CSE508 Network Security

9/14/2017

Core Protocols: BGP

Michalis Polychronakis

Stony Brook University

IP Addressing and Forwarding

Packets are routed based on their dst. IP address

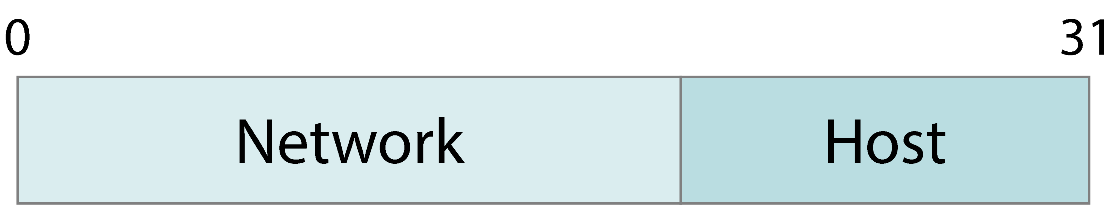
Router's task: for every possible IP address, forward packet to the next hop

- Table lookup for each packet in a routing table

For 32-bit addresses, 2^{32} possibilities! ➔ impractical

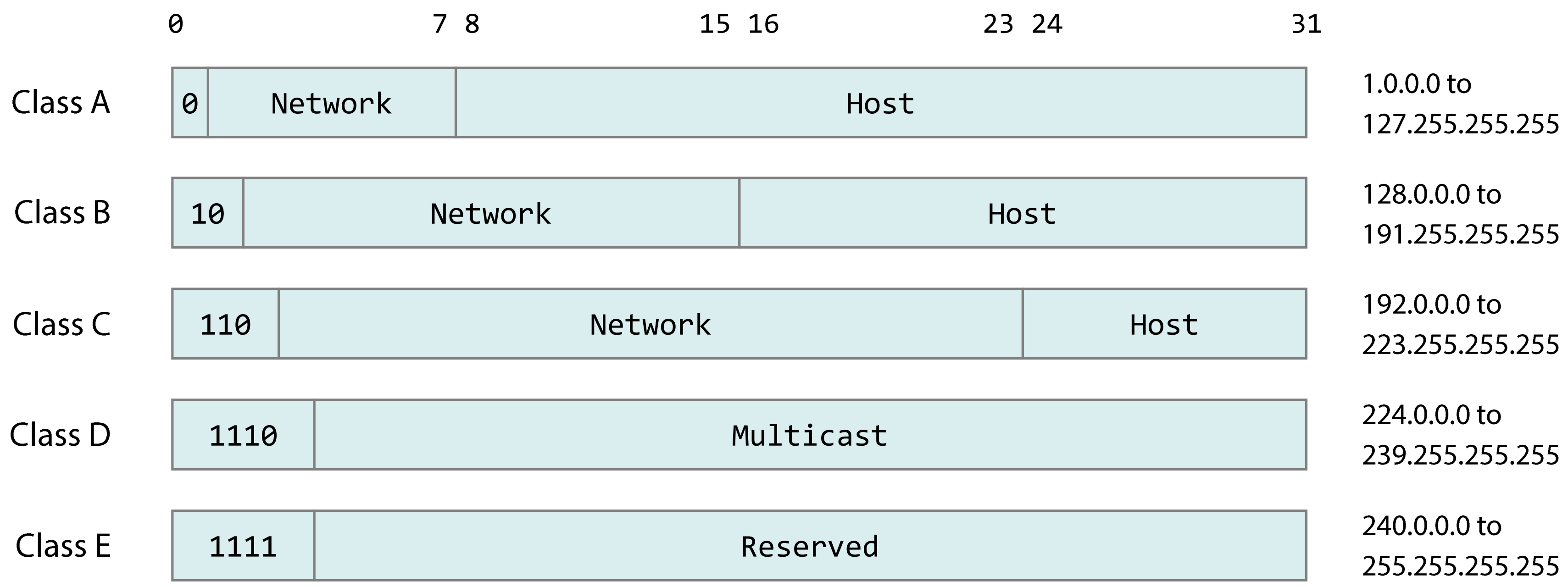
- **Solution: hierarchical address scheme**

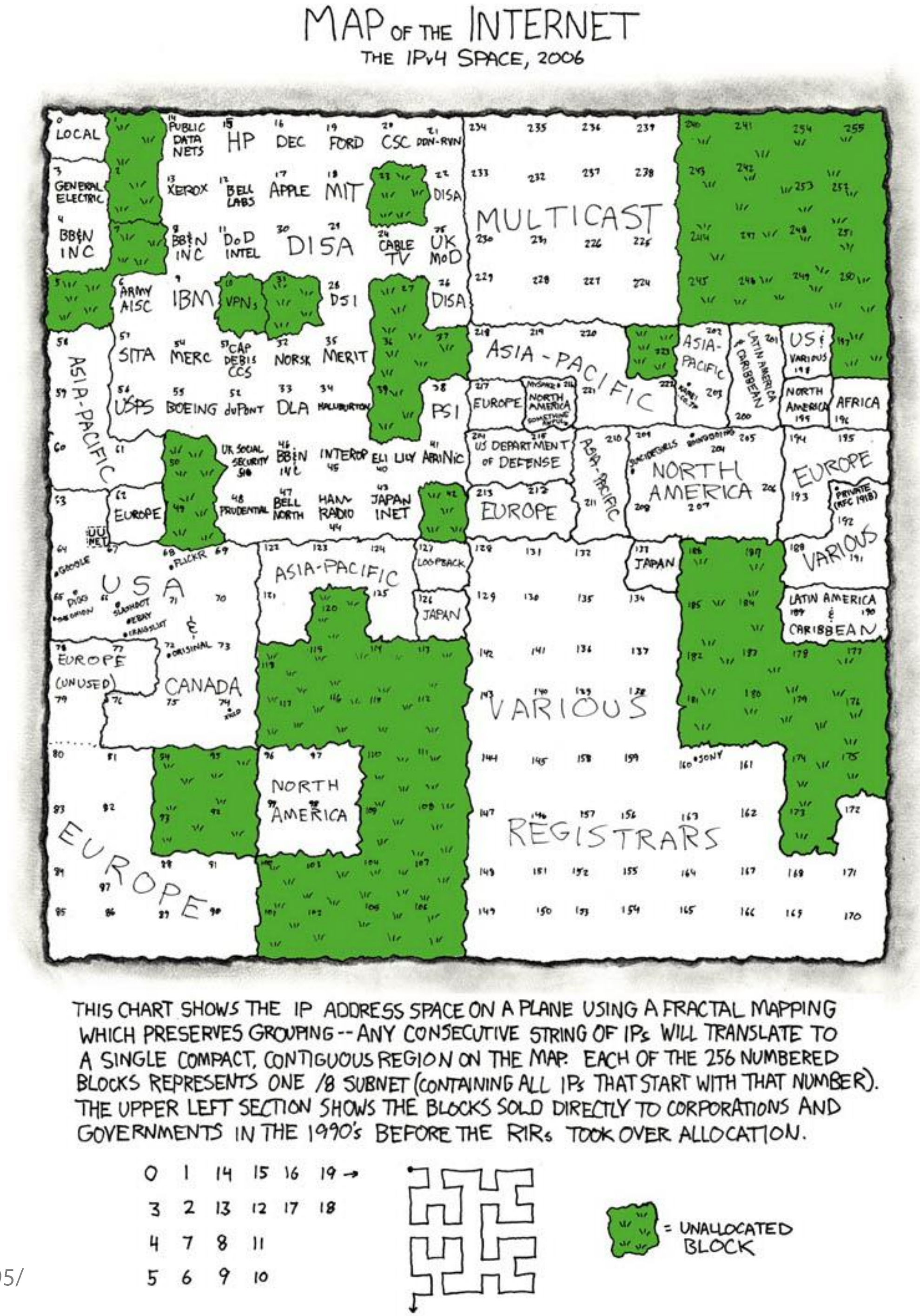
IP:



Known by all routers   *Known by edge/internal (LAN) routers*

IPv4 Address Classes





No green patches after 2011…

© XKCD - https://xkcd.com/195/

IPv4 Census Map

June – October 2012

Utilization

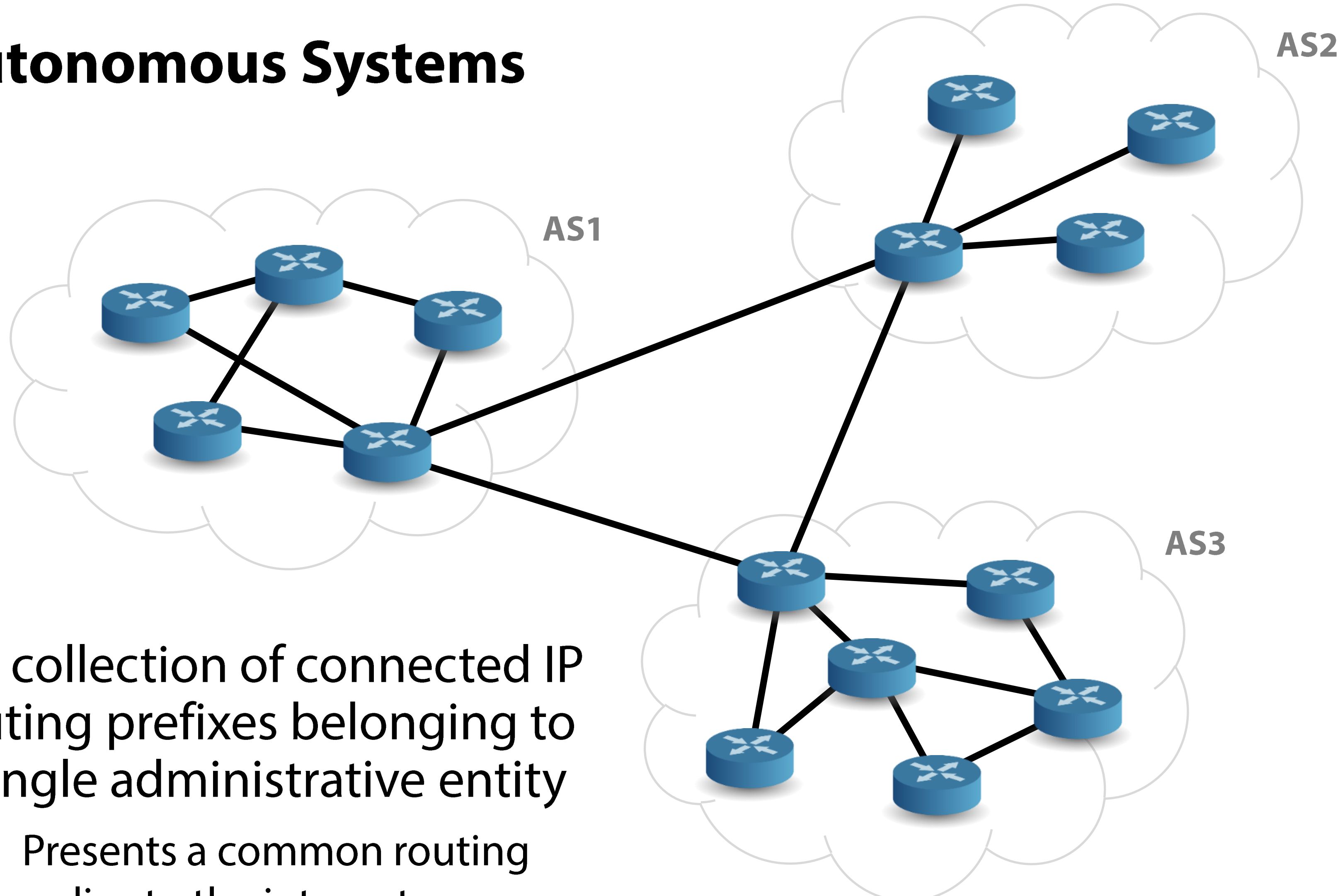
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

Prefix Sizes

= /8
= /12
= /16
= /20
= /24

420 Million hosts that responded to ICMP Ping at least 2 times between June and October 2012
Source: Carna Botnet

Autonomous Systems



AS: collection of connected IP routing prefixes belonging to a single administrative entity

- Presents a common routing policy to the internet

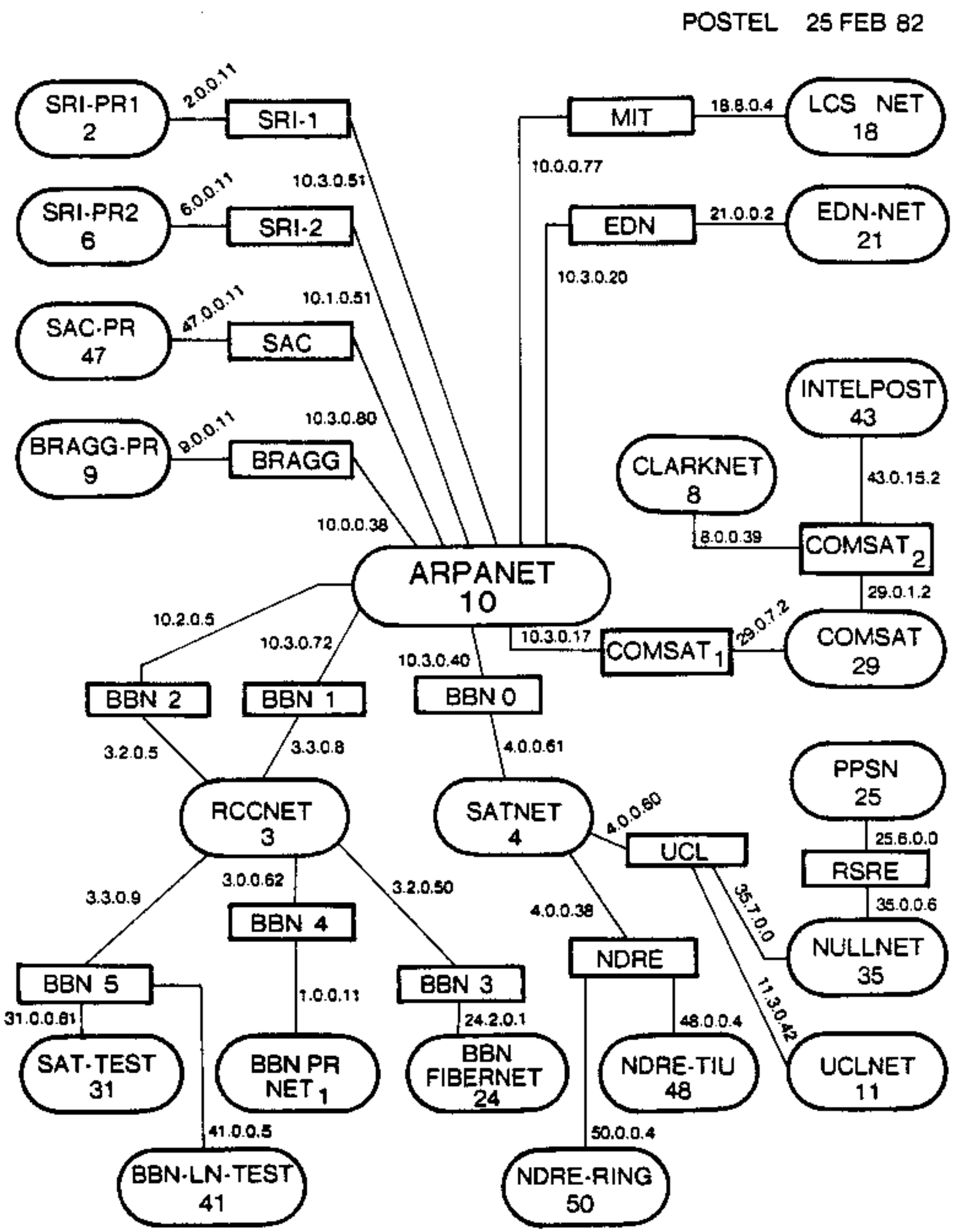
AS number defined as 16-bit integer

- ~47,000 ASNs as of 2014, assigned by IANA

Map of the internet, 1982

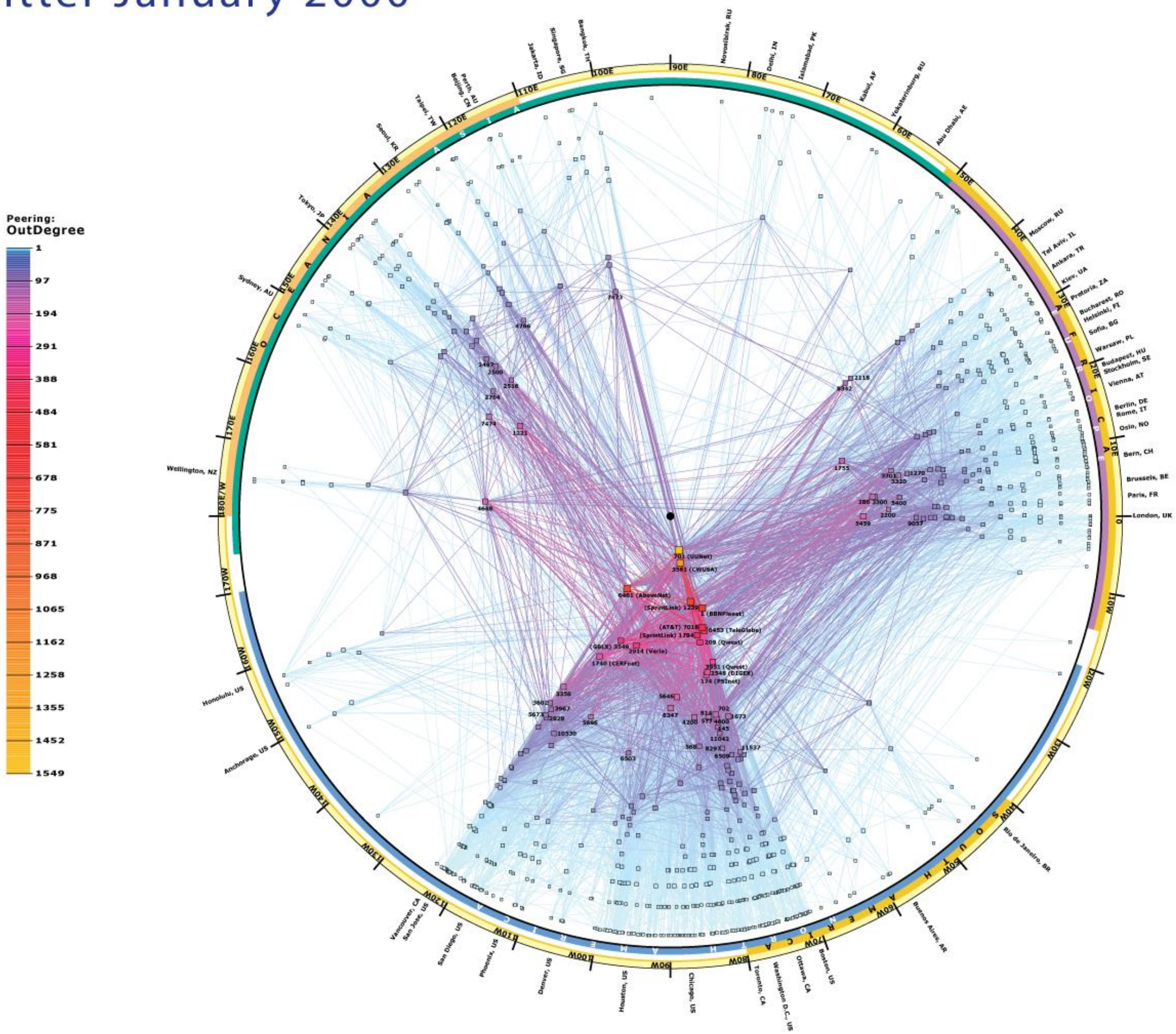
Ovals: sites/networks
Rectangles: routers

Created by Jon Postel



CAIDA's IPv4 AS Core AS-level INTERNET GRAPH

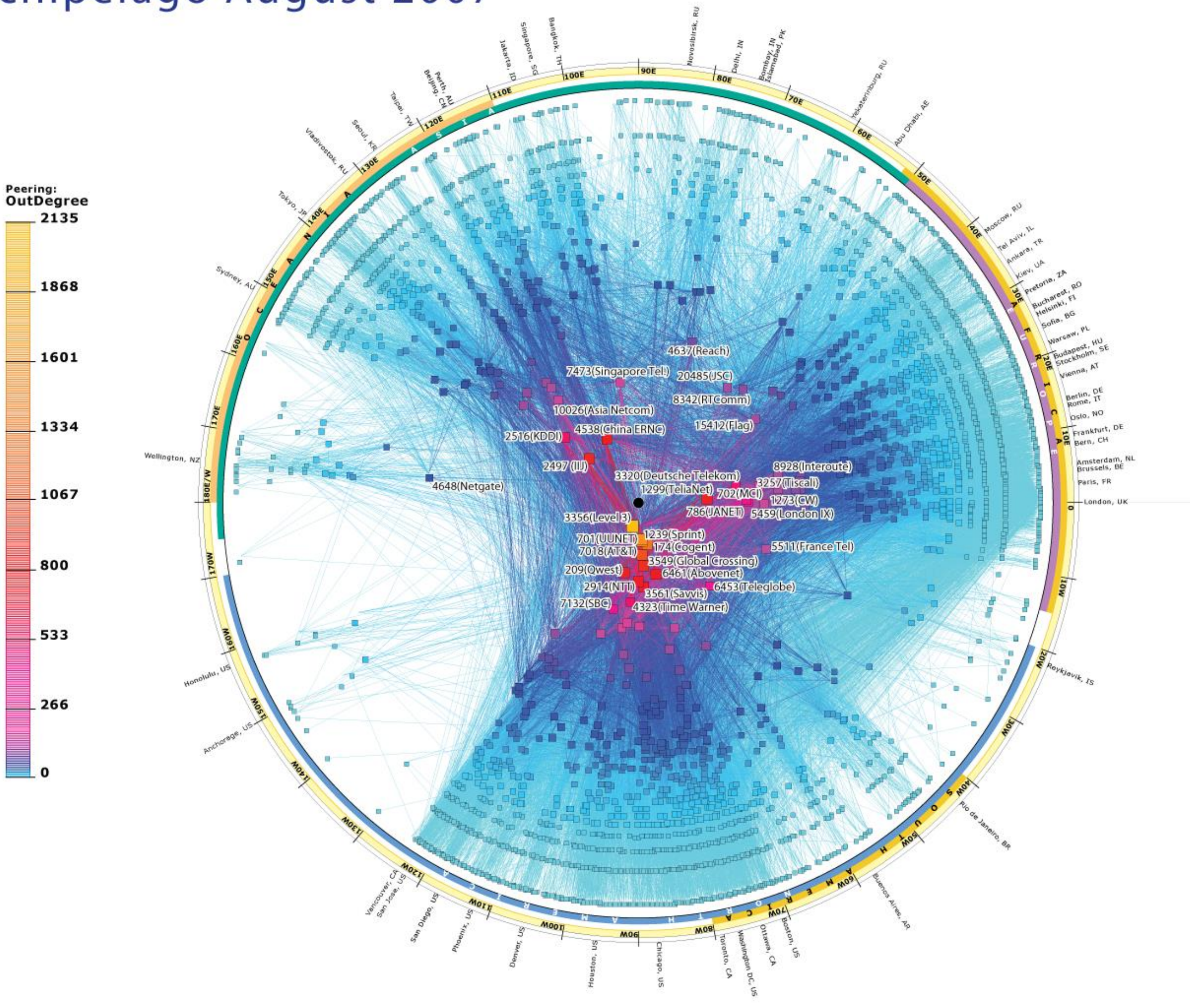
Skitter January 2000



copyright © 2000 UC Regents. all rights reserved.

CAIDA's IPv4 AS Core
AS-level INTERNET GRAPH

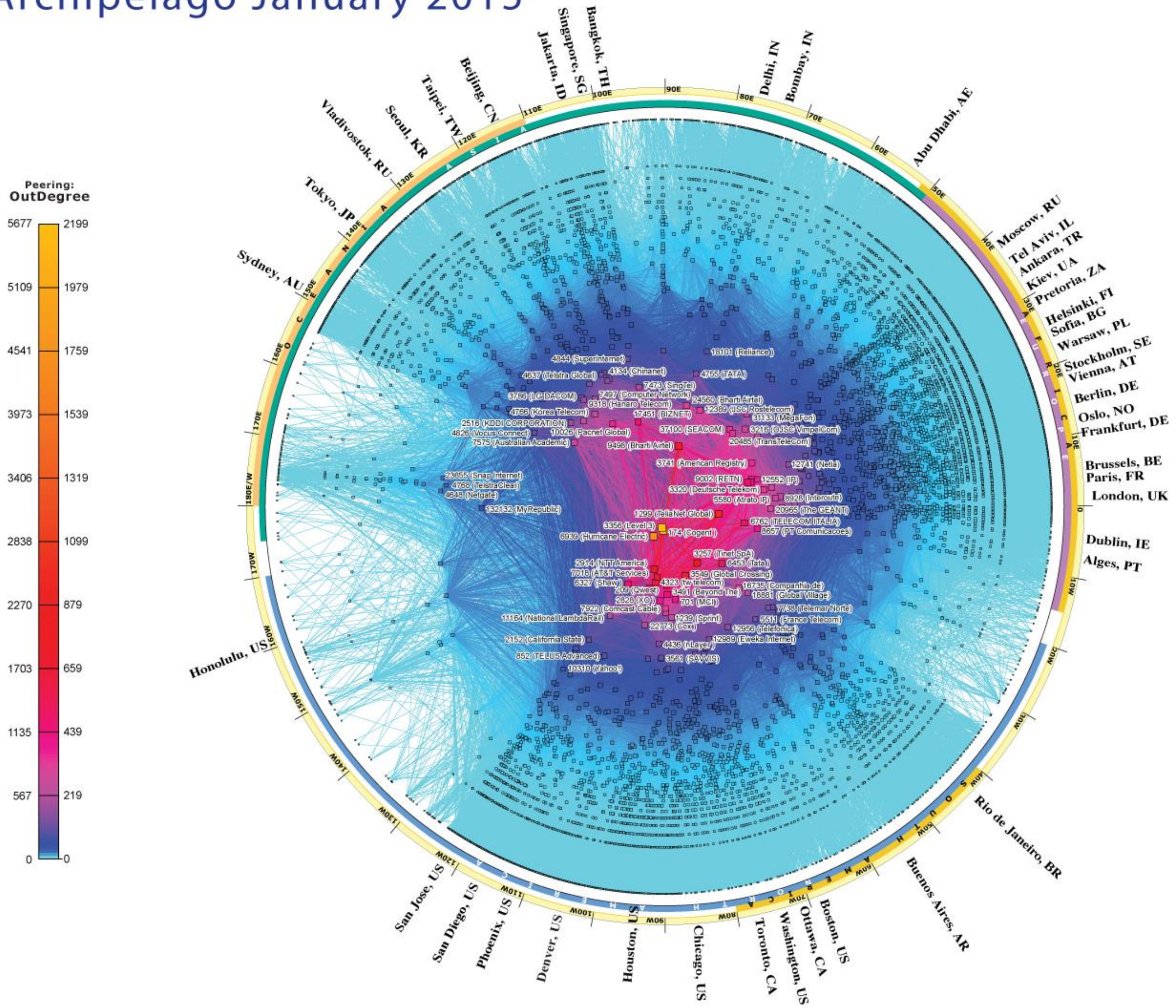
Archipelago August 2007



copyright © 2007 UC Regents. all rights reserved.

CAIDA's IPv4 AS Core AS-level INTERNET GRAPH

Archipelago January 2015



copyright © 2015 UC Regents. All rights reserved.

Internet Routing

Routers speak to each other to establish internet paths

- Exchange topology and cost information
- Calculate the best path to each destination

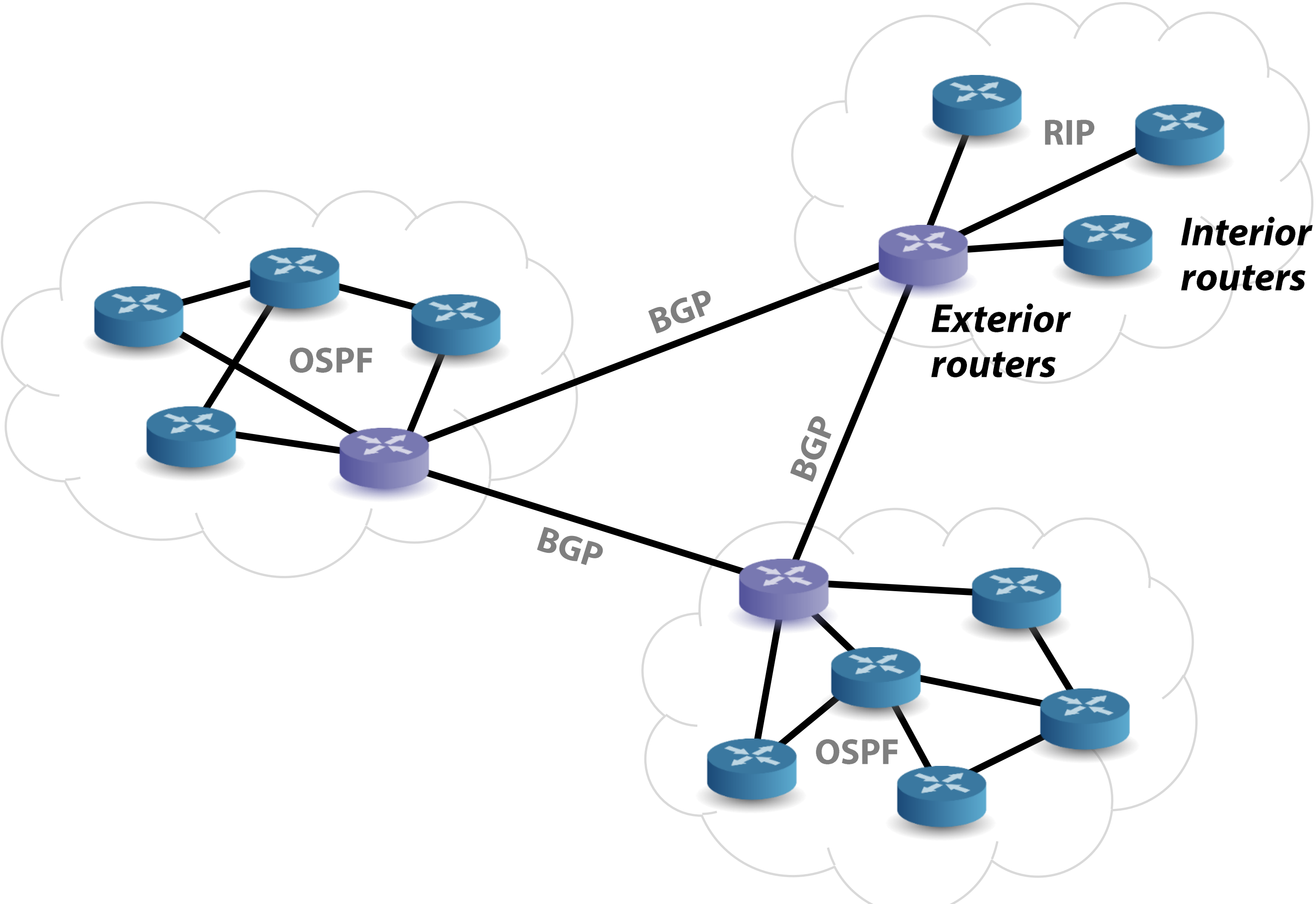
Intra-domain routing: set up routes within a single network/AS

- **RIP** (Routing Information Protocol): distance vector
- **OSPF** (Open Shortest Path First): link state

Inter-domain routing: set up routes between networks

- **BGP** (Border Gateway Protocol)
- Advertisements contain a prefix and a list of ASes to traverse to reach that prefix

Internet Routing



BGP

The de facto standard inter-AS routing protocol in today's Internet

Main goals

- Obtain subnet reachability information from neighboring ASs
- Propagate the reachability information to all internal routers
- Determine "good" routes to subnets based on the reachability information and AS policy

BGP is what enables subnets to advertise their existence to the rest of the Internet

Root Causes of BGP Security Issues

No authentication of path announcements

- Neighbor adjacencies can be "secured" using MD5 digests

BGP messages are sent over TCP connections

- All the usual problems: eavesdropping, content manipulation, …

Misconfigurations are easy

- BGP is a complex protocol, with complex interactions

Attackers can lie to other routers

Routing Attacks

Blackholing

False route advertisements to attract and drop traffic

Redirection

Force traffic to take a different path, either for interception (MitM) or to cause congestion

Instability

Frequent advertisements and withdrawals and/or increased BGP traffic to cause connectivity outages

How?

Configuration mistakes

Insider attacks

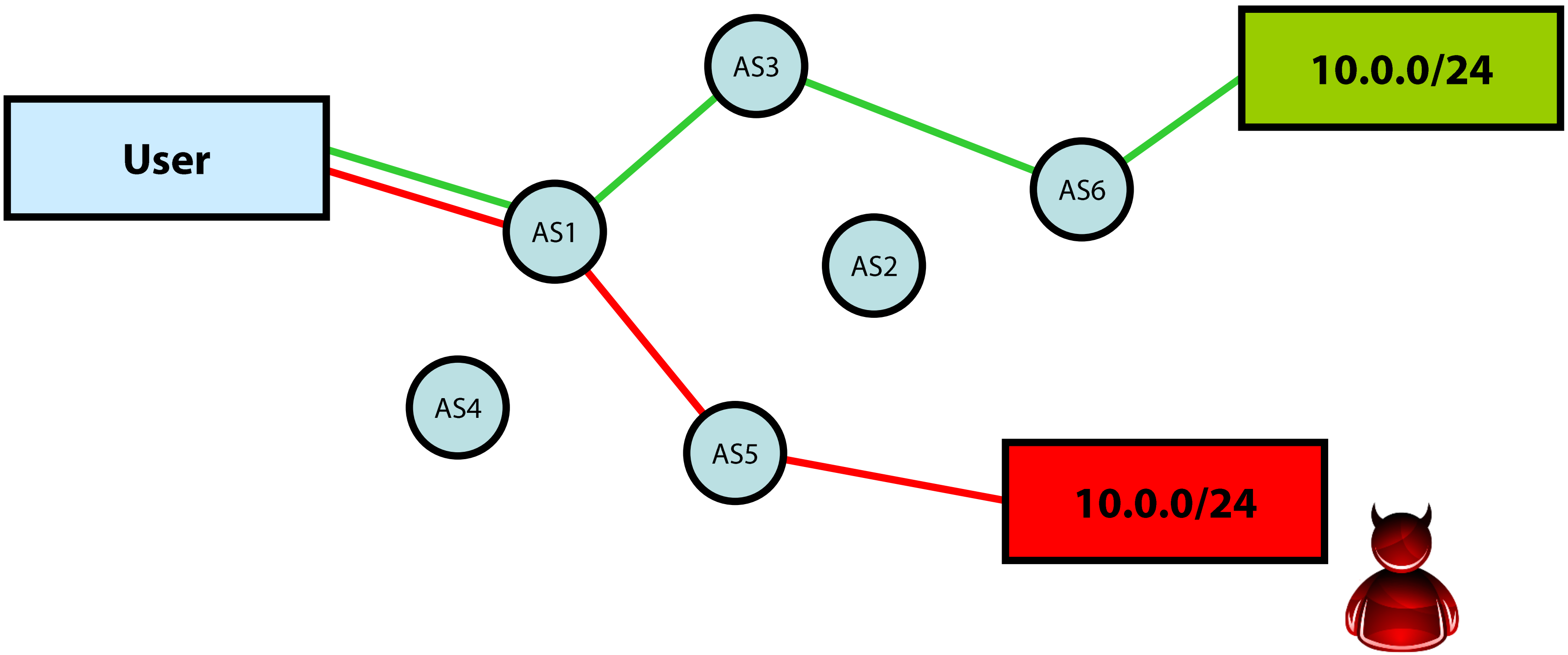
Compromised routers

BGP traffic manipulation

Prefix Hijacking

Announce someone else's prefix

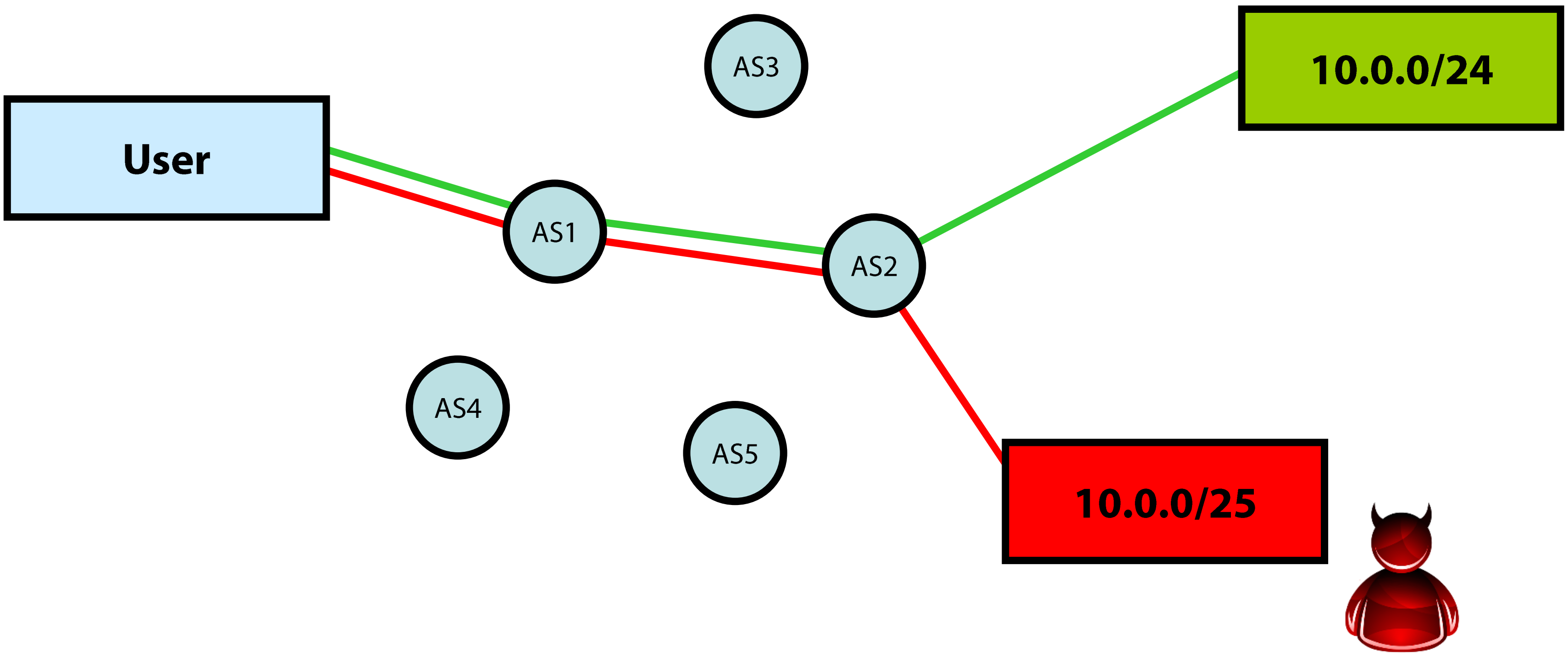
- Victim prefers the *shortest* path



Prefix Hijacking

Announce a more specific prefix than someone else

- Victim prefers the *more specific* path



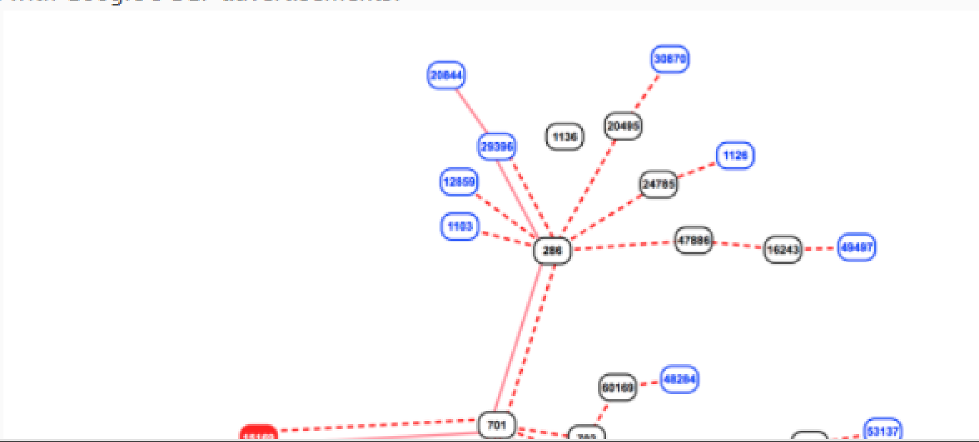
BGP leak causing Internet outages in Japan and beyond.

Posted by Andree Toonk – August 26, 2017 – BGP instability – No Comments

Yesterday some Internet users would have seen issues with their Internet connectivity, experiencing slowness or parts of the Internet as unreachable. This incident hit users in Japan particularly hard and it caused the Internal Affairs and Communications Ministry of Japan to start an investigation into what caused the large-scale internet disruption that slowed or blocked access to websites and online services for dozens of Japanese companies.

In this blog post we will take a look at the root cause of these outages, who was affected and what networks were involved.

Starting at 03:22 UTC yesterday (aug 25) followers of @BGPstream would have seen an increase in alerts involving Google. The BGPstream alerts were informing us that Google was announcing the peering lan prefixes of a few well known Internet exchanges. This in itself is actually a fairly common type of incident and typically indicates something isn't quite right within the networks hijacking those prefixes and so these alerts were the first clues that something wasn't quite right with Google's BGP advertisements.



Latest Tweets

Tweets by @bgpmon

BGPmon.net @bgpmon

New blog: Route leak via Google and Verizon causing internet outages in japan and beyond bgpmon.net/bgp-leak-causi...

Aug 26, 2017

BGPmon.net Retweeted

bgpstream @bgpstream

BGP,OT,KP,Korea, Democratic People's Republic of,-,Outage affected 4 prefixes, bgpstream.com/event/95347

Aug 14, 2017

BGPmon.net @bgpmon

Another Internet outage in Syria. Interestingly one remaining Syrian telecom network still BGP visible 91.144.0.0/20 twitter.com/bgpstream/stat...

Embed View on Twitter

Pakistan's Accidental You ×

www.wired.com/2008/02/pakistans-accid/

verizon What network are you living on? SEE WHAT FiOS INTERNET CAN DO FOR YOU. Learn More

6 MONTHS FOR $5 + FREE HAT.
SUBSCRIBE | GIVE A GIFT | RENEW | INTERNATIONAL ORDERS

Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net

BY RYAN SINGEL 02.25.08 | 10:37 AM | PERMALINK

Share 4 Tweet 4 g+1 0 in Share Pin it

Secure Your Cloud
cavirin.com
Free download: Best Practices For Ensuring Cloud Compliance.

Threat Protection Tool
C++ Static Analysis
AVG® Business Research
Security White Papers
Cisco® ACI Virtualization
IoT Security Explained
Immediate Risk Assessment

Government: you have to block this YouTube video

Pakistan Telecom: OK

Use URL filtering?

No

Change the DNS record?

No

Use IP blocking?

No

Blackhole 208.65.153.0/24?

Yes!

PTA

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA — February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

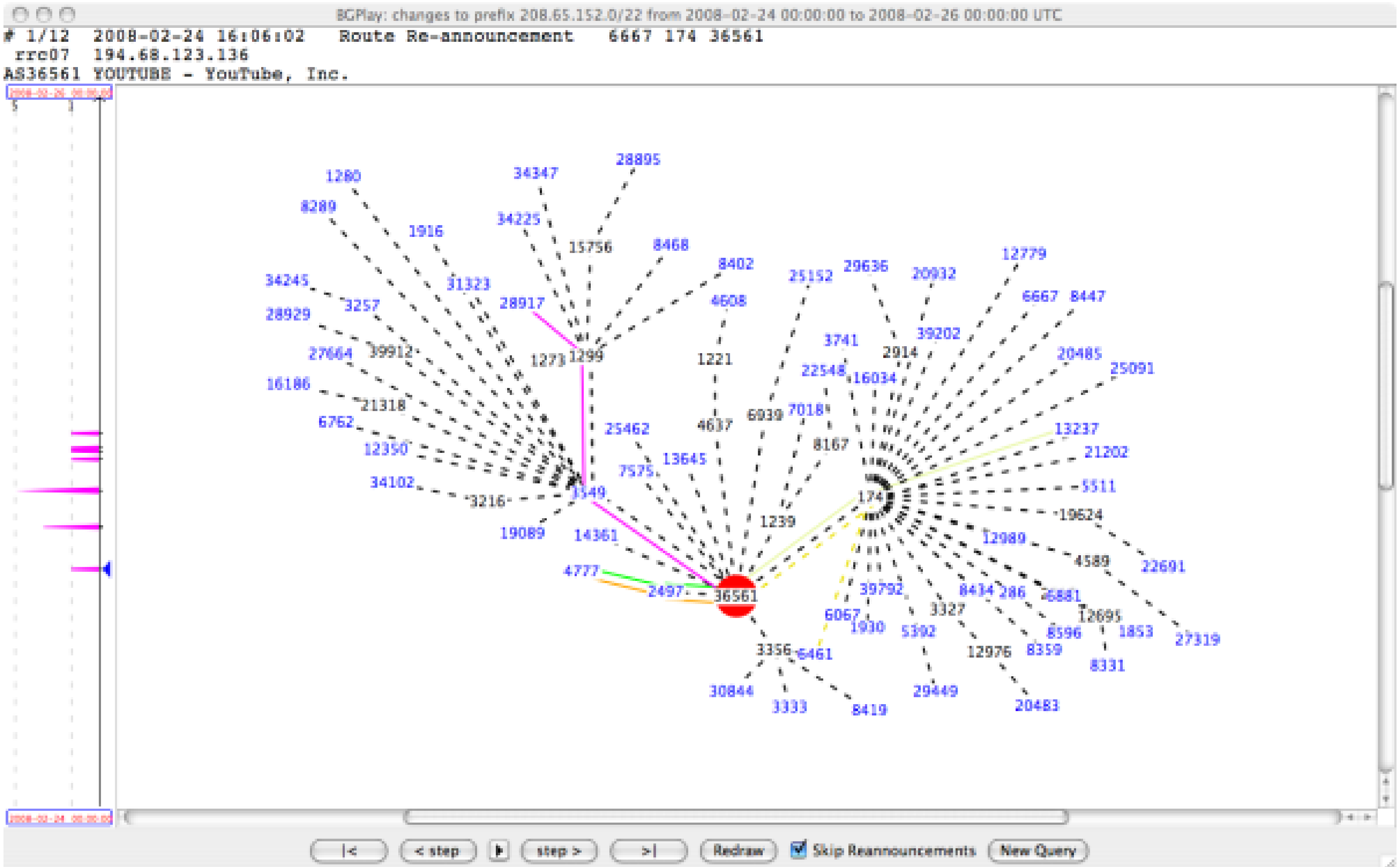
IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Deputy Director
(Enforcement)

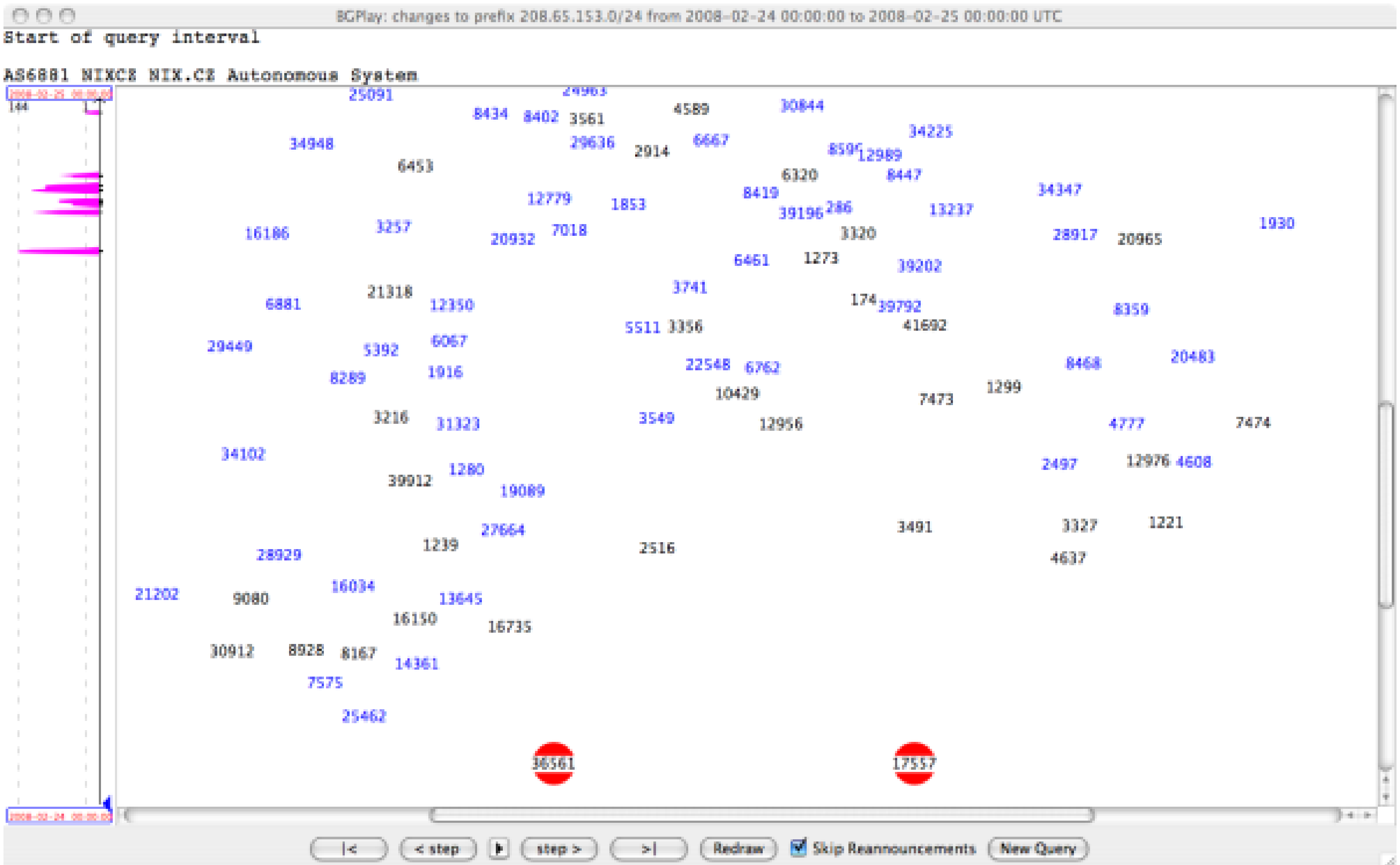
To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.

AS36561 (YouTube) announces 208.65.152.0/22



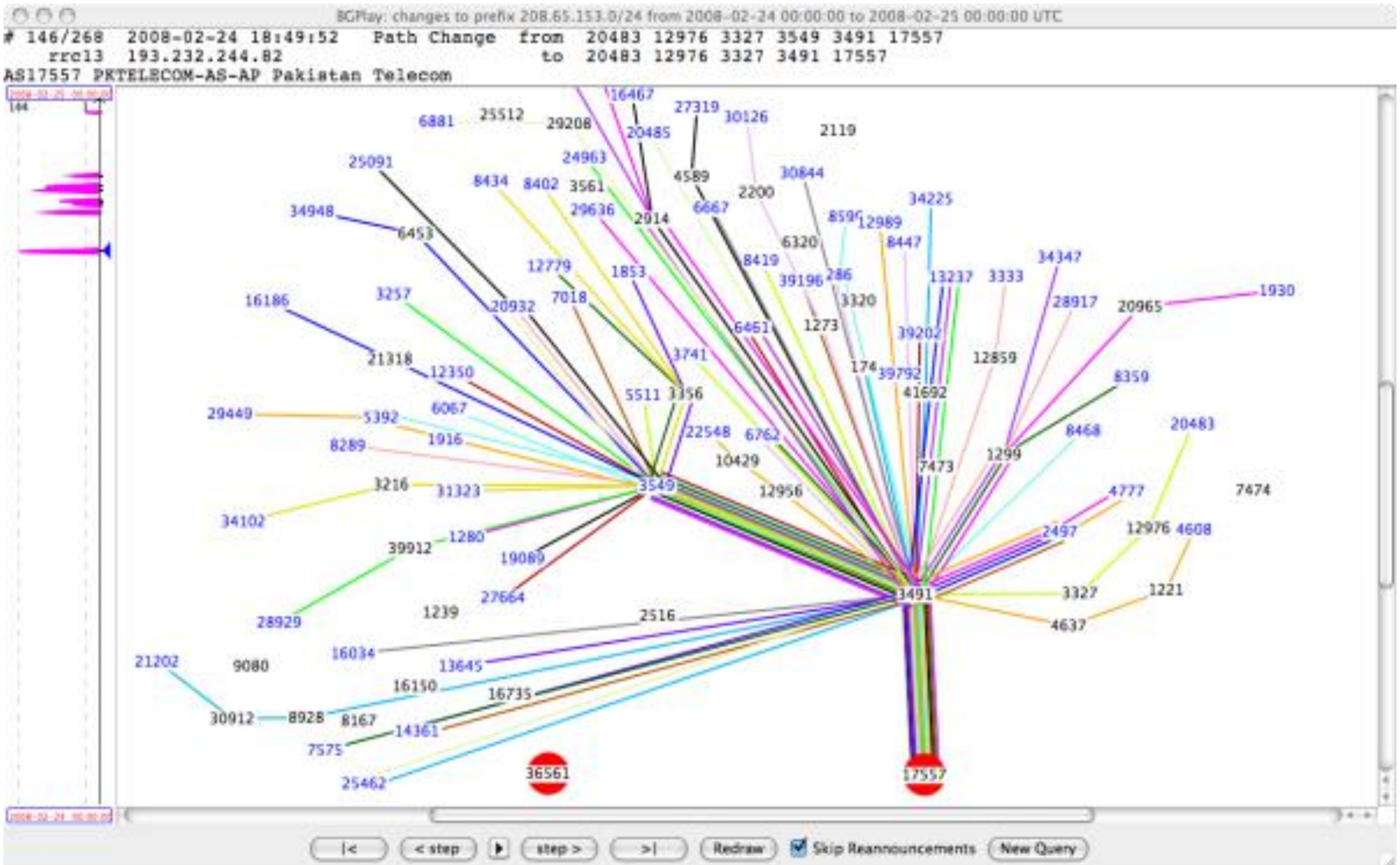
© RIPE NCC - https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

The prefix 208.65.153.0/24 is not announced on the Internet before the event



© RIPE NCC - https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

AS17557 (Pakistan Telecom) announces 208.65.153.0/24

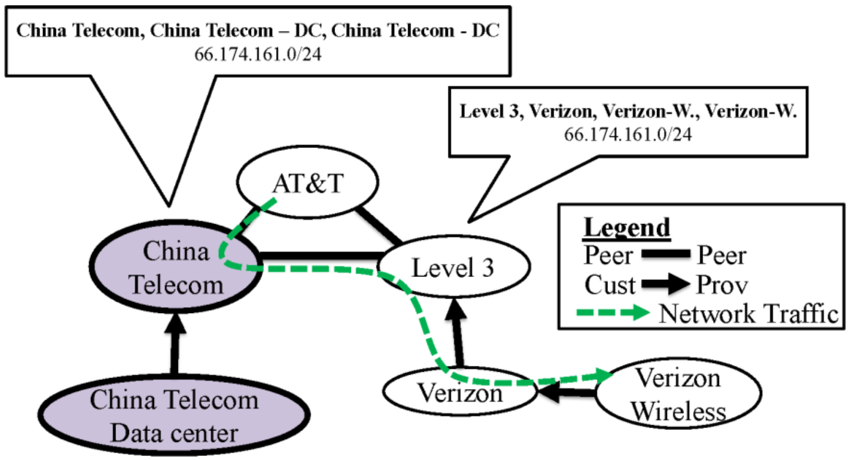


© RIPE NCC - https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Other Notable Incidents

April 2010: China Telecom announced bogus paths to 50,000 IP prefixes

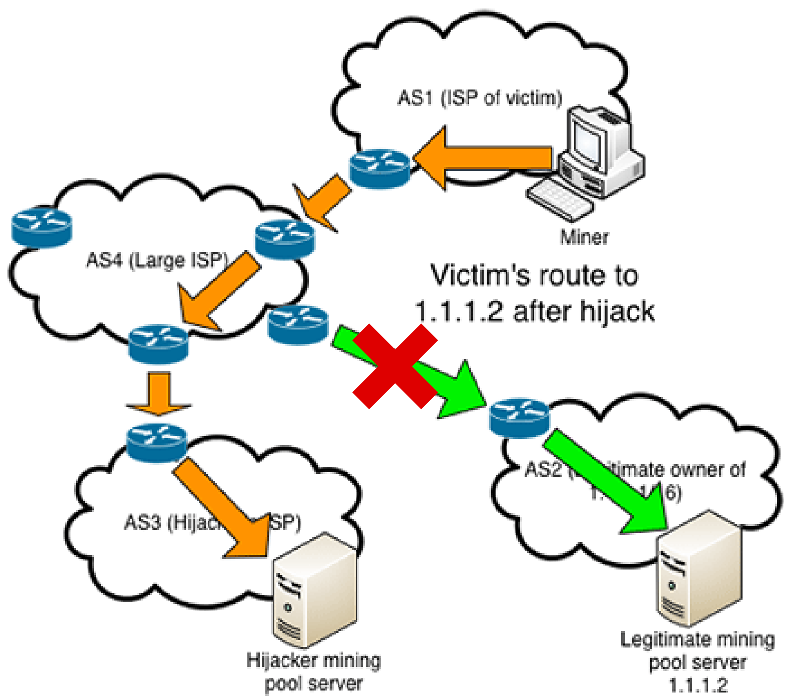
Enabled traffic interception



February 2014: hijacking of 51 networks (incl. Amazon, Digital Ocean, OVH)

Miner connections were redirected to an attacker-controlled mining pool

Attacker collected the miners' profit (est. $83,000 in 4 months)



© Phillipa Gill - https://citizenlab.org/2012/12/characterizing-large-scale-routing-anomalies-a-case-study-of-the-china-telecom-incident/
© Pat Litke and Joe Stewart - http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

Mitigating BGP Threats

Neighbor authentication

Only authorized peers can establish a given BGP neighbor relationship

TTL check

Most external peering sessions established between adjacent routers

Good idea: set TTL=1 ➔ an attacker X hops away can still set TTL=1+X

Better idea: set TTL=255 and accept only packets with TTL=255 ➔ an attacker further away cannot spoof such a packet

BGP prefix restrictions and filtering

Accept only a certain number of prefixes, ignore unwanted/illegal prefixes, limit the number of accepted AS path segments, …

ACLs to explicitly permit only authorized BGP traffic

According to existing security policies and configurations

Securing BGP

Secure BGP (S-BGP)

Each node signs its announcements

Resource Public Key Infrastructure (RPKI)

Certified mapping from ASes to public keys and IP prefixes

Secure origin BGP (soBGP)

Origin authentication + trusted database that guarantees that a path exists

BGPPSec

Allow recipients to validate the AS path included in update messages

Many deployment challenges

No complete, accurate registry of prefix ownership

Need for a public-key infrastructure

Cannot react rapidly to changes in connectivity

Cost of cryptographic operations

Incremental deployment not always possible