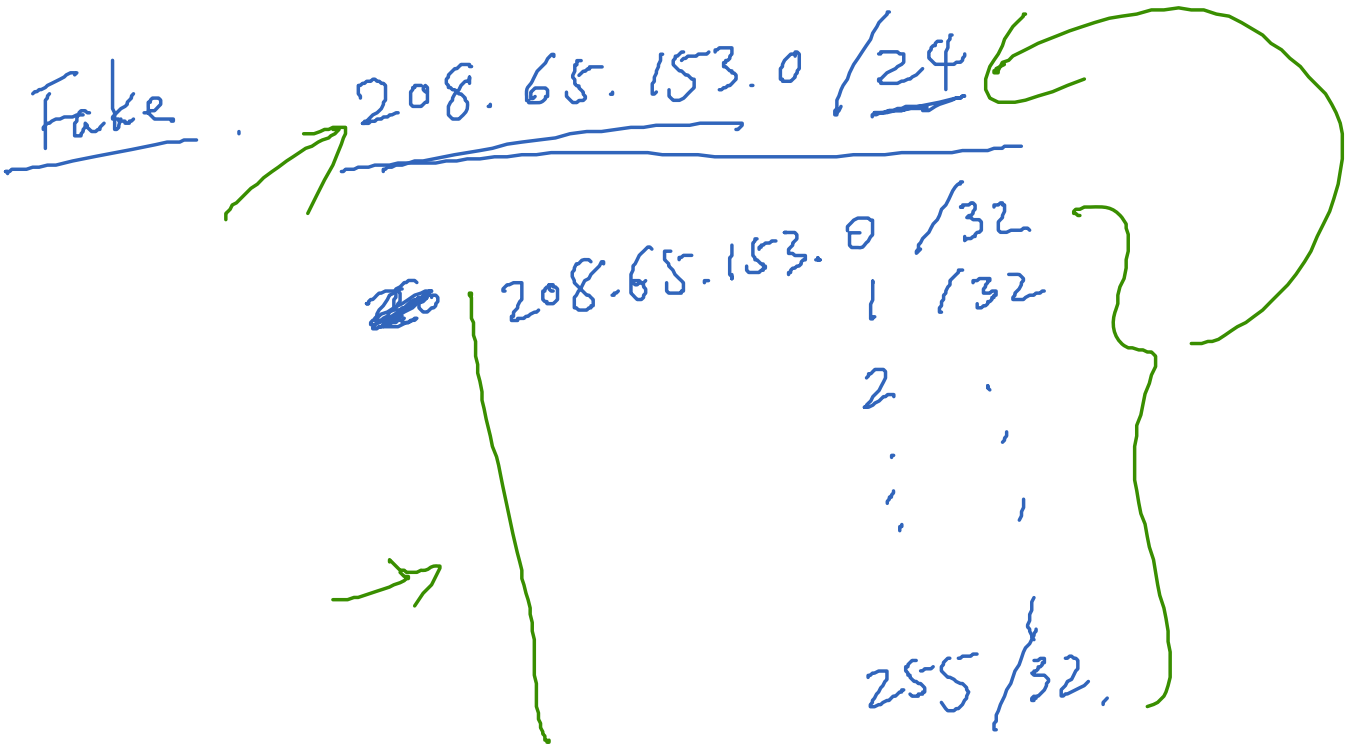
Late in the (UTC) day on 24 February 2008, Pakistan Telecom (AS 17557) began advertising a small part of YouTube's (AS 36561) assigned network. This story is almost as old as BGP. Old hands will recognize this as, fundamentally, the same problem as the infamous AS 7007 from 1997, a more recent ConEd mistake of early 2006 and even TTNet's Christmas Eve gift 2004.

Just before 18:48 UTC, Pakistan Telecom, in response to government order to block access to YouTube (see news item) started advertising a route for 208.65.153.0/24 to its provider, PCCW (AS 3491). For those unfamiliar with BGP, this is a more specific route than the ones used by YouTube (208.65.152.0/22), and therefore most routers would choose to send traffic to Pakistan Telecom for this slice of YouTube's network.



Question: Response to the Attack

In the Pakistan case, if you were managing YouTube's network, what would you do immediately to minimize the damage?



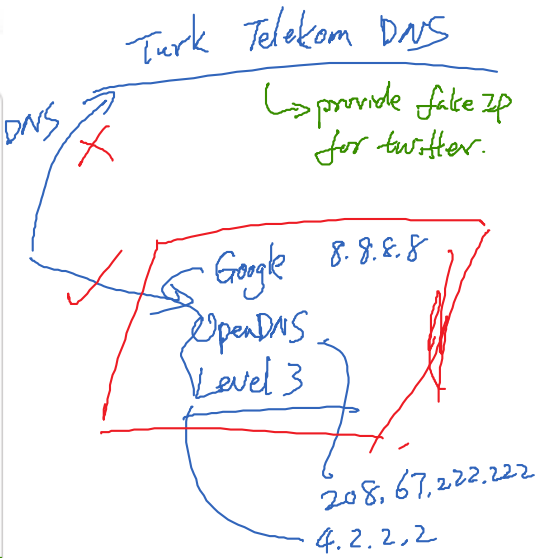
Turkey Hijacks Global DNS Providers

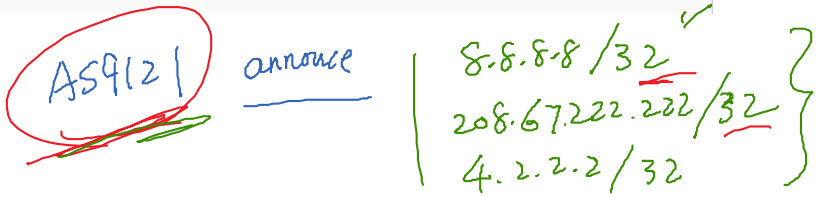
Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk - March 29, 2014 - Hijack, News and Updates - 26 Comments

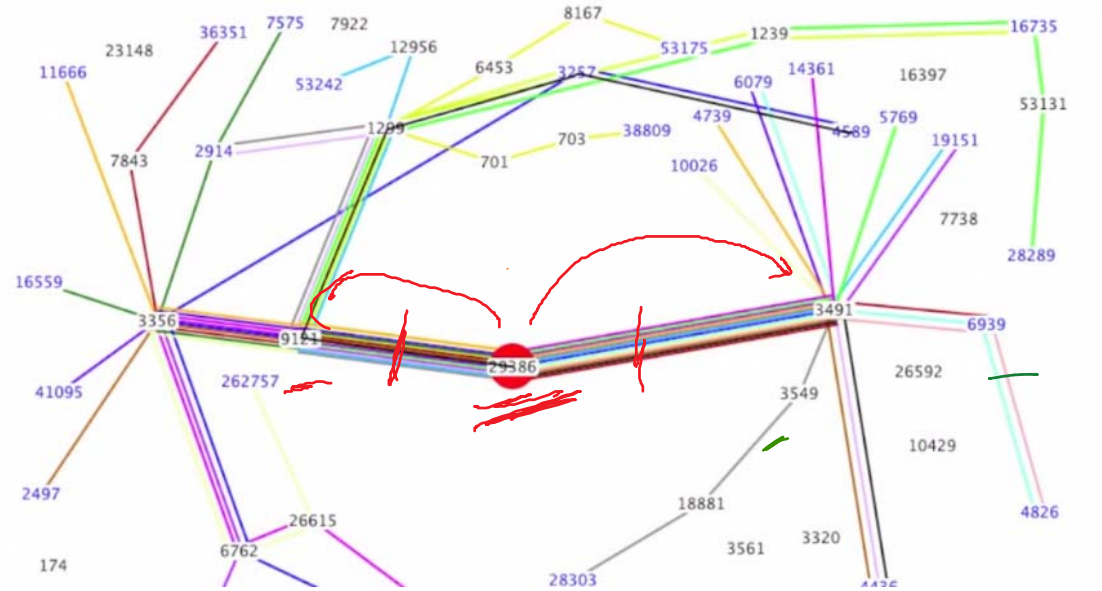
At BGPmon we see numerous BGP hijacks every single day, some are interesting because of the size and scale of the hijack or as we've seen today because of the targeted hijacked prefixes. It all started last weekend when the Turkish president ordered the censorship of twitter.com. This started with a block of twitter by returning false twitter IP addresses by Turk Telekom DNS servers. Soon users in Turkey discovered that changing DNS providers to Google DNS or OpenDNS was a good method of bypassing the censorship.
But as of around 9am UTC today (Saturday March 29) this changed when Turk Telekom started to hijack the IP address for popular free and open DNS providers such as Google's 8.8.8.8, OpenDNS' 208.67.222.222 and Level3's 4.2.2.2.

BGP hijack
Using the Turk Telekom looking glass we can see that AS9121 (Turk Telekom) has specific /32 routes for these IP addresses. Since this is the most specific route possible for an IPv4 address, this route will always be selected and the result is that traffic for this IP address is sent to this new bogus route.





Case Study: Syria Turned Off Its Internet



AS9121 Turk Telecom

AS3491 PCCW Global

Internet Cables: Physical Attacks

Ship's anchor accidentally slices Internet cable, cutting off access in six African countries

How to destroy the Internet

http://gizmodo.com/5912383/how-to-destroy-the-internet

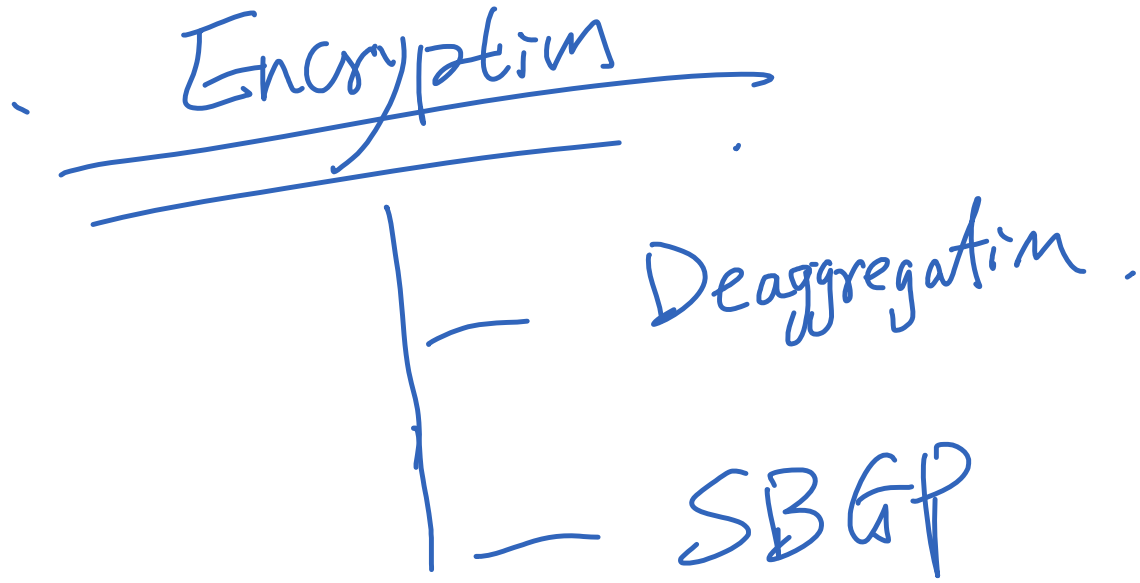
The hidden cables under a Cornish beach feeding the world's Internet

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Protecting BGP

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Protecting BGP



SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Summary

- How the Internet is connected
- Internet exchange and peering
- Network tiers and disputes
- BGP and how it works
- BGP prefix deaggregation and IP anycast
- Attacks on BGP and case studies

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE