Border Gateway Protocol (BGP) Security

BGP Hijacks, Attacks, Defense Mechanisms

Network Security AS 2020

27 October 2020

Markus Legner
(based on slides by A. Perrig, R. Jaufeerally, C. Pappas, L. Vanbever)

ETH zürich

BGP making headlines …

… since 1997

Router glitch cuts Net access

A major outage shuts down Internet access in some parts of the country for as long as two hours.

BY CNET NEWS STAFF | APRIL 25, 1997

Indian ISP's routing hiccup briefly tak Google down worldwide

Broadband provider announced the wrong routes for many Google services.

SEAN GALLAGHER - 3/12/2015, 4:50 PM

BGP making headlines …

THE VERGE TECH

TECH | CYBERSECURITY | ENTERPRISE

Hackers emp
basic infrastr

By Russell Brandom | @russellbrandom |

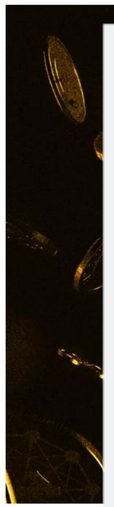
SHARE

BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 6:30 PM



THE ACCIDENTAL LEAK —

Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

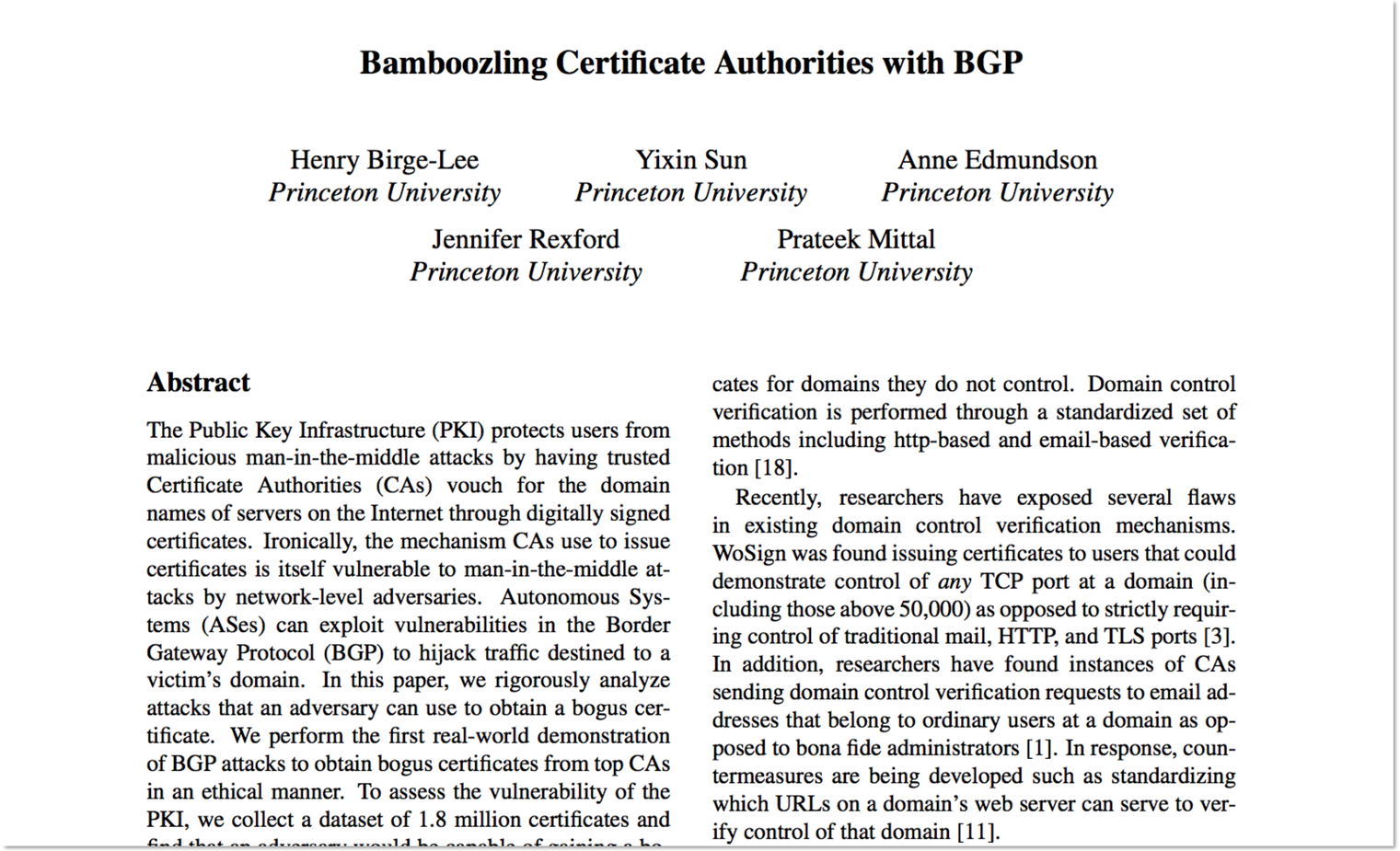
DAN GOODIN - 11/13/2018, 8:25 AM

Why are rerouting attacks so problematic?

- We have TLS, VPNs, etc. An attacker cannot read encrypted data. Why do we need to care about rerouting?
- Not all traffic is encrypted/authenticated: DNS, HTTP~~S~~
- Even encrypted traffic leaks timing information (→ fingerprinting)
- Rerouting can cause dropped packages and widespread outages
- Hard to notice and impossible to solve without ISP cooperation
- 12’600 routing incidents in 2018 (https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/)

What can go wrong?

Routing attacks can be used to obtain fake TLS certificates (https://secure-certificates.princeton.edu/)



Bamboozling Certificate Authorities with BGP

Henry Birge-Lee, *Princeton University*
Yixin Sun, *Princeton University*
Anne Edmundson, *Princeton University*
Jennifer Rexford, *Princeton University*
Prateek Mittal, *Princeton University*

Abstract

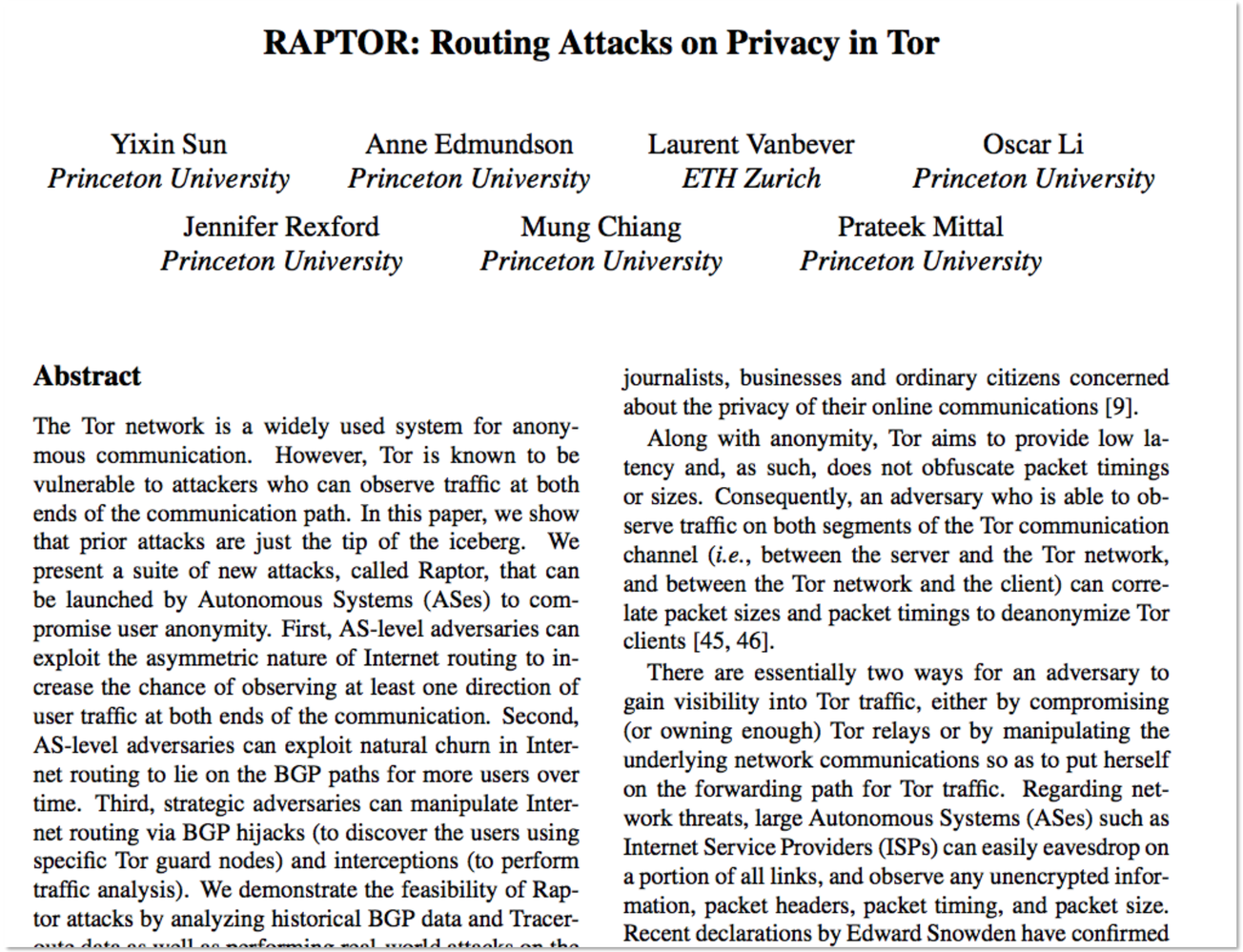
The Public Key Infrastructure (PKI) protects users from malicious man-in-the-middle attacks by having trusted Certificate Authorities (CAs) vouch for the domain names of servers on the Internet through digitally signed certificates. Ironically, the mechanism CAs use to issue certificates is itself vulnerable to man-in-the-middle attacks by network-level adversaries. Autonomous Systems (ASes) can exploit vulnerabilities in the Border Gateway Protocol (BGP) to hijack traffic destined to a victim's domain. In this paper, we rigorously analyze attacks that an adversary can use to obtain a bogus certificate. We perform the first real-world demonstration of BGP attacks to obtain bogus certificates from top CAs in an ethical manner. To assess the vulnerability of the PKI, we collect a dataset of 1.8 million certificates and find that an adversary would be capable of gaining a ba-

cates for domains they do not control. Domain control verification is performed through a standardized set of methods including http-based and email-based verification [18].

Recently, researchers have exposed several flaws in existing domain control verification mechanisms. WoSign was found issuing certificates to users that could demonstrate control of *any* TCP port at a domain (including those above 50,000) as opposed to strictly requiring control of traditional mail, HTTP, and TLS ports [3]. In addition, researchers have found instances of CAs sending domain control verification requests to email addresses that belong to ordinary users at a domain as opposed to bona fide administrators [1]. In response, countermeasures are being developed such as standardizing which URLs on a domain's web server can serve to verify control of that domain [11].

What can go wrong?

Routing attacks can be used to deanonymize TOR users
(https://www.usenix.org/node/190965)



RAPTOR: Routing Attacks on Privacy in Tor

Yixin Sun, *Princeton University*
Anne Edmundson, *Princeton University*
Laurent Vanbever, *ETH Zurich*
Oscar Li, *Princeton University*
Jennifer Rexford, *Princeton University*
Mung Chiang, *Princeton University*
Prateek Mittal, *Princeton University*

Abstract

The Tor network is a widely used system for anonymous communication. However, Tor is known to be vulnerable to attackers who can observe traffic at both ends of the communication path. In this paper, we show that prior attacks are just the tip of the iceberg. We present a suite of new attacks, called Raptor, that can be launched by Autonomous Systems (ASes) to compromise user anonymity. First, AS-level adversaries can exploit the asymmetric nature of Internet routing to increase the chance of observing at least one direction of user traffic at both ends of the communication. Second, AS-level adversaries can exploit natural churn in Internet routing to lie on the BGP paths for more users over time. Third, strategic adversaries can manipulate Internet routing via BGP hijacks (to discover the users using specific Tor guard nodes) and interceptions (to perform traffic analysis). We demonstrate the feasibility of Raptor attacks by analyzing historical BGP data and Traceroute data as well as performing real-world attacks on the

journalists, businesses and ordinary citizens concerned about the privacy of their online communications [9].

Along with anonymity, Tor aims to provide low latency and, as such, does not obfuscate packet timings or sizes. Consequently, an adversary who is able to observe traffic on both segments of the Tor communication channel (*i.e.*, between the server and the Tor network, and between the Tor network and the client) can correlate packet sizes and packet timings to deanonymize Tor clients [45, 46].

There are essentially two ways for an adversary to gain visibility into Tor traffic, either by compromising (or owning enough) Tor relays or by manipulating the underlying network communications so as to put herself on the forwarding path for Tor traffic. Regarding network threats, large Autonomous Systems (ASes) such as Internet Service Providers (ISPs) can easily eavesdrop on a portion of all links, and observe any unencrypted information, packet headers, packet timing, and packet size. Recent declarations by Edward Snowden have confirmed

What can go wrong?

Routing attacks can be used to hijack DNS requests (https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum)

Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | Apr 24, 2018, 1:40pm EDT

What can go wrong?

Routing attacks can be used to
partition the Bitcoin network!
(https://btc-hijack.ethz.ch)

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

https://btc-hijack.ethz.ch

Maria Apostolaki
ETH Zürich
apmaria@ethz.ch

Aviv Zohar
The Hebrew University
avivz@cs.huji.ac.il

Laurent Vanbever
ETH Zürich
lvanbever@ethz.ch

***Abstract*—As the most successful cryptocurrency to date, Bitcoin constitutes a target of choice for attackers. While many attack vectors have already been uncovered, one important vector has been left out though: attacking the currency via the Internet routing infrastructure itself. Indeed, by manipulating routing advertisements (BGP hijacks) or by naturally intercepting traffic, Autonomous Systems (ASes) can intercept and manipulate a large fraction of Bitcoin traffic.**

This paper presents the first taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting individual nodes, and large-scale attacks, targeting the network as a whole. While challenging, we show that two key properties make routing attacks practical: *(i)* the efficiency of routing manipulation; and *(ii)* the significant centralization of Bitcoin in terms of mining and routing. Specifically, we find that any network attacker can hijack few (<100) BGP prefixes to isolate ~50% of the mining power—even when considering that mining pools are heavily multi-homed. We also show that on-path network attackers can considerably slow down block propagation by interfering with few key Bitcoin messages.

We demonstrate the feasibility of each attack against the deployed Bitcoin software. We also quantify their effectiveness on the current Bitcoin topology using data collected from a Bitcoin supernode combined with BGP routing data.

The potential damage to Bitcoin is worrying. By isolating parts of the network or delaying block propagation, attackers can cause a significant amount of mining power to be wasted, leading to revenue losses and enabling a wide range of exploits such as double spending. To prevent such effects in practice, we provide both short and long-term countermeasures, some of which can be deployed immediately.

One important attack vector has been overlooked though: attacking Bitcoin via the Internet infrastructure using *routing attacks*. As Bitcoin connections are routed over the Internet—in clear text and without integrity checks—any third-party on the forwarding path can eavesdrop, drop, modify, inject, or delay Bitcoin messages such as blocks or transactions. Detecting such attackers is challenging as it requires inferring the exact forwarding paths taken by the Bitcoin traffic using measurements (e.g., traceroute) or routing data (BGP announcements), both of which can be forged [41]. Even ignoring detectability, mitigating network attacks is also hard as it is essentially a human-driven process consisting of filtering, routing around or disconnecting the attacker. As an illustration, it took Youtube close to 3 hours to locate and resolve rogue BGP announcements targeting its infrastructure in 2008 [6]. More recent examples of routing attacks such as [51] (resp. [52]) took 9 (resp. 2) hours to resolve in November (resp. June) 2015.

One of the reasons why routing attacks have been overlooked in Bitcoin is that they are often considered too challenging to be practical. Indeed, perturbing a vast peer-to-peer network which uses random flooding is hard as an attacker would have to intercept many connections to have any impact. Yet, two key characteristics of the Internet's infrastructure make routing attacks against Bitcoin possible: *(i)* the efficiency of routing manipulation (BGP hijacks); and *(ii)* the centraliza-

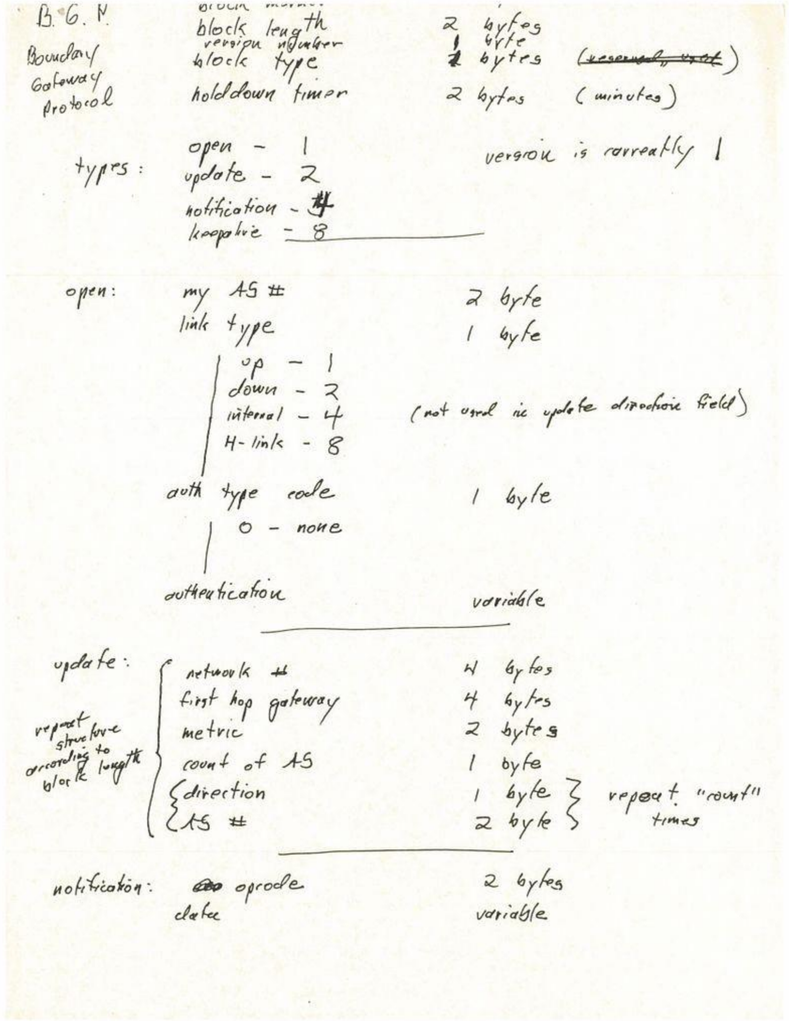
Outline

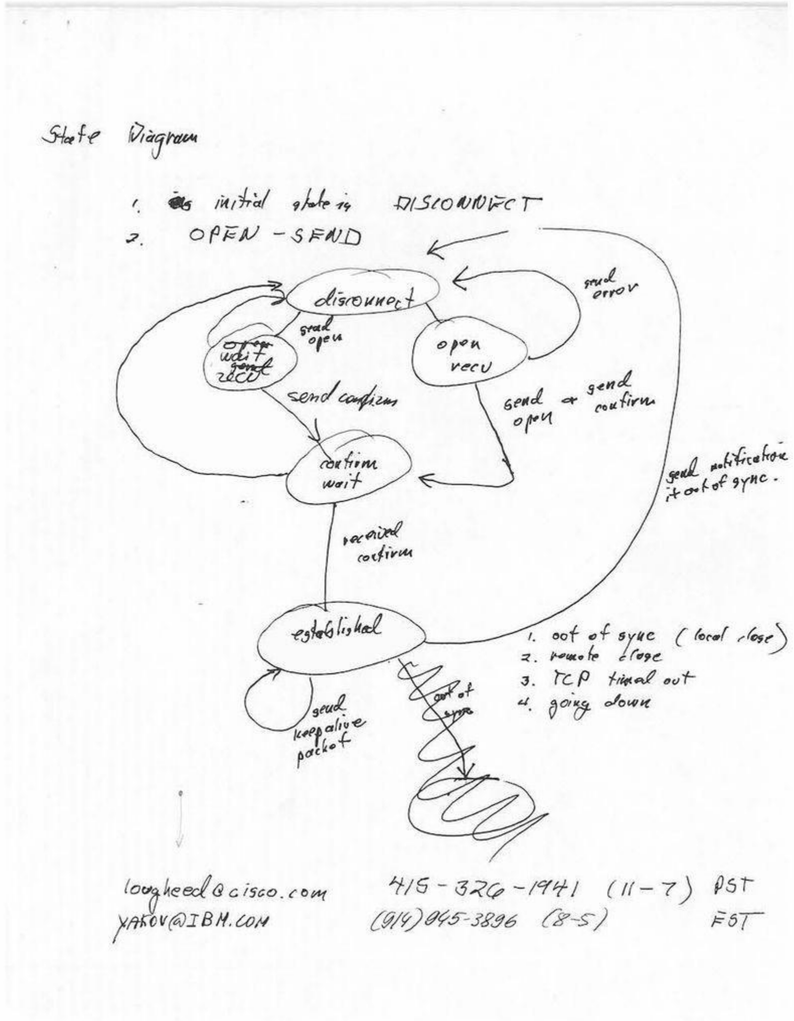
- BGP hijacks
  - How do BGP hijacks work and why are they possible?
  - Attacks enabled by hijacks
- Countermeasures
  - Best Current Practices (BCPs)
  - RPKI
  - BGPsec
- Outlook and summary
- Background (repetition)
  - IP addresses and autonomous systems (ASes)
  - The Border Gateway Protocol (BGP)

BGP Hijacks

Mechanisms and Attacks

BGP: The Two-Napkin Protocol





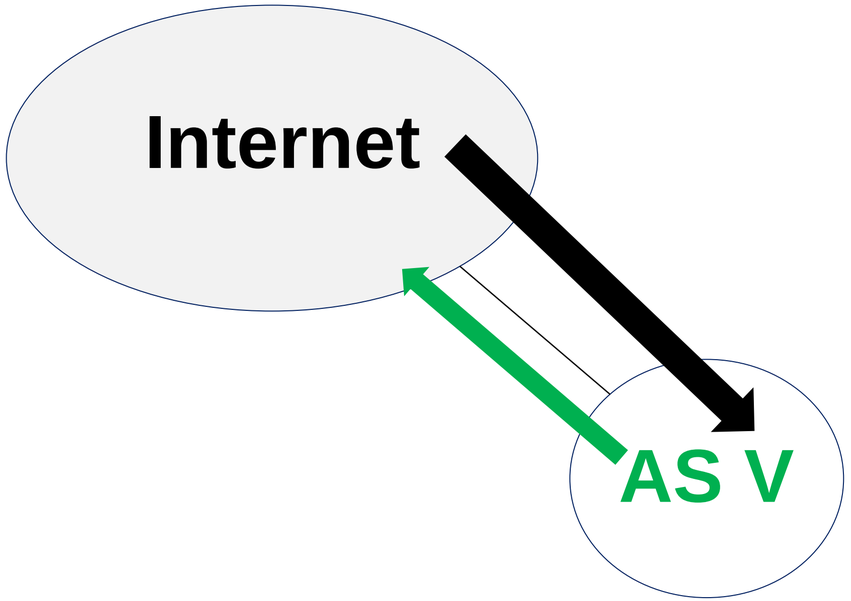
Prefix Origination and Hijacking

- IP prefix origination into BGP
  - Prefix advertised by the AS who owns the prefix
  - … or by upstream provider(s) on its behalf
- IP prefix hijacking
  - A malicious (or misconfigured) AS originates a prefix *it does not own*
  - Today, no proper verification in place

Problem 1:

BGP does not validate the origin of advertisements

Prefix Hijacking

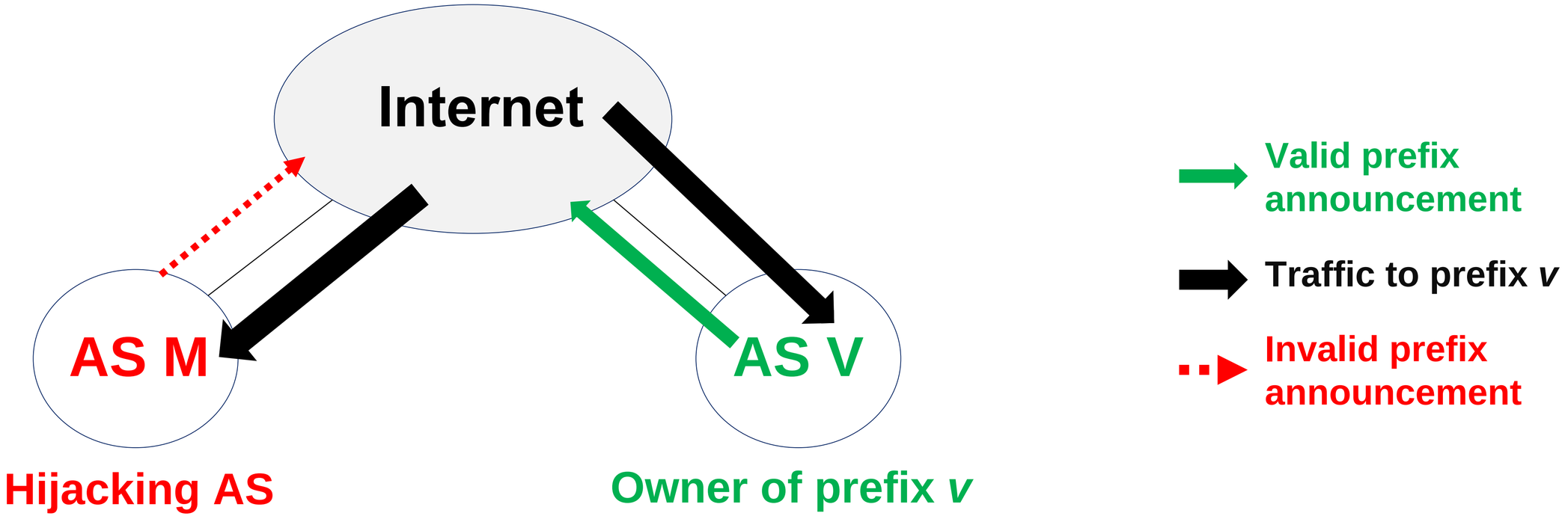


Valid prefix announcement

Traffic to prefix *v*

Owner of prefix *v*
(129.132.0.0/16)

Prefix Hijacking

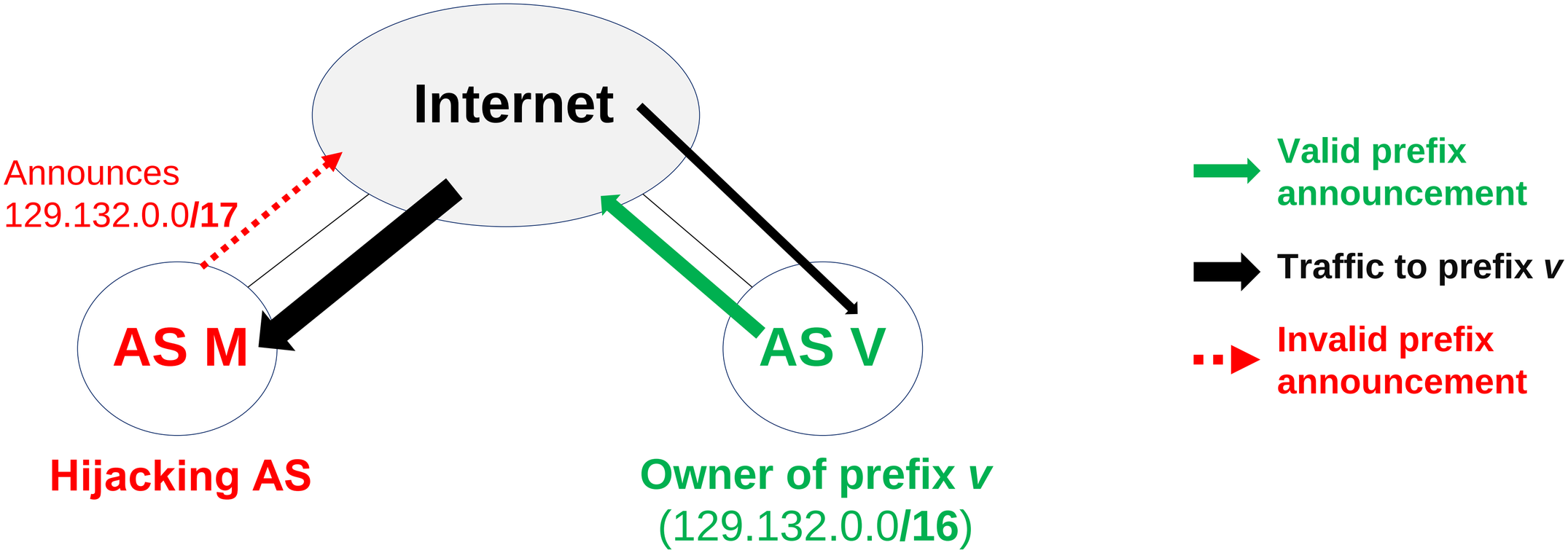


Problem: fraction of traffic to *prefix v* is hijacked by AS M

Number of affected sources depends on business relationships, topology, policies.

Further literature: https://www.princeton.edu/~pmittal/publications/sico-ccs19.pdf

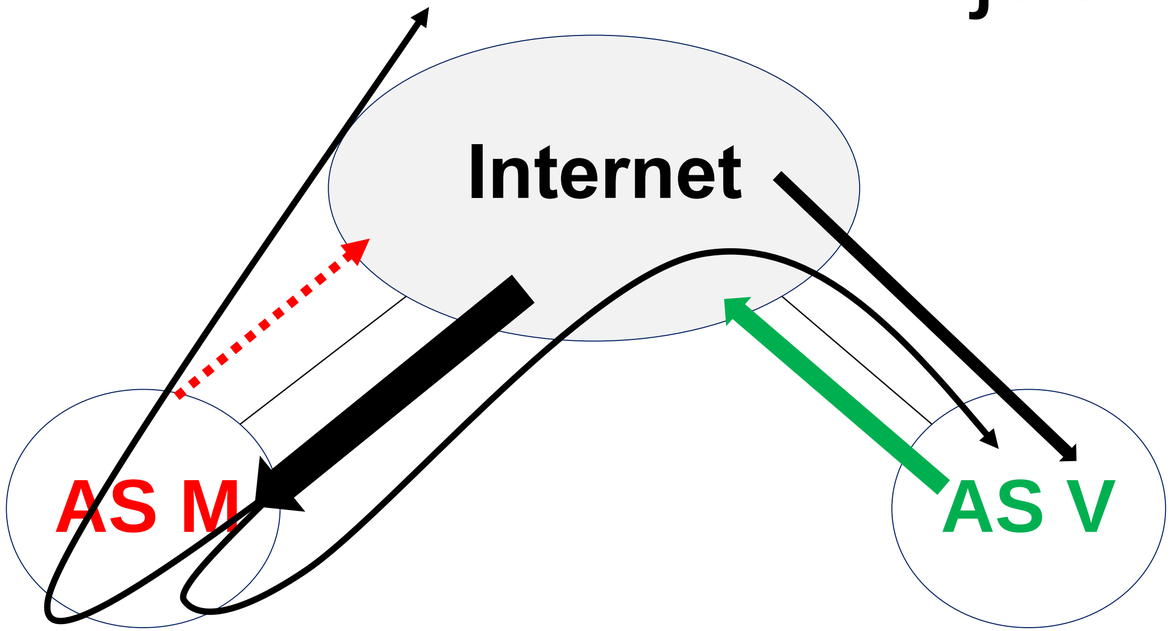
Prefix Hijacking



Stronger Variation: Sub-Prefix Hijacking

- AS M originates a longer (more specific) prefix for the victim's address space (up to /24 is allowed)
- Traffic follows the **longest (most specific)** matching prefix
- Why can't V announce more specific prefixes by default?

Prefix Hijacking



Hijacking AS

Owner of prefix *v*

Valid prefix announcement

Traffic to prefix *v*

Invalid prefix announcement

What can be done to the hijacked traffic?

- Blackholed (drop traffic) } **Traffic does not reach destination**
- Redirected
- Intercepted } **Traffic reaches destination**

How to perform BGP *interception*

- *Selective announcement* of hijacked prefix only to some neighbors
  - Problem: neighbors may still learn hijacked routes from their peers
- Use *BGP poisoning* (see next slides)
  - Only select neighbors use hijacked route
- Use *BGP communities* to ensure the announcement only reaches certain ASes
  - Can tell an AS not to forward announcement to specific other ASes using the “NoExportSelect” action
  - [Birge-Lee, Wang, Rexford, Mittal 2019]
    “SICO: Surgical Interception Attacks by Manipulating BGP Communities

Prefix Hijacking Examples

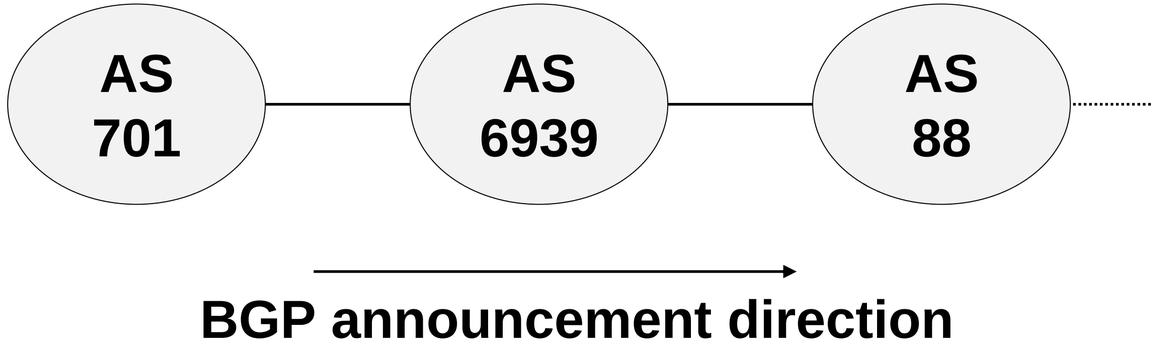
How to do BGP hijacking in 3 steps

1. Set up an AS and border router or compromise someone else's router
2. Configure router to originate the target (sub-)prefix
3. Get other ASes to accept the wrong route
   - Many ASes do not discard wrong routes (no or insufficient filtering)

Problem 2:
BGP does not validate the content of advertisements

ASes can modify the BGP path

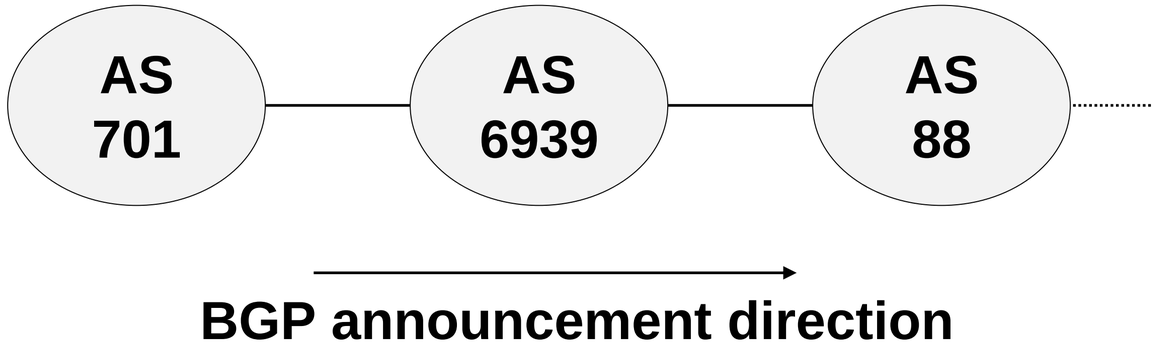
- Remove ASes from the AS path
  - Legitimate AS Path: [AS 701, AS 6939, AS 88]
  - Remove AS 6939: [AS 701, AS 88]



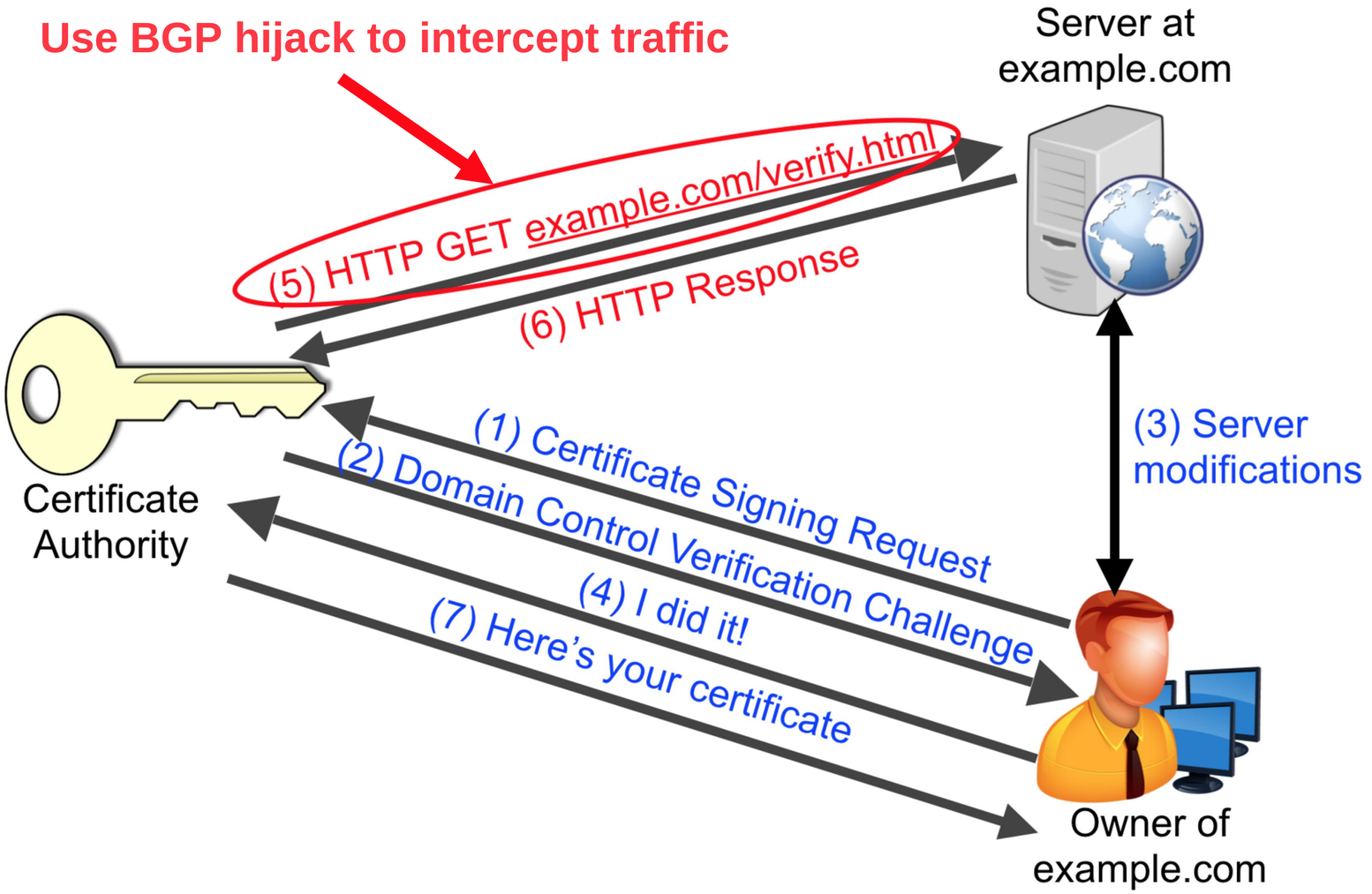
- Motivation
  - Attract traffic by making path look shorter
  - Attract sources that try to avoid AS 6939
- Who can tell that this AS path is a lie?
  - Only AS 701; AS 88 *could* have a direct connection to AS 701

ASes can modify the BGP path

- Add ASes to the AS path
  - Legitimate AS Path: [AS 701, AS 88]
  - Add 6939 in-between:
    [AS 701, AS 6939, AS 88]
- Motivation
  - Trigger loop detection in AS 6939
    - Denial-of-service attack on AS 6939
    - “BGP poisoning”: AS 6939 will not accept this announcement and forward traffic based on other announcements
  - Make your AS look like it has richer connectivity
- Who can tell that this AS path is a lie?
  - AS 6939 could, if it sees the route
  - AS 701 could, but may not care



Obtaining Fake Certificates with ACME



Source: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-birge-lee.pdf

Other Attacks on BGP

- Denial-of-service attacks
  - Overloading the link between BGP routers
    - Cause packet loss and delay
  - Send bogus TCP packets
    - FIN/RST to close the session
    - SYN floods to overload the router
- Eavesdrop on or tamper with messages by tapping the link
- Most such attacks are easy to defend against and are no longer a large concern

Countermeasures

Best Current Practices, RPKI, BGPsec

What properties do we want?

1. Only an AS that owns an IP prefix is allowed to announce it
   - Can be proven cryptographically
2. Routing messages are authenticated by all ASes on the path
   - Cryptographic protection
   - ASes cannot add or remove other ASes in BGP announcements

BGP Security Today

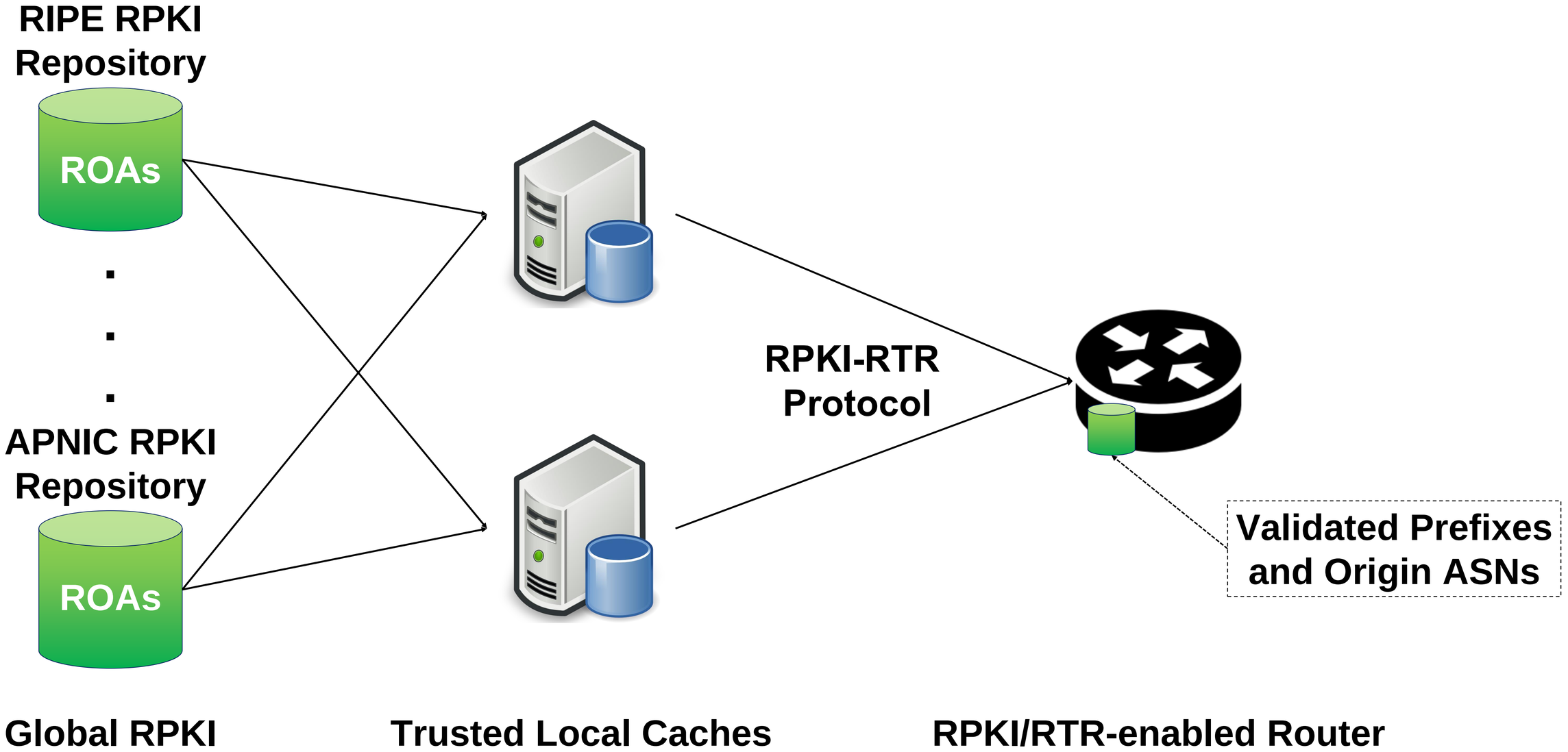
BGP Security Today

- Applying Best Current Practices (BCPs)
  - Securing the BGP peering session between routers (authentication, priority over other traffic)
  - Filtering routes by prefix and AS path
  - Filters to block unexpected control traffic
- Enter prefixes into Internet Routing Registries (IRRs) and filter based on these entries
- This is not good enough
  - Depends on vigilant application of BCPs
  - Doesn't address fundamental problems
    - Can't tell who owns an IP address block
    - Can't tell if the AS path is bogus or invalid
    - Can't be sure the data packets follow the chosen route

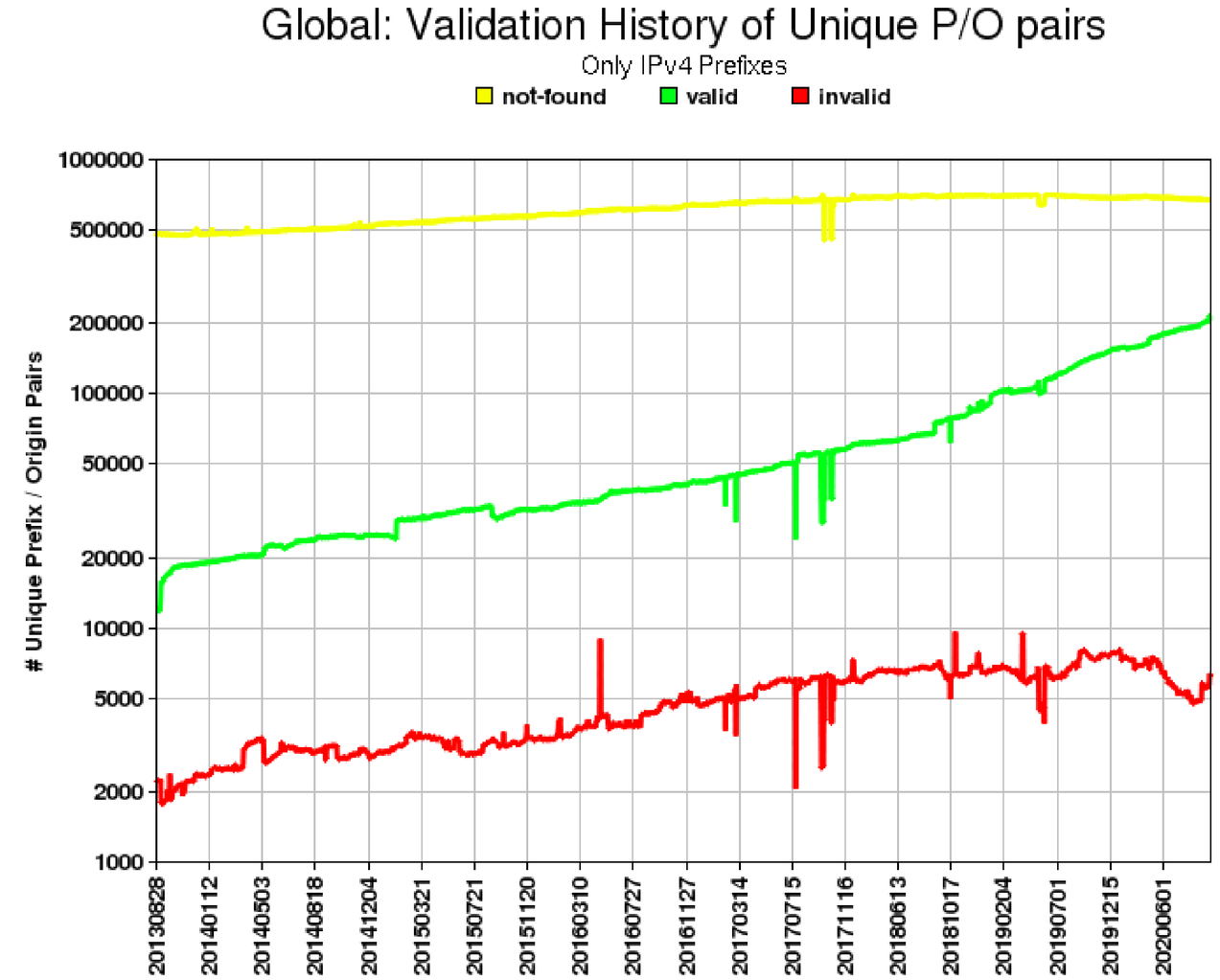
Solution to Problem 1: Origin Authentication

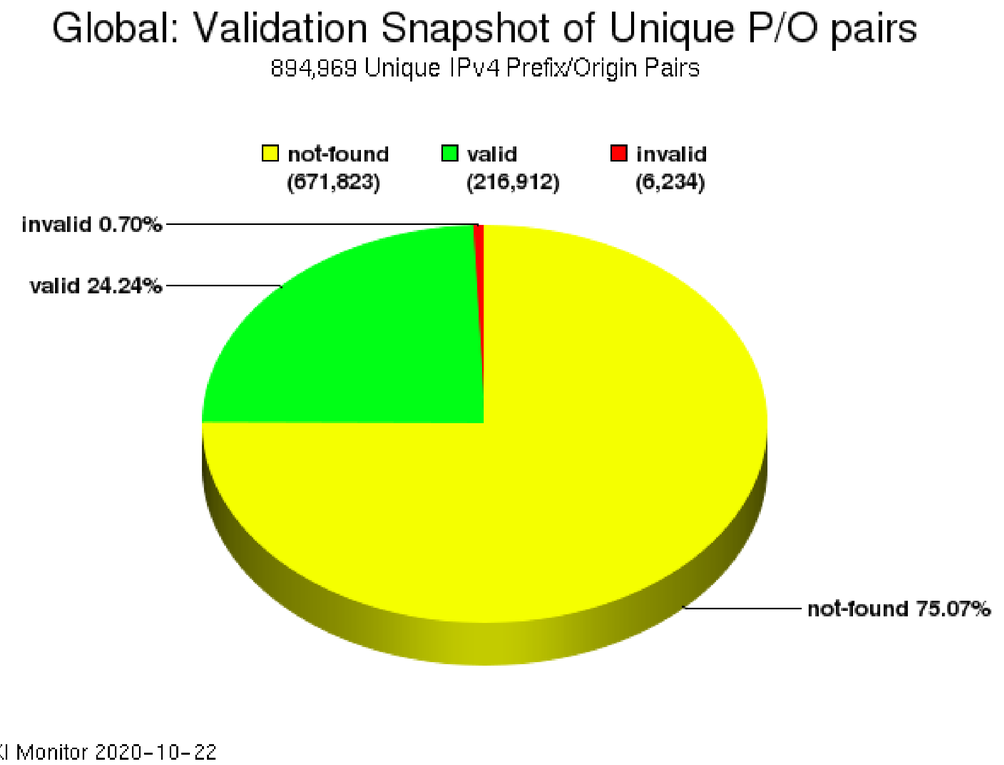
- Required: Ability to prove ownership of resources
- Resource Public-Key Infrastructure (RPKI)
  - A “secure database” to map Internet number resources to a trust anchor
  - A digital certificate proves that an AS is the current holder of a specific resource
  - Each RIR is a root of trust
- Enables issuance of Route Origination Authorizations (ROAs)
  - States which AS is authorized to announce certain IP prefixes
  - Can determine the maximum length of the prefix that the AS is allowed to advertise → avoid sub-prefix hijacking
  - Certificates follow same delegation as IP addresses from RIRs
  - Signed and distributed out-of-band
- Requires no actual modification to BGP (out-of-band checking)

Origin Authentication in an ISP



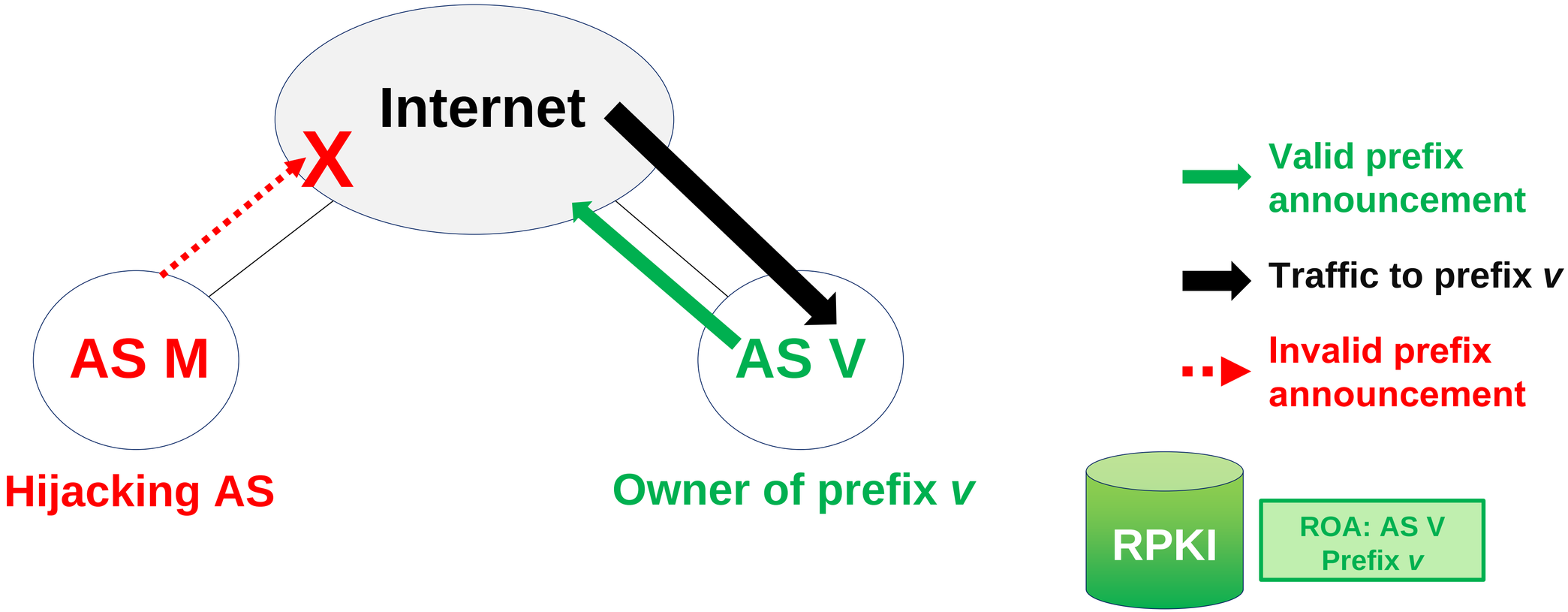
Deployment of Origin Authentication





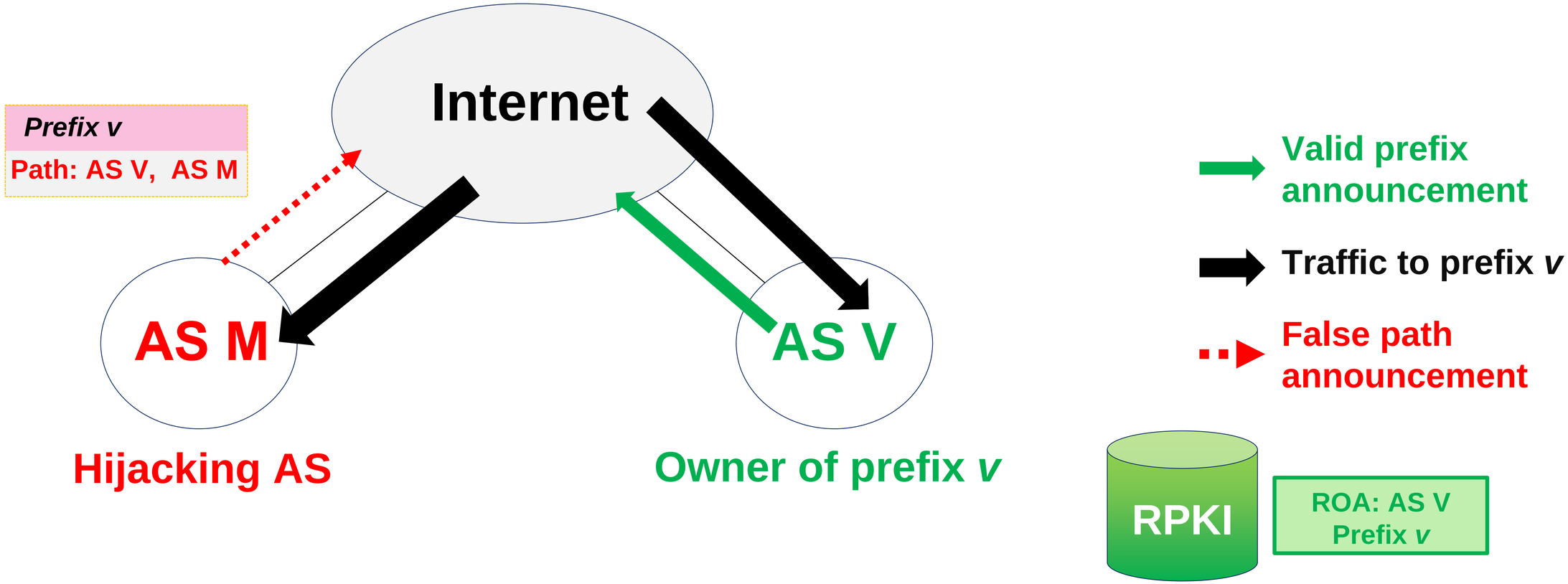
Source: https://rpki-monitor.antd.nist.gov/

Origin Authentication Operation



- BGP routers in other ASes receive the announcement from AS M for prefix *v*
- BGP routers in other ASes check against ROAs in RPKI for prefix *v*
- BGP routers would drop the announcement since no valid ROA for AS M

Origin Authentication Is Not Enough

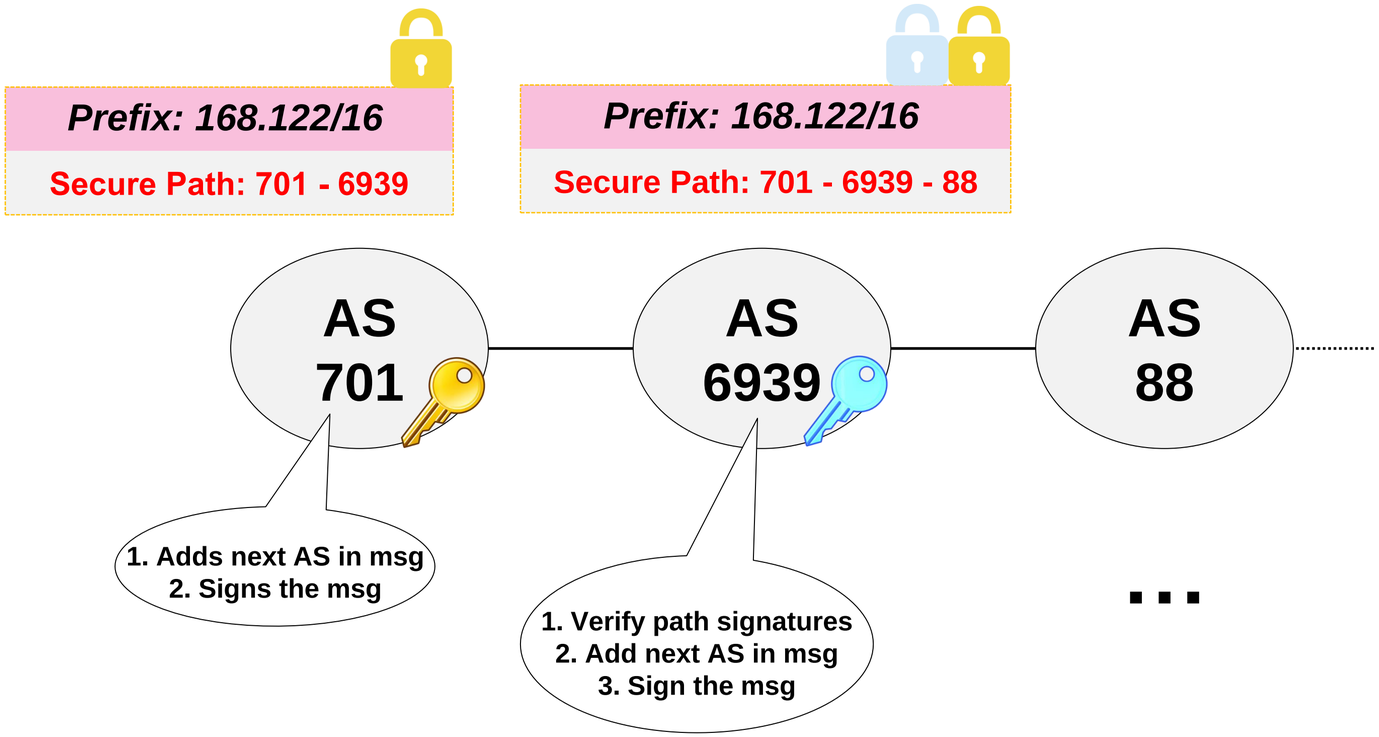


- AS M appends itself on the path after the entry for AS V
- BGP routers in other ASes check against ROAs in RPKI for prefix *v*, and find a valid ROA for prefix *v*
- AS M manages to attract a fraction of traffic for AS V

Solution to Problem 2: BGPsec

- Secure version of BGP
  - Based on S-BGP (2000)
  - Standardized in RFC 8205 (2017)
- Secures the AS-PATH attribute
  - Prevents crafting a valid origin on path
  - Prevents path poisoning
- Idea: Origin authentication + cryptographic signatures
  - Sign received update message to prove that path was correctly updated
  - Include the next AS in the signature

BGPsec : Secure Version of BGP



- BGPsec can validate that
  - the AS path indicates the order ASes were traversed and
  - no intermediate ASes were added or removed
- RPKI is used to verify AS key material (as in origin authentication)

BGPsec in Incremental Deployment

- Insecure ASes use legacy BGP, and secure ASes must accept legacy insecure routes
- Problem 1: routing policies can interact in ways that can cause BGP wedgies [RFC 4264] [Lychev, Goldberg, Shapira, 2013]
  - How to prioritize security in routing decisions?
  - Prioritize security over business relationships or AS-path length?
  - NANOG survey of 100 network operators shows that 10%, 20%, and 41% would place security as a 1st, 2nd, and 3rd priority respectively [Gill, Shapira, Goldberg, 2012]
- Problem 2: protocol downgrade attacks
  - If operators don't prioritize security, an attacker can just use legacy BGP to announce bogus routes to BGPsec neighbors

BGPsec in Incremental Deployment

- Problem 3: performance degradation
  - Prefix aggregation no longer possible
  - Expensive asymmetric cryptography (signature and validation)
  - → Slower convergence
- Unless security is the first priority or BGPsec deployment is very large, security benefits from partially deployed BGPsec are meager
  [Lychev, Goldberg, Shapira, 2013]
- Deployment challenges
  - Different message format
  - Complete, accurate registries (e.g., prefix ownership)
  - Public-Key Infrastructure

} **applies also to origin auth.**

Outlook and Summary

Other Approaches: Extensive Monitoring

- Monitoring BGP update messages and use past history
  - Remember which ASes originate which prefixes
    - e.g., prefix 129.132.0.0/16 usually originated by AS 559
  - Remember AS-level edges and paths
    - e.g., never seen the sub-path “7018 88 1785”
  - Prefer routes that agree with the past
  - Delay adoption of unfamiliar routes when possible
- Out-of-band detection mechanism
  - Generate reports and alerts
  - ARTEMIS: https://www.inspire.edu.gr/artemis/
  - Internet Alert Registry (no longer active): https://www.cs.unm.edu/~karlinjf/IAR/
  - Prefix Hijack Alert System: https://dl.acm.org/citation.cfm?id=1267347

Other Approaches: Redesign Inter-domain Routing

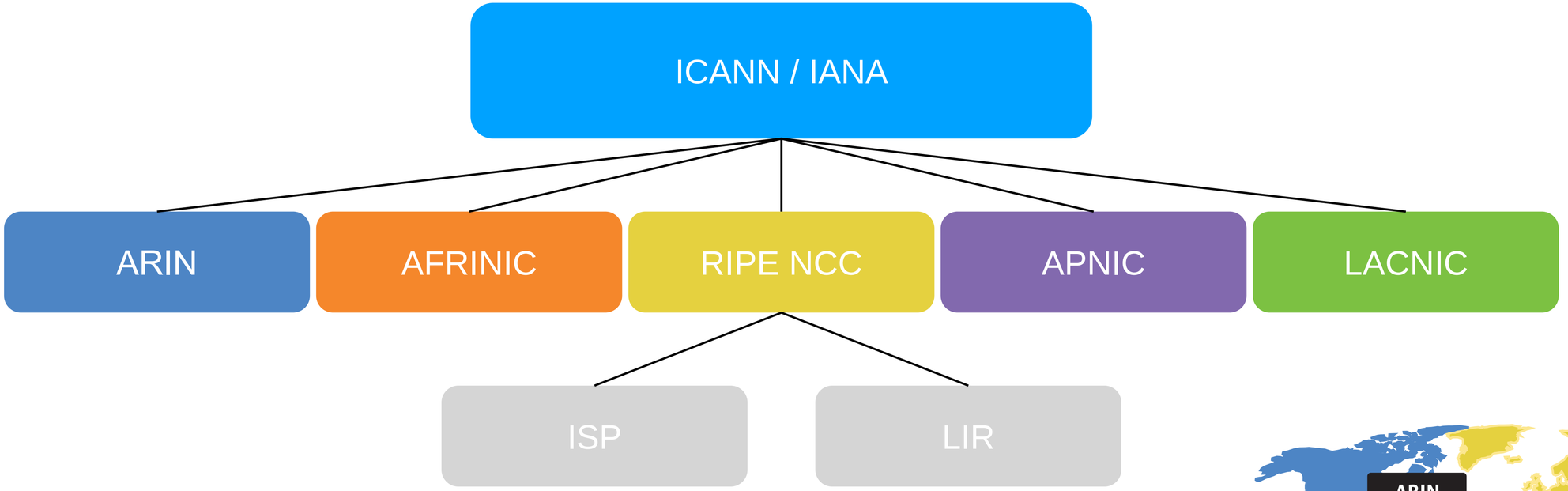
- BGP was not designed with security in mind
  - Entities that participate need to be trusted
  - Most security solutions are simple patches
  - Fundamental security problems don’t go away
- Proposals to redesign inter-domain routing with security in mind
  - Named-Data Networking & Information-Centric Networking
  - Accountable Internet Protocol
  - Passport: Secure and Adoptable Source Authentication
  - SCION: **S**calability, **C**ontrol, and **I**solation **o**n **N**ext-Generation Networks

Conclusions

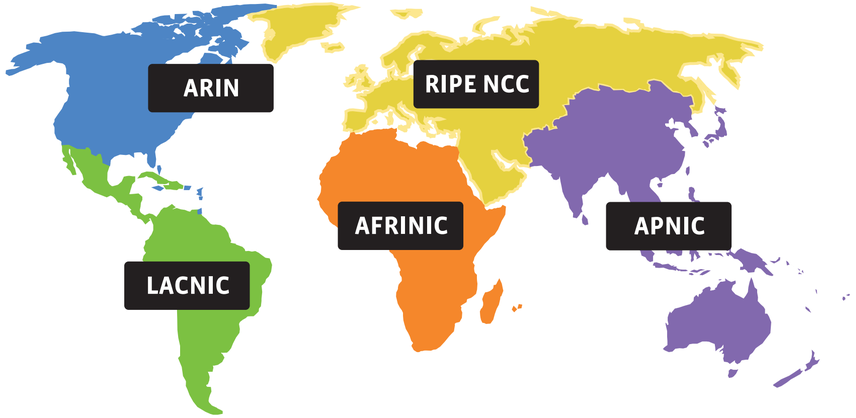
- “BGP is one of the largest threats on the Internet. It’s incredible, the insecurity of the routing system.”
  (Danny McPherson, CSO at Arbor Networks, Jan 2009)
- Lacking security of the routing protocol enables a myriad of attacks
- Improving inter-domain security is challenging
  - Upgrading equipment is expensive
  - Requires cooperation amongst many entities
  - Unclear benefits for first-movers
- Proposals to improve BGP or completely replace it are emerging, but large-scale deployment is difficult

IP Addresses, Autonomous Systems, and the Border Gateway Protocol

Allocation and Ownership of IP Addresses



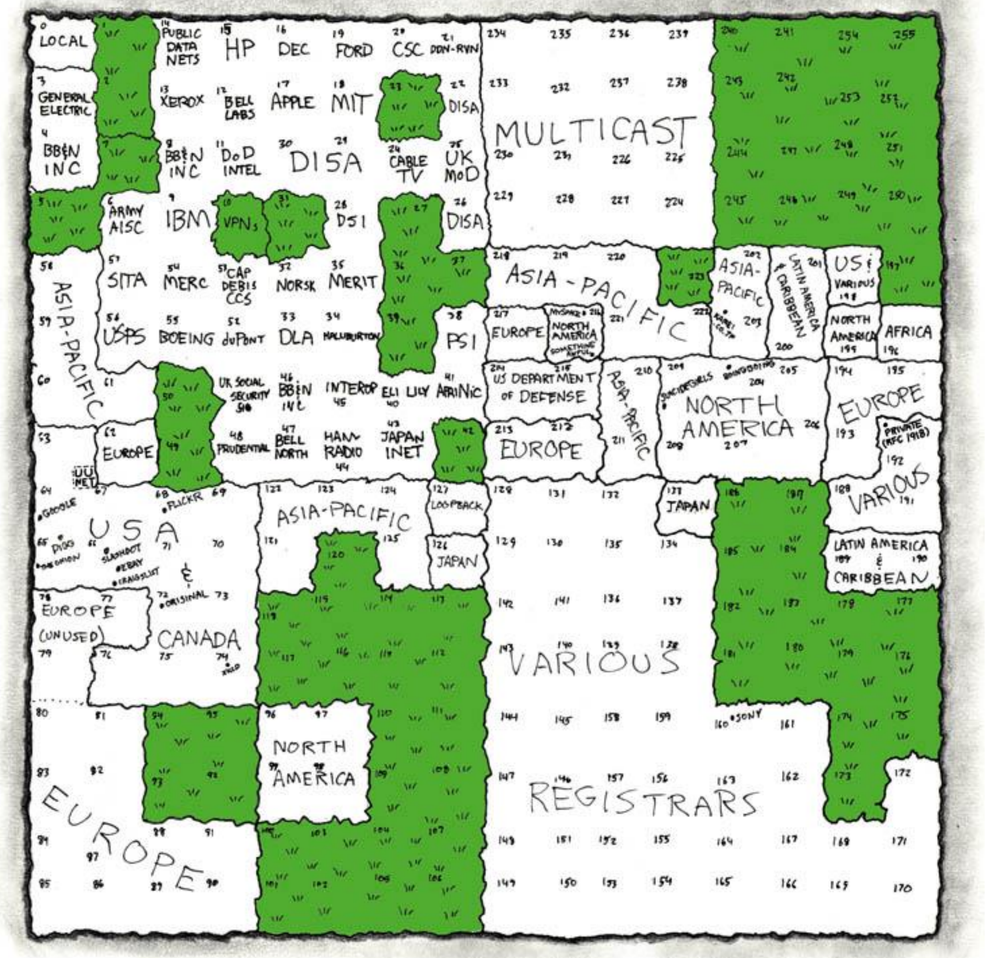
Regional Internet Registries (RIRs)



Source: https://www.iana.org/numbers

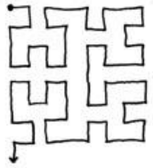
MAP OF THE INTERNET

THE IPv4 SPACE, 2006



THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

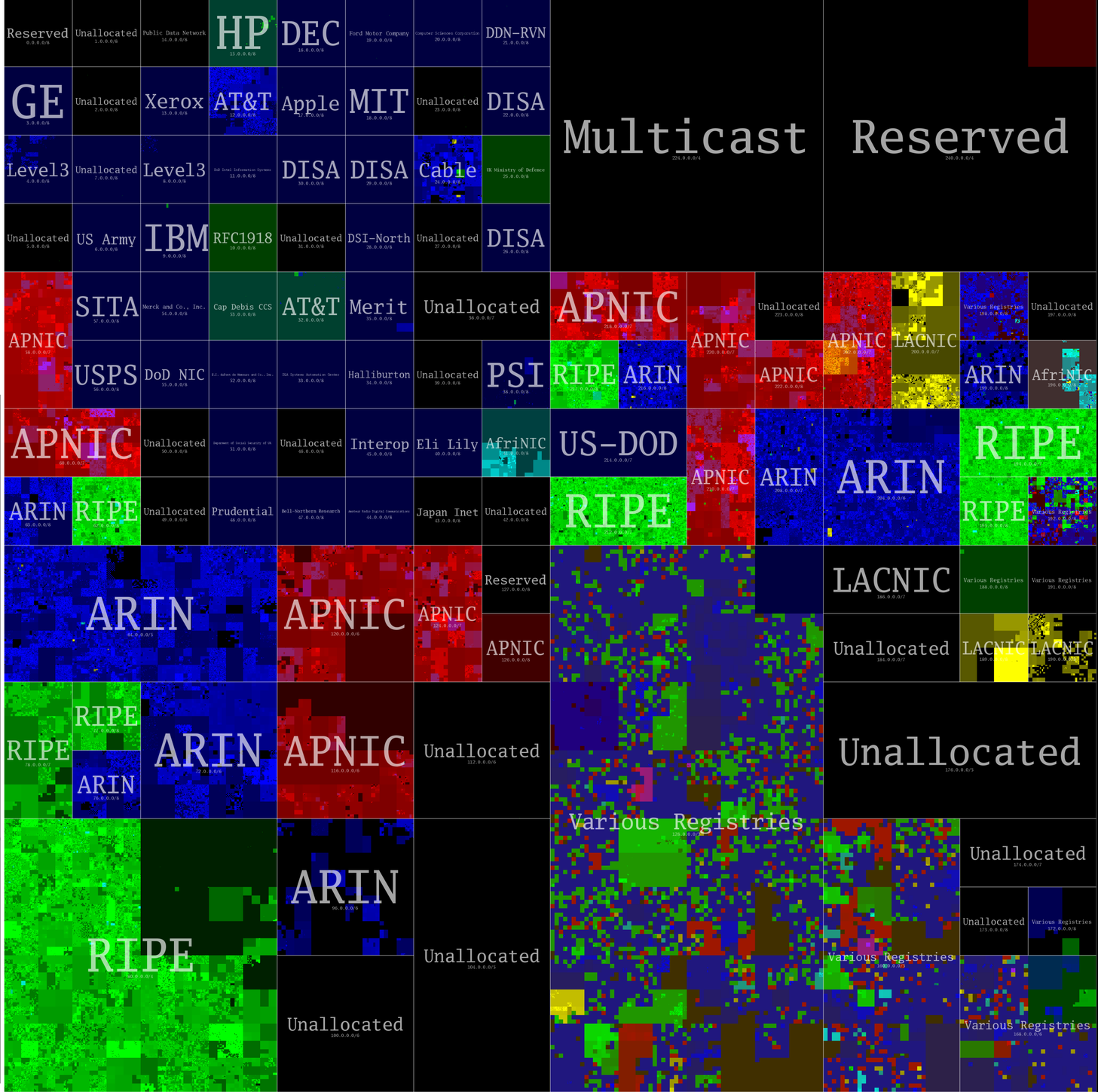
0 1 14 15 16 19 →
3 2 13 12 17 18
4 7 8 11
5 6 9 10



= UNALLOCATED BLOCK

https://xkcd.com/195/

https://www.caida.org/research/id-consumption/whois-map/



Today, at 15:35 UTC+1 on 25 November 2019, we made our final /22 IPv4 allocation from the last remaining addresses in our available pool.

We have now run out of IPv4 addresses.

[RIPE NCC]

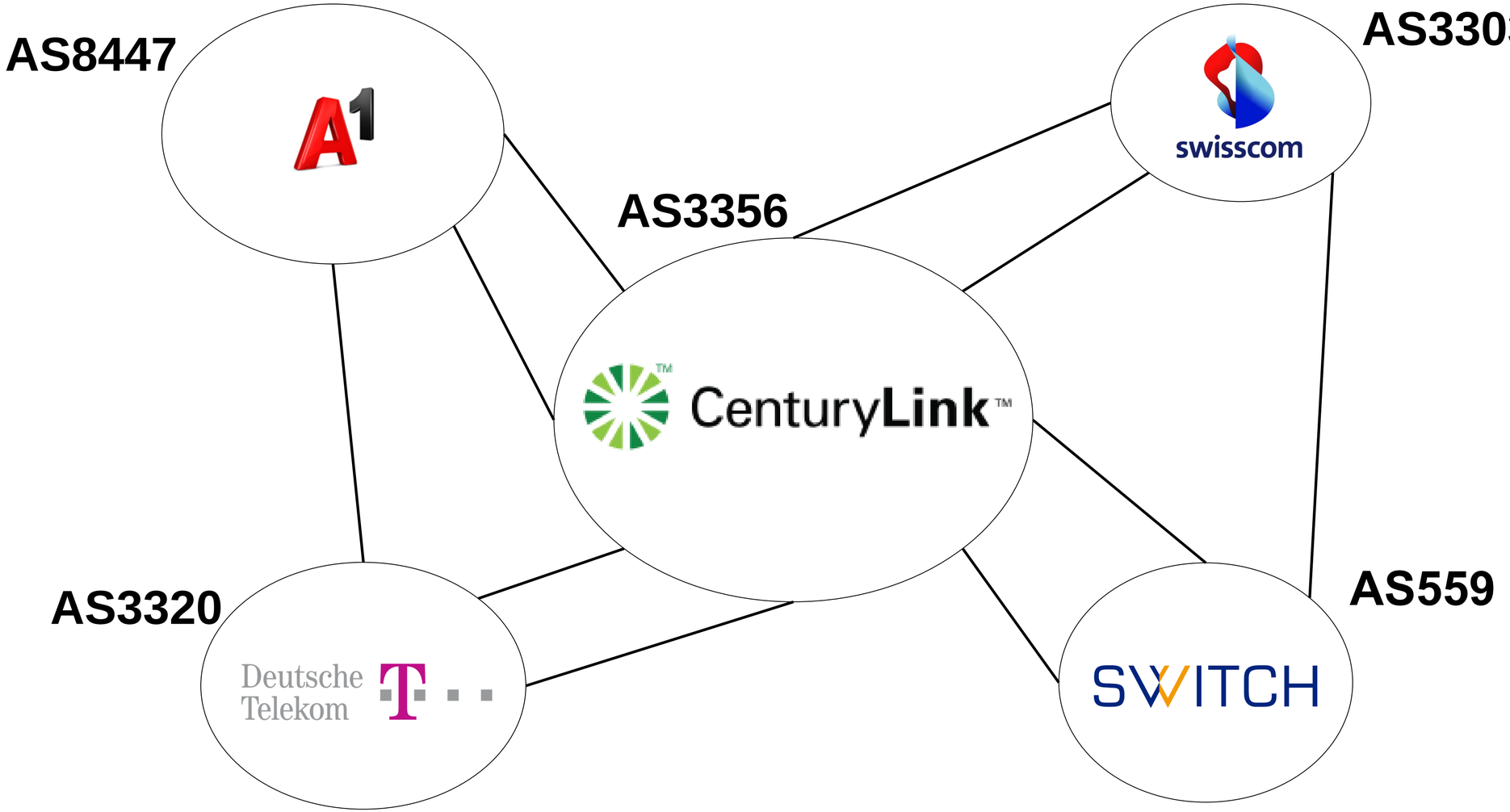
Allocation and Ownership of IP Addresses

- Highest authority: Internet Corporation for Assigned Names and Numbers (ICANN), Internet Assigned Numbers Authority (IANA)
- IP address ownership:
  - ICANN assigns address space to regional Internet registries (RIRs)
  - RIRs assign address space to ISPs or local internet registries (LIRs)
  - LIRs and ISPs assign individual addresses to end customers
- IP address space is allocated in *prefixes*: “<address>/<prefix length>”
  - 129.132.0.0/16: all IP addresses that start with 129.132 (first 16 bits)

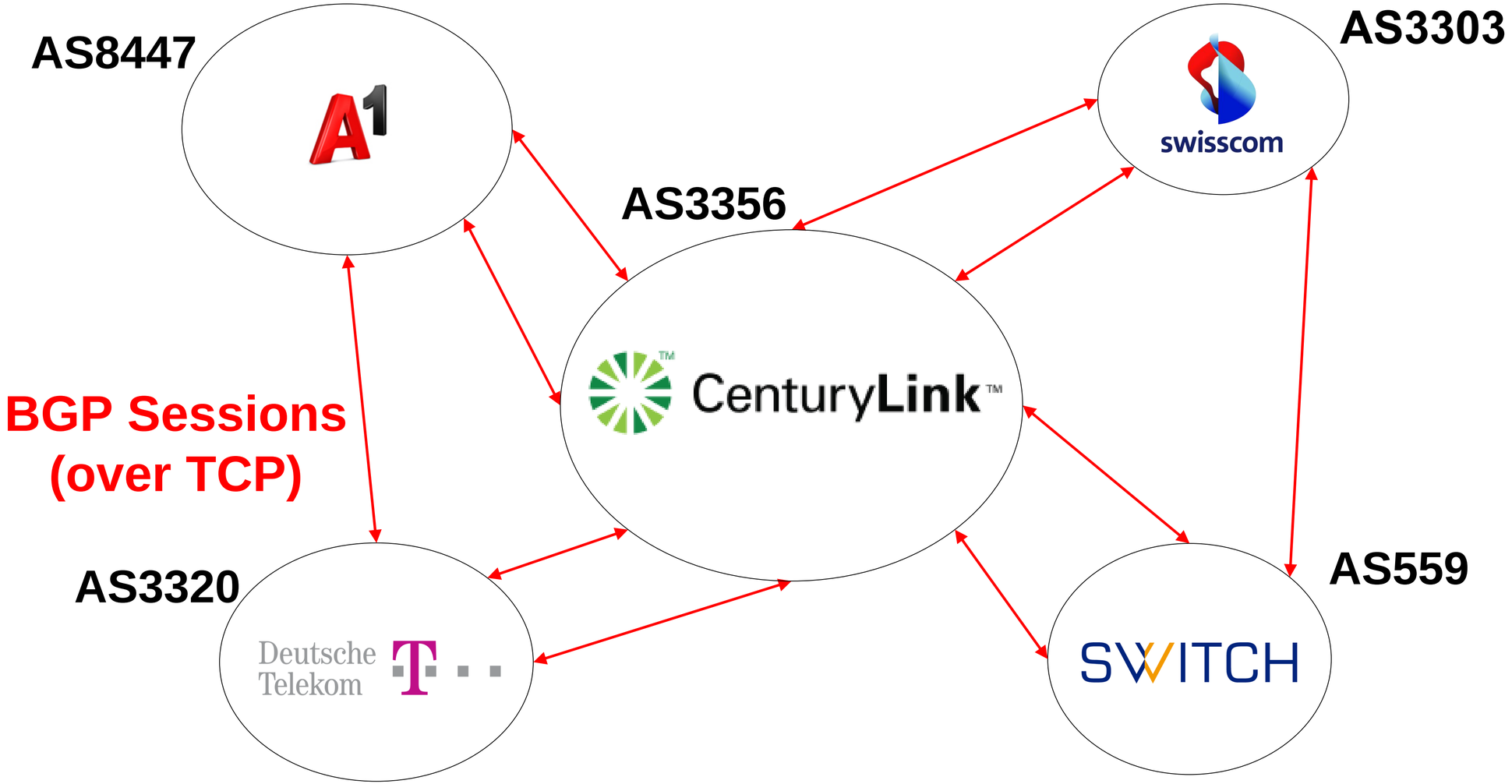
The Internet and BGP

- The Internet is a network of networks
  - More than 60’000 autonomous systems (ASes)
    - Internet service providers (ISPs, e.g., Swisscom, Deutsche Telekom)
    - Global backbone networks (CenturyLink, Verizon)
    - Universities, large companies (Google, Cloudflare)
- The Border Gateway Protocol (BGP) “glues” the Internet together
  - The routing protocol between ASes
  - Disseminates information about location and paths for IP prefixes
  - A path-vector protocol
- Business relationships shape topology

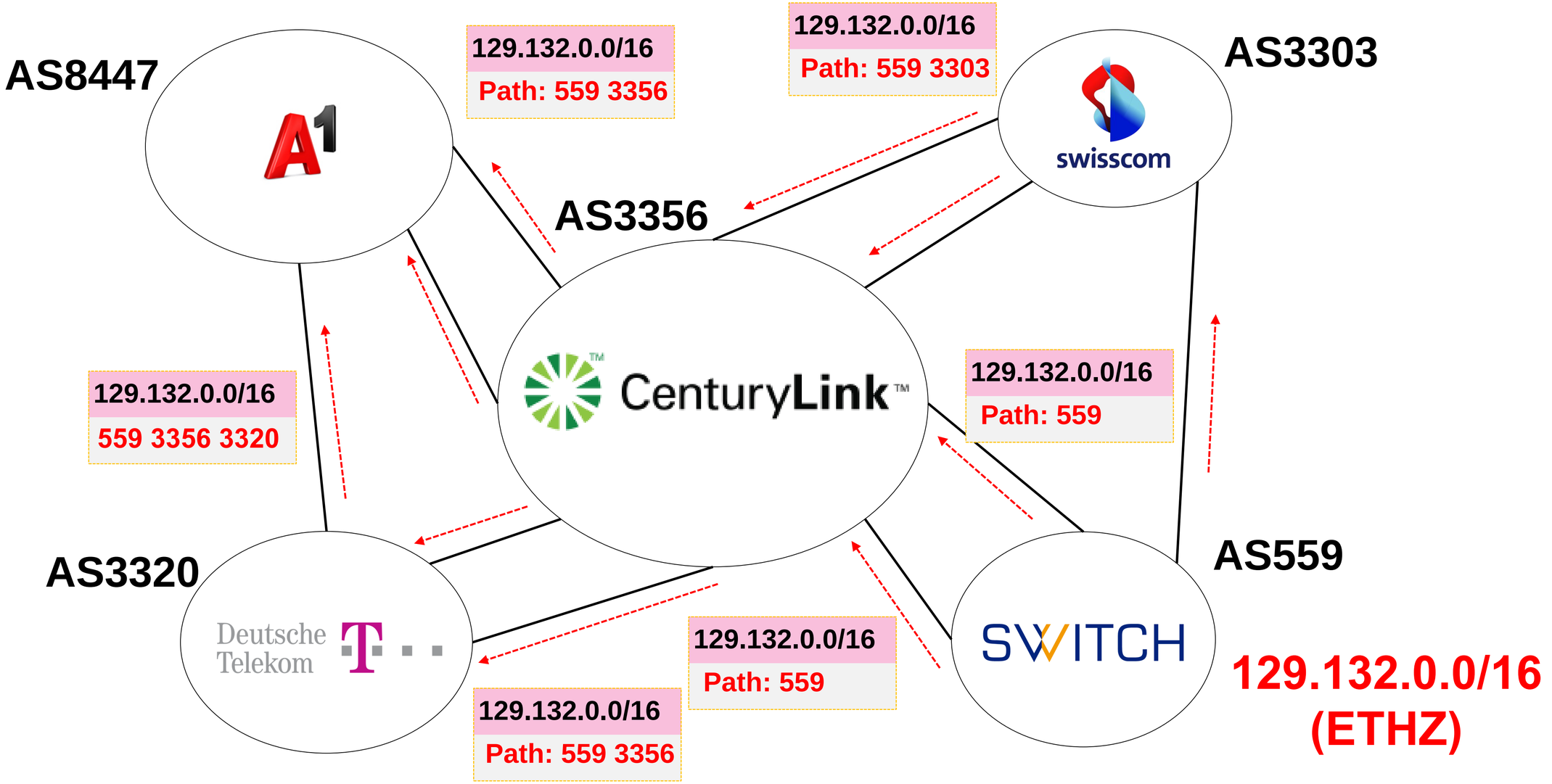
The Internet is a network of networks (ASes)



BGP “glues” these systems together

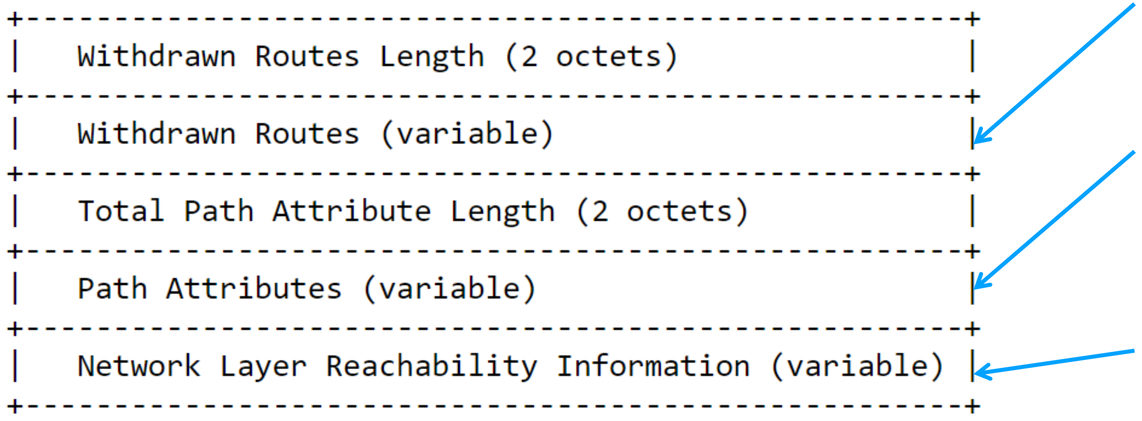


ASes exchange information about IP prefixes they can reach directly or indirectly



BGP Protocol Details

- BGP speaker sends and receives messages from peers over TCP connections on port 179.
- Messages sent include: OPEN, UPDATE, KEEPALIVE, NOTIFICATION.
- Route information is disseminated through UPDATE message using attributes:



IP prefixes which are no longer reachable via this path.

Information about the path itself, i.e., which ASes it traverses.

Details of prefixes which can be reached via this path. Includes address family (e.g. IPv4, IPv6, others) and address ranges.

Source: RFC4271

Relationships between ASes

- Several applications to look for AS relationships and IP prefixes
- Hurricane Electric BGP tool: https://bgp.he.net/
- Example: query for “AS559” (SWITCH)

Company Website: http://www.switch.ch/
Company Looking Glass: http://lg.net.switch.ch/

Country of Origin: Switzerland

Internet Exchanges: 4

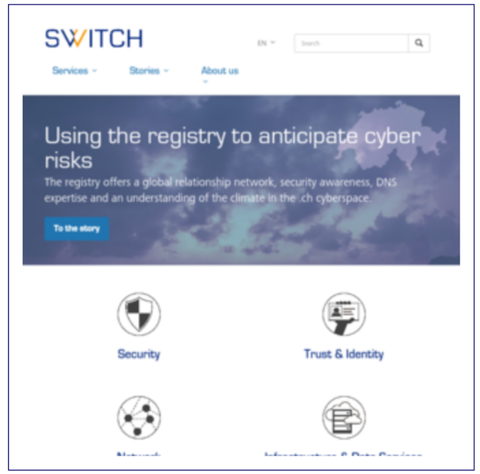
Prefixes Originated (all): 119
Prefixes Originated (v4): 107
Prefixes Originated (v6): 12

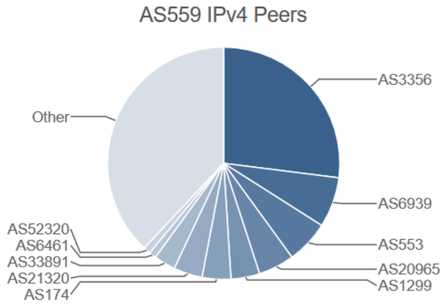
Prefixes Announced (all): 133
Prefixes Announced (v4): 120
Prefixes Announced (v6): 13

BGP Peers Observed (all): 162
BGP Peers Observed (v4): 148
BGP Peers Observed (v6): 105

IPs Originated (v4): 2,253,312
AS Paths Observed (v4): 502
AS Paths Observed (v6): 395

Average AS Path Length (all): 3.203
Average AS Path Length (v4): 3.247
Average AS Path Length (v6): 3.147



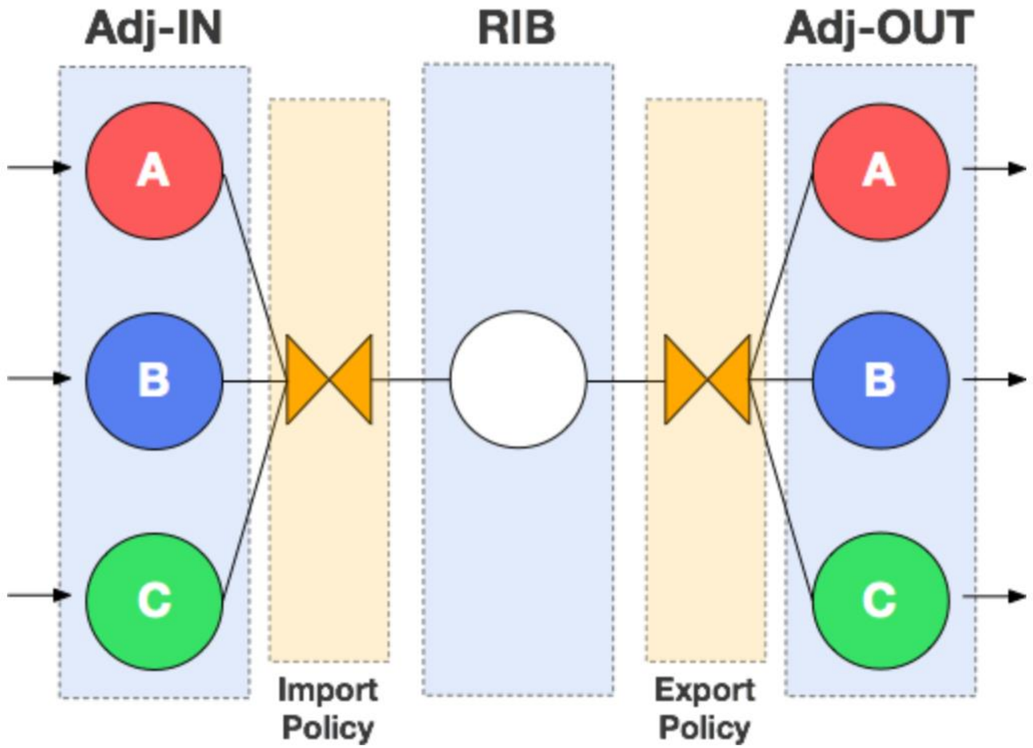


ASN	Name
AS3356	Level 3 Parent, LLC
AS6939	Hurricane Electric LLC
AS553	Universitaet Stuttgart
AS20965	GEANT Vereniging
AS1299	Telia Company AB
AS174	Cogent Communications
AS21320	GEANT Vereniging
AS33891	Core-Backbone GmbH
AS6461	Zayo Bandwidth
AS52320	GlobeNet Cabos Submarinos Colombia, S.A.S.

Source: https://bgp.he.net/AS559

Peering Policies

- Routes are accepted and advertised based on policies
- Policies are configured in the BGP daemons of the AS
- Policies can be used to *implement filters to prevent route leaks* (= falsely announced prefixes), or for business reasons



Source: https://github.com/osrg/gobgp/blob/master/docs/sources/policy.md

Internet Routing Registry

- Contains administrative, contact, and policy information
- Query European records at https://ripe.net
- Example: query for “AS3303” (Swisscom)

Responsible organisation: Swisscom (Schweiz) AG
Abuse contact info: abuse@ip-plus.net

Login to update | RIPEstat

```
aut-num:        AS3303
as-name:        SWISSCOM
descr:          Swisscom (Switzerland) Ltd
descr:          IP-Plus Internet Backbone
descr:
descr:          ---------------------------------------------------------------------
descr:
descr:          Abuse issues abuse@ip-plus.net
descr:          Operational issues noc@ip-plus.net
descr:          Peering requests IP-Plus.Peering@swisscom.com
descr:          Other info http://www.ip-plus.net
descr:
descr:          ---------------------------------------------------------------------
org:            ORG-SI1-RIPE # Transit:
import:         from AS3320 action pref=700; accept ANY
export:         to AS3320 announce AS-SWCMGLOBAL
import:         from AS174 action pref=700; accept ANY
export:         to AS174 announce AS-SWCMGLOBAL # Peers:
import:         from AS42 action pref=700; accept AS-PCH
import:         from AS137 action pref=700; accept AS-GARR
import:         from AS209 action pref=700; accept AS-QWEST
import:         from AS237 action pref=700; accept AS-MICHNET
import:         from AS286 action pref=700; accept AS-KPN
import:         from AS513 action pref=700; accept AS-CERNEXT
import:         from AS553 action pref=700; accept AS-BELWUE
import:         from AS577 action pref=700; accept AS577:AS-CUSTOMERS
import:         from AS680 action pref=700; accept AS-DFNTOWINISP
import:         from AS702 action pref=700; accept AS702:RS-EURO AS702:RS-CUSTOMER
import:         from AS766 action pref=700; accept AS-REDIRIS
import:         from AS786 action pref=700; accept AS-JANETPLUS
```

Source: https://apps.db.ripe.net/db-web-ui/#/query?bflag&searchtext=as3303&source=RIPE

How to create your own ISP in 4 steps

1. Register an autonomous system number to be able to connect via BGP to other networks
2. Request Internet number resources from your regional network coordination center:
   - Get assigned IPv4 and IPv6 prefixes which can be announced over BGP
3. Find other networks to connect to and exchange traffic with:
   - Typically interconnection at an exchange point such as SwissIX (peering)
   - Find an upstream ISP which will carry traffic to other parts of the world (IP transit)
4. Deploy hardware to the peering location and announce IP prefixes