BGP Insecurity

Understanding and mitigating BGP routing incidents

Presented at SGNOG7 by Lim Fung

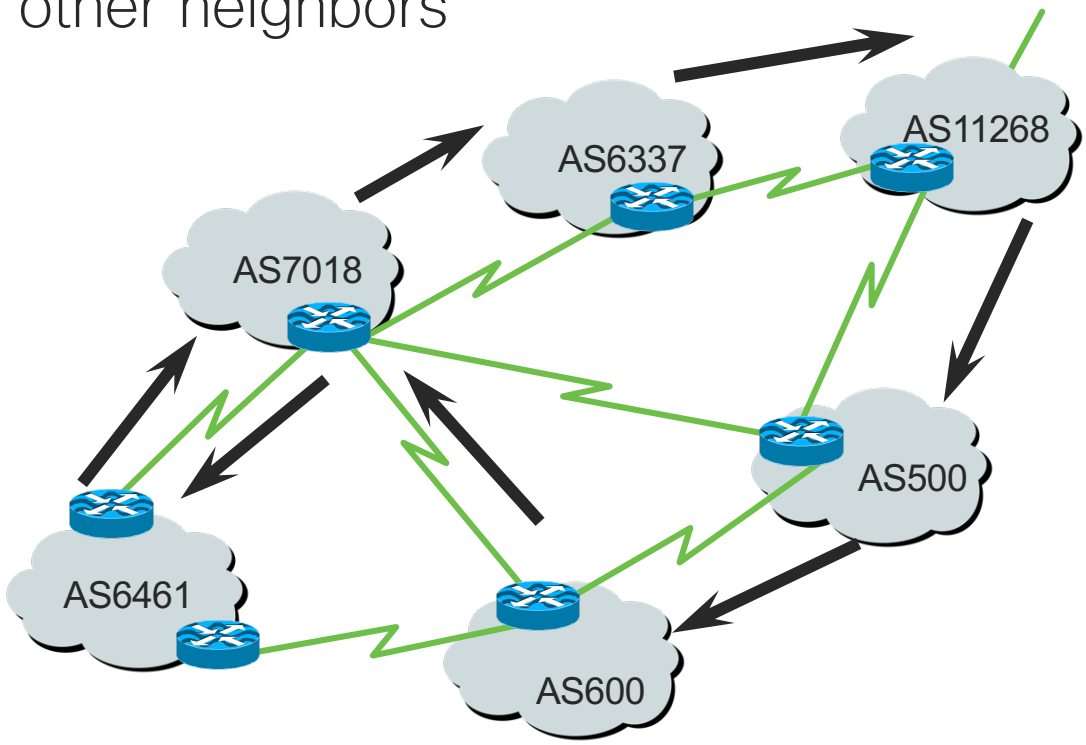
12th July 2019

Scope

- Introduction
- BGP Insecurity
- BGP vulnerabilities
- Mitigating Route Hijack
- Conclusion

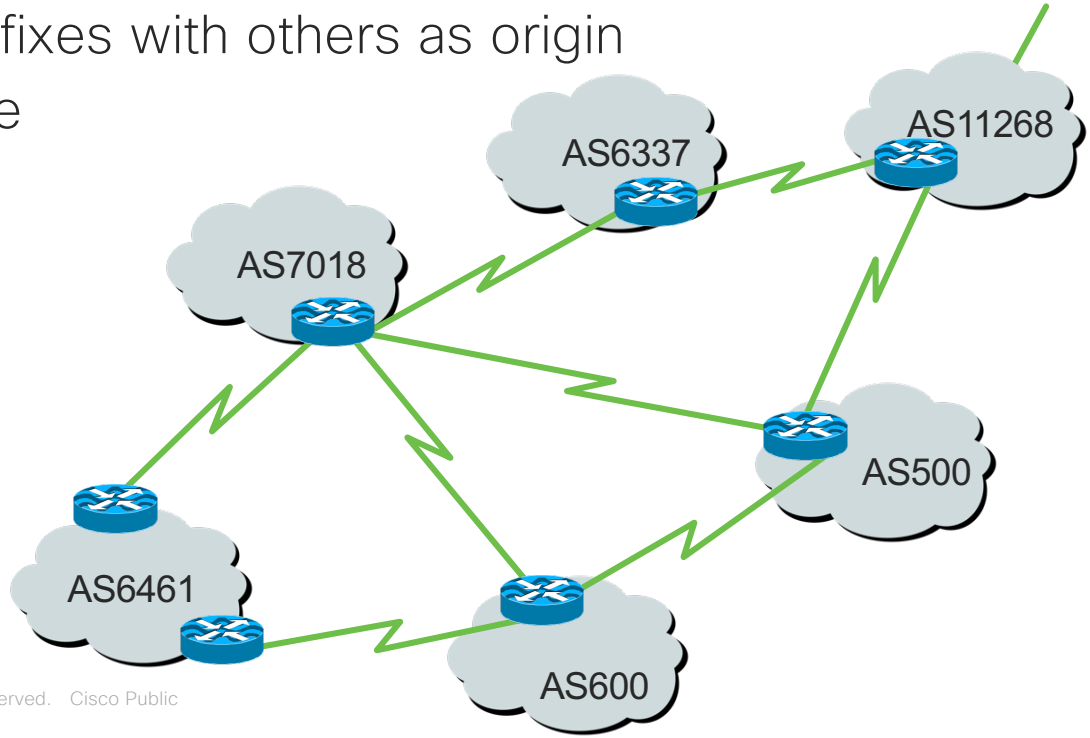
BGP insecurity

- Route distribution occurs by learning routes from a neighbor and advertising to other neighbors



BGP insecurity

- Route policies are required and used to prevent accepting bad stuff
  - BOGONS (Unassigned, Martian, Private address space)
  - Our own prefixes with others as origin
  - Default Route



BGP insecurity

- Policy about every prefix and every ASN requires a lot of work to create and update for constant changes – But is needed for protection
- Where do we get reliable data for this?

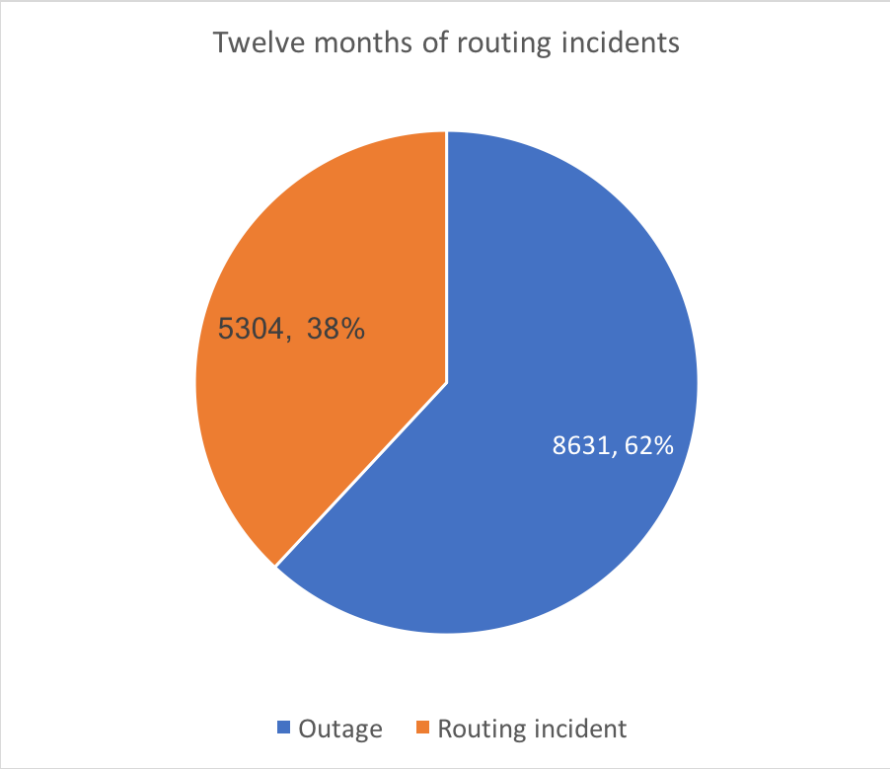
BGP insecurity

- Data sources such as IRR provide some automated ways. Data accuracy and reliability is not good.
- Poor adoption due to work involved and constant updating
- Historically it has been trust based – we advertise our prefixes and expect everyone to do same.
  - If we catch some one advertising wrong prefixes, we tell them not to. If it was a mistake they would comply.
  - If they don't stop advertising wrong prefixes, call their providers and tell them to not accept/filter out.

How prevalent are routing incidents?

State of Internet's routing system in 2017

- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident

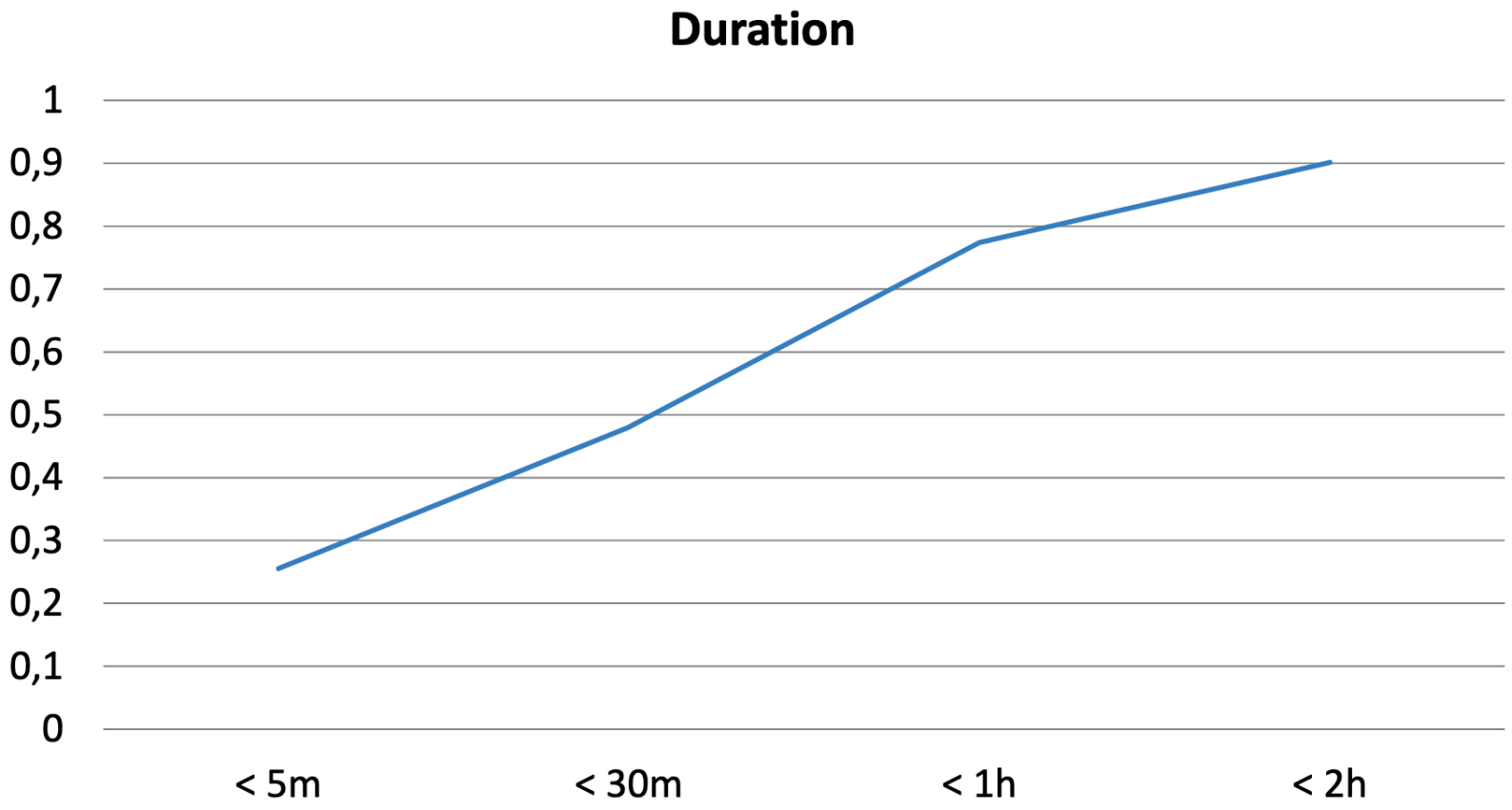


Source: https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

BGP insecurity

- BGP incidents may be transient, lasting from minutes to days or weeks. Incidents may be localized.
- Often a reactive approach, post customer complain, detecting service outage or high latency. Many incidents may go undetected.
- Traditionally, troubleshooting and verification of BGP advertisement involves use of ”Looking Glass” and “Route Servers” in different geographical locations.

Route leak dynamics



Source: Detecting Routing Incidents Alexander Azimov Qrator Labs

BGP vulnerabilities

- BGP session hijack
- BGP route leaking
- BGP route hijacking

BGP session hijack

- BGP runs over TCP/179
- Sent in clear-text over TCP, may be hijacked
- Mitigated with the use of TCP Authentication Option (TCP-AO) and Generalized TTL Security Mechanism (GTSM) configured on eBGP peers.
- Limit BGP Control Plane traffic to configured BGP peers only.

BGP route leaking

- Route leak definition (RFC7908):

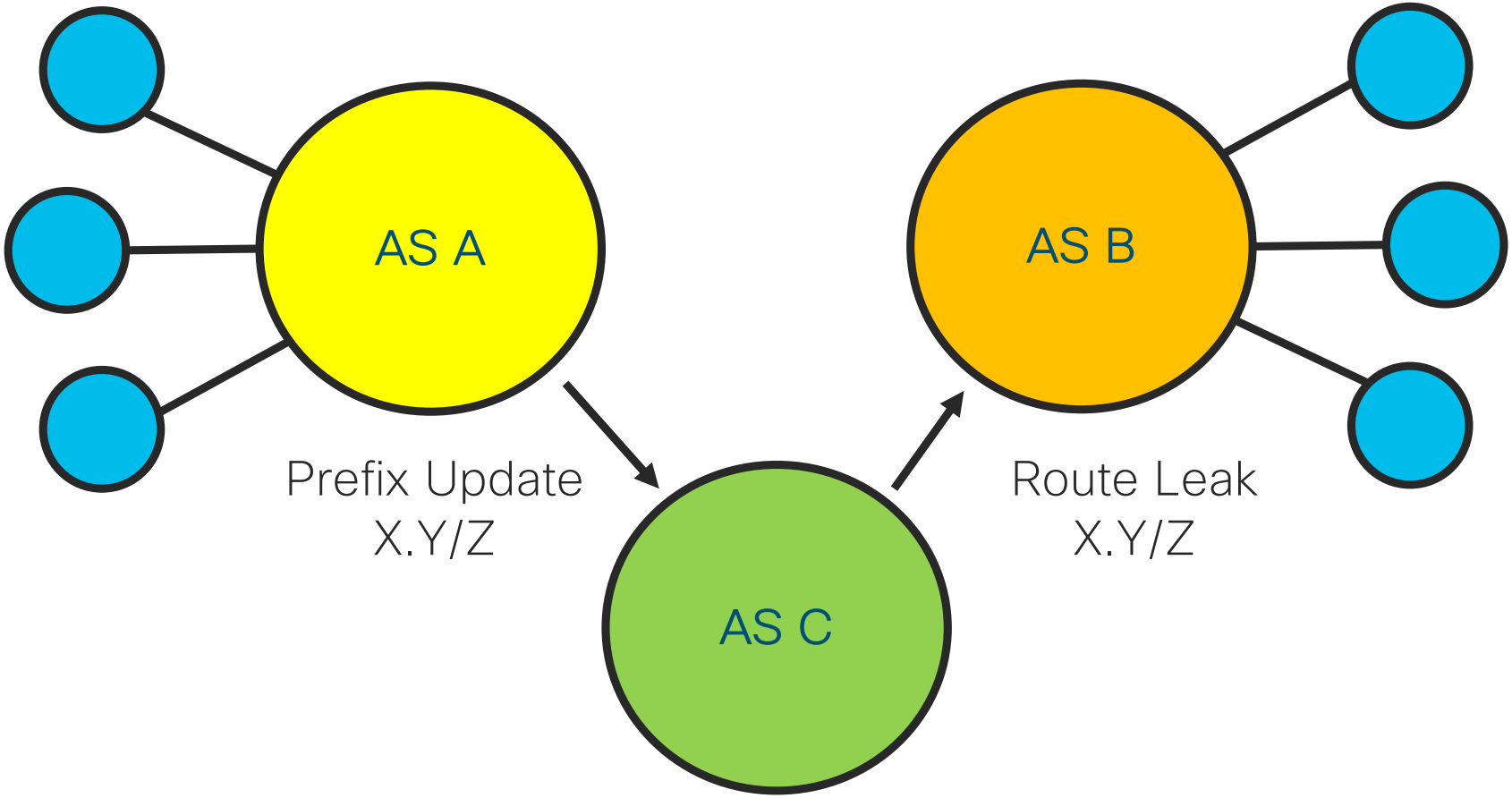
  “A route leak is the propagation of routing announcement(s) beyond their intended scope. That is, an announcement from an Autonomous System (AS) of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, and/or one of the ASes along the preceding AS path”

BGP route leaking

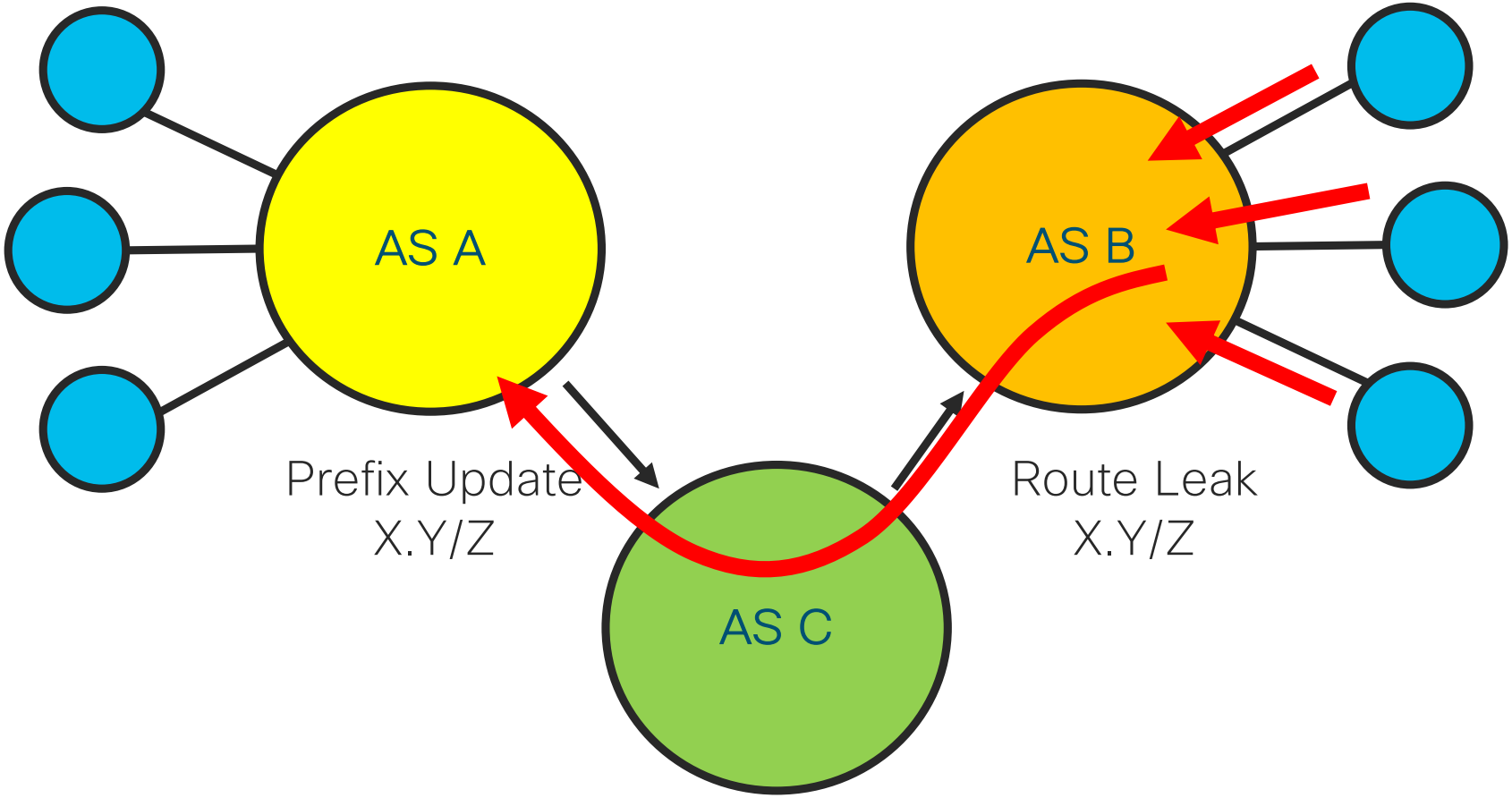
- Consequences of Route leak (RFC7908):

  "The result of a route leak can be redirection of traffic through an unintended path that may enable eavesdropping or traffic analysis and may or may not result in an overload or black hole. Route leaks can be accidental or malicious but most often arise from accidental misconfigurations."

Example: Classic BGP route leak



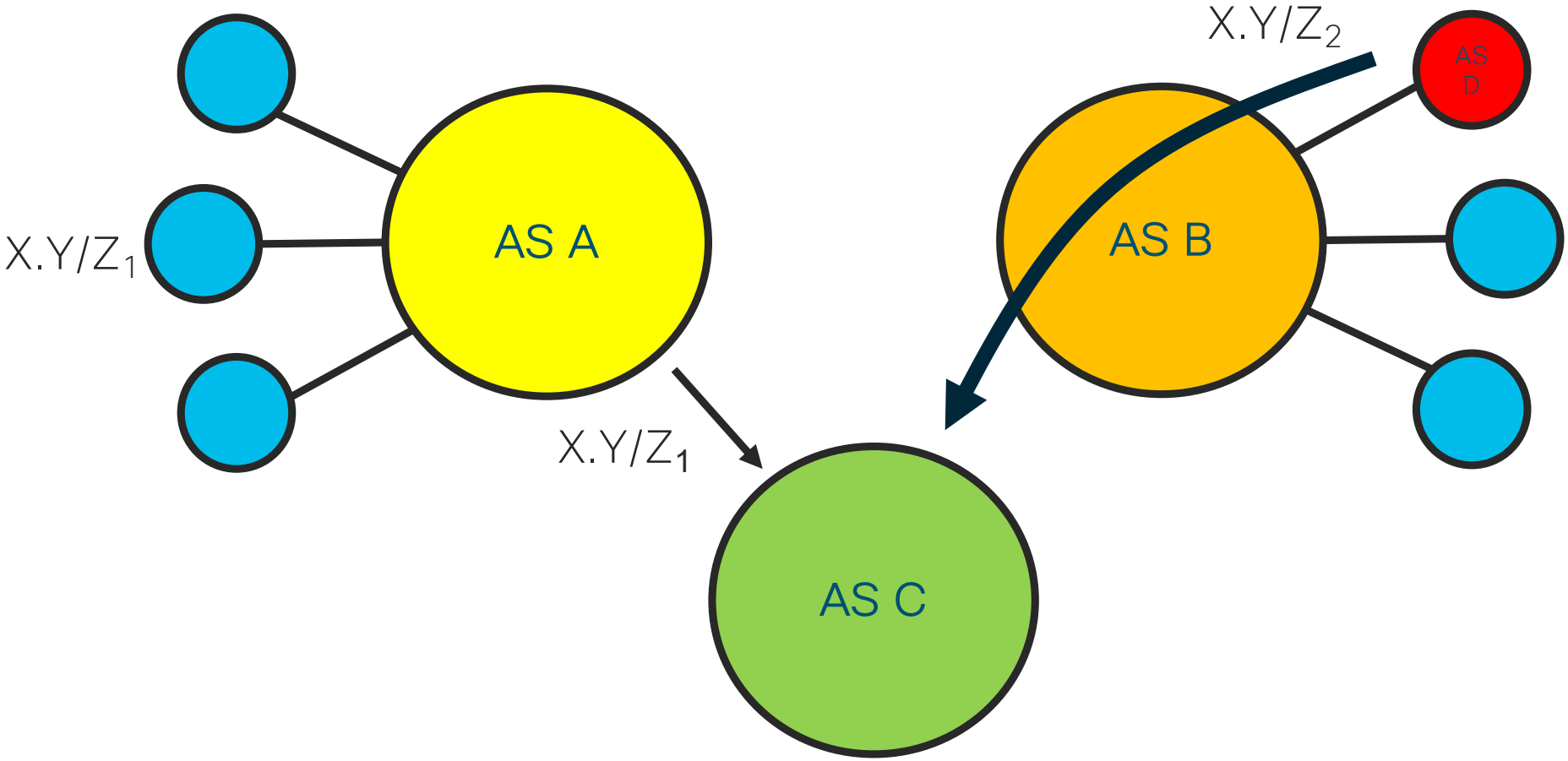
Example: Classic BGP route leak



BGP route hijacking

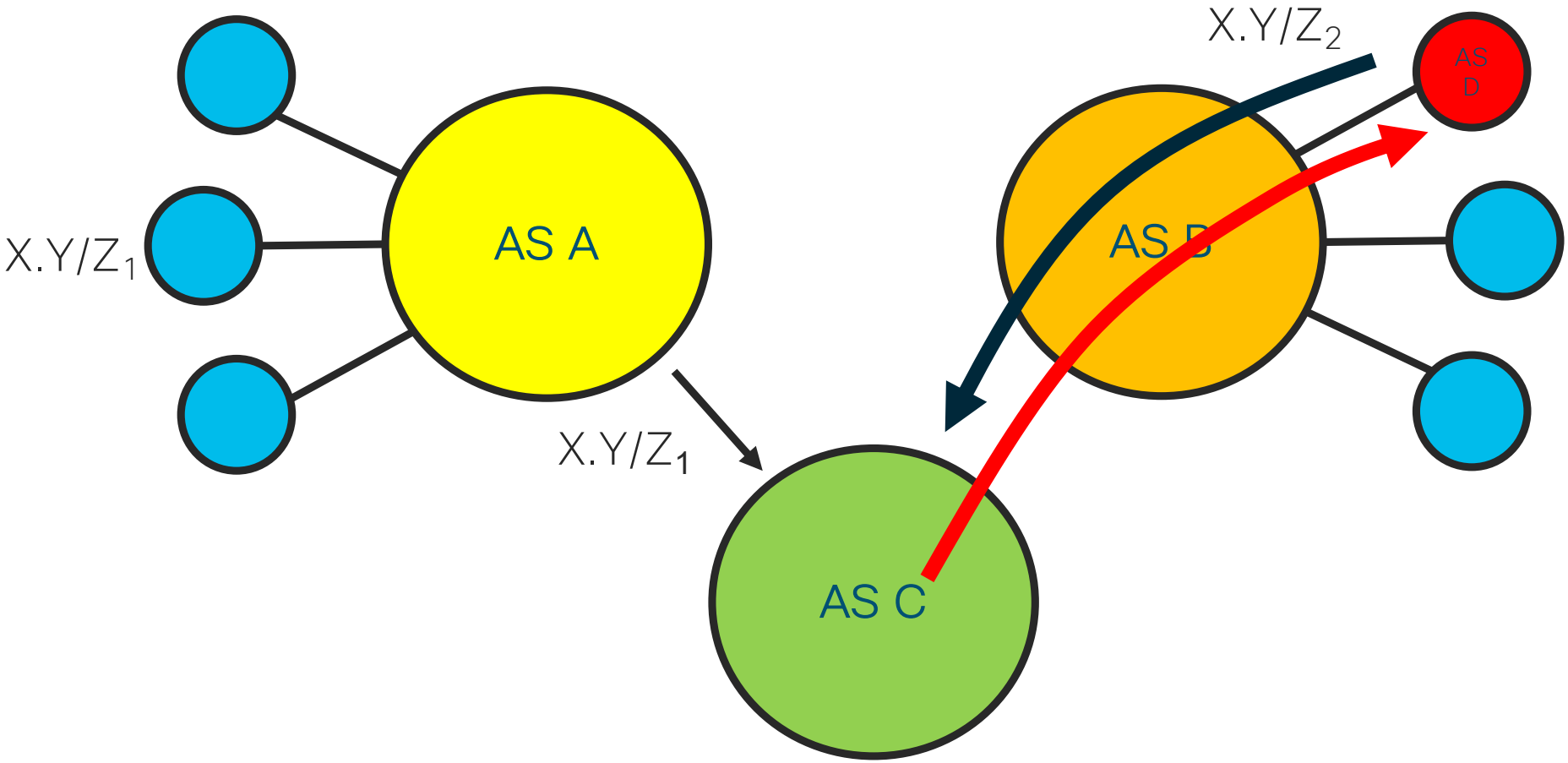
- Maliciously reroute Internet traffic destined towards specific destinations
- Achieved by announcing false ownership of IP prefixes
- Mechanisms are somewhat similar to BGP Route leaking
  - i.e. advertising unauthorized prefixes
- Motivations for BGP hijack
  - Censorship, Denial of service (e.g. traffic back holing)
  - Spam
  - Surveillance, MITM Attack, Phishing
  - etc.

Example: Global BGP route hijacking



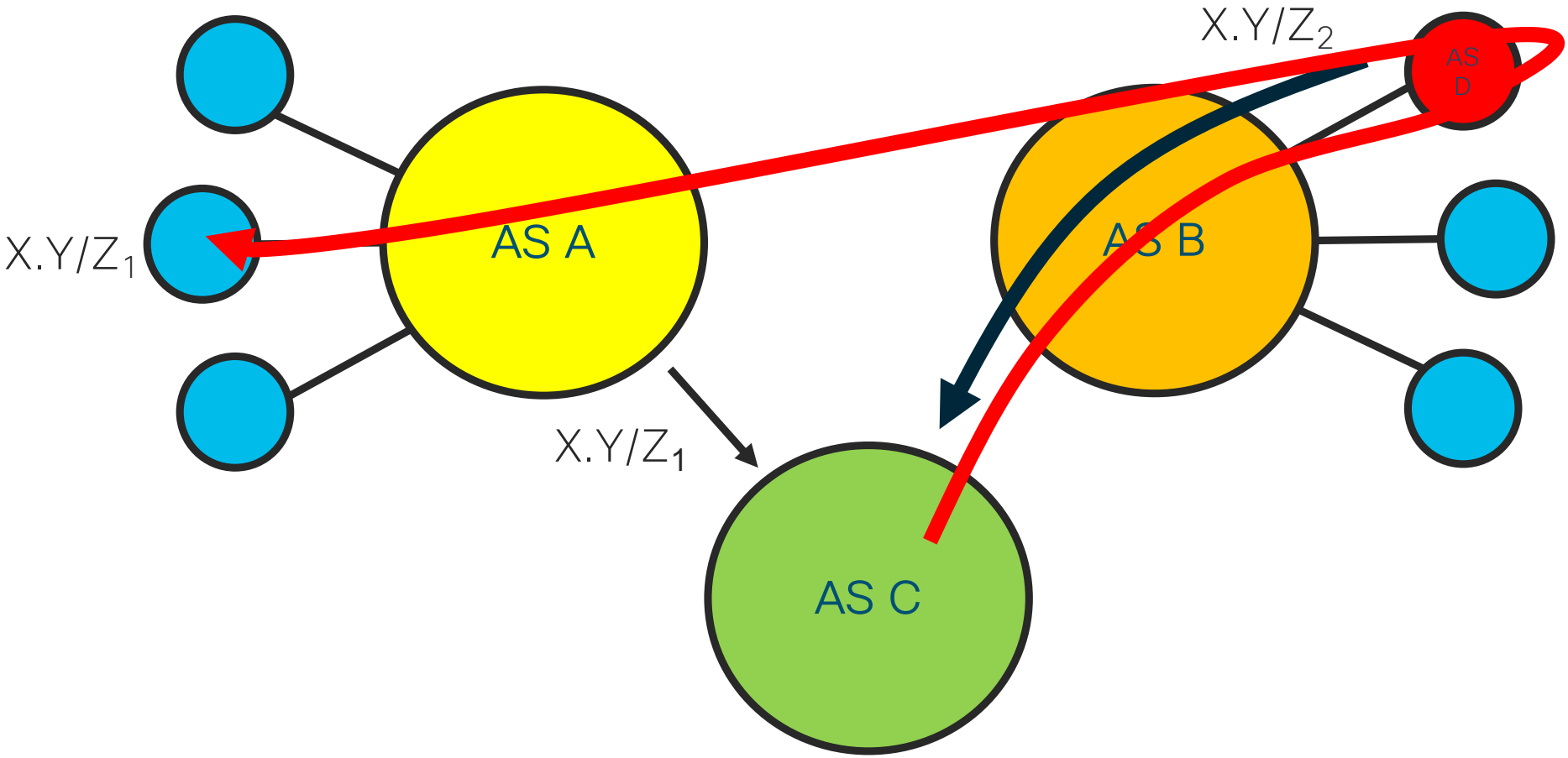
$X.Y/Z_2$ is more specific route than $X.Y/Z_1$

Example: Global BGP hijacking



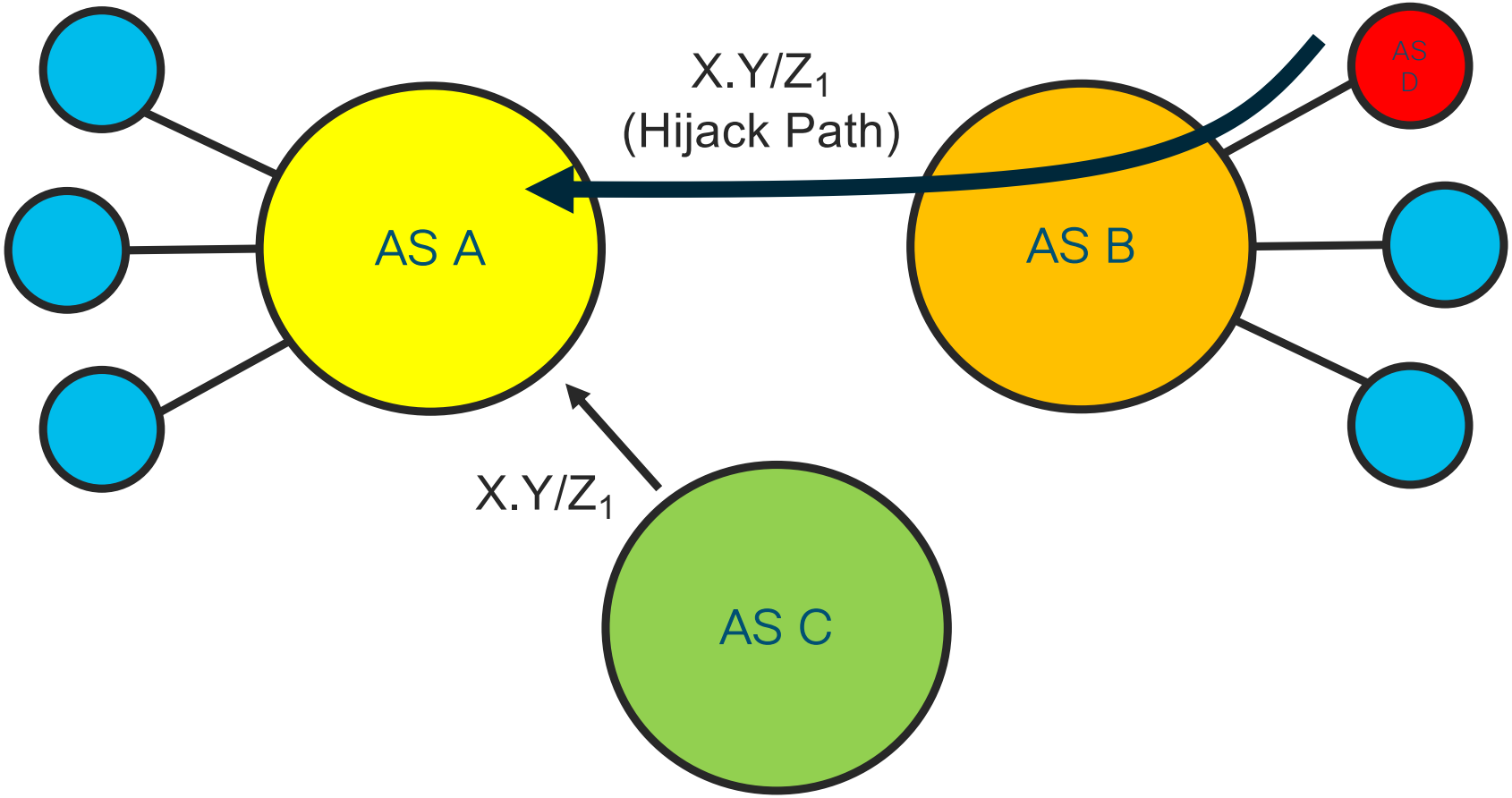
$X.Y/Z_2$ is more specific route than $X.Y/Z_1$

Example: Global BGP hijacking

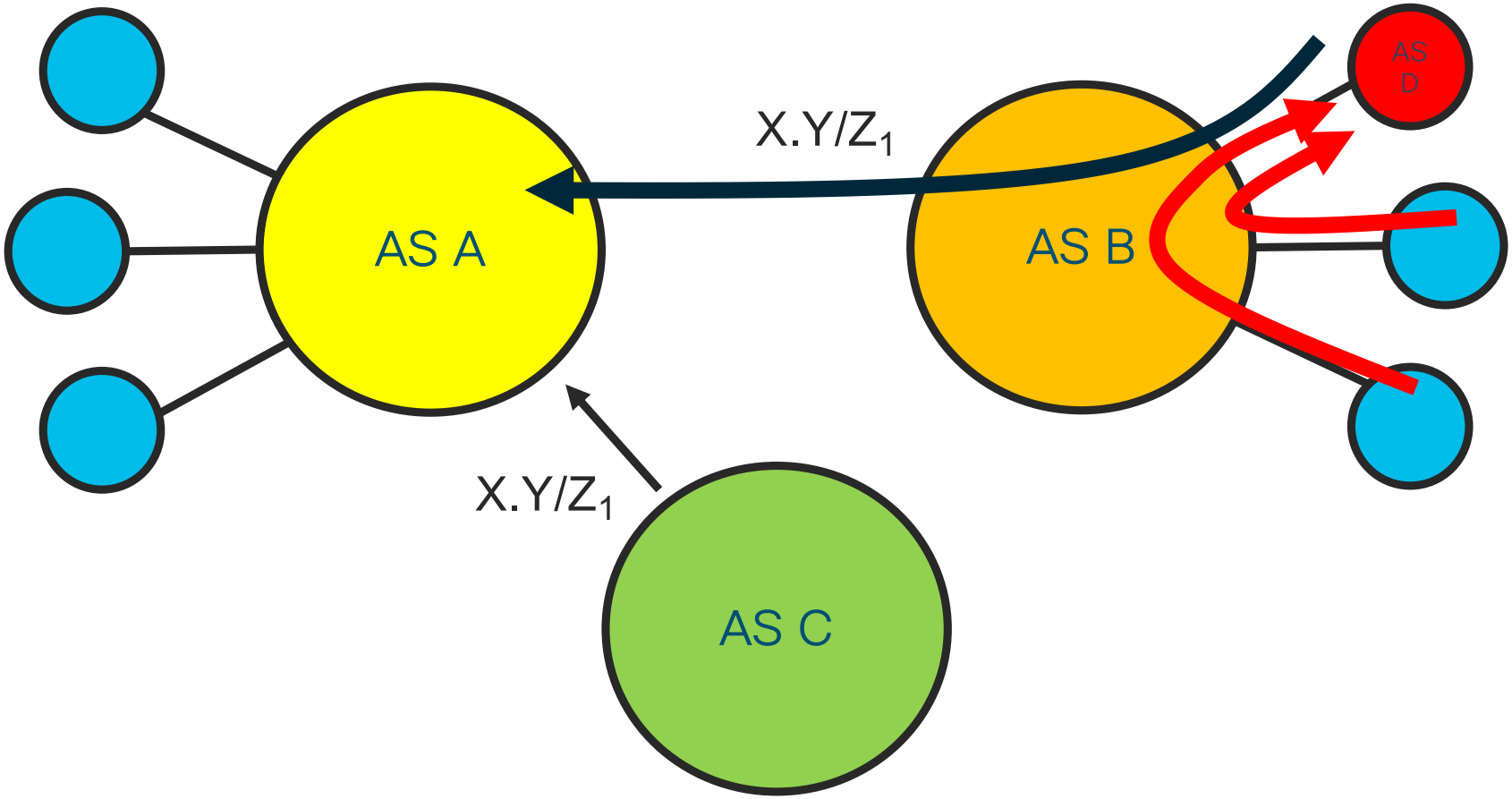


$X.Y/Z_2$ is more specific route than $X.Y/Z_1$

Example: “Local” BGP hijacking

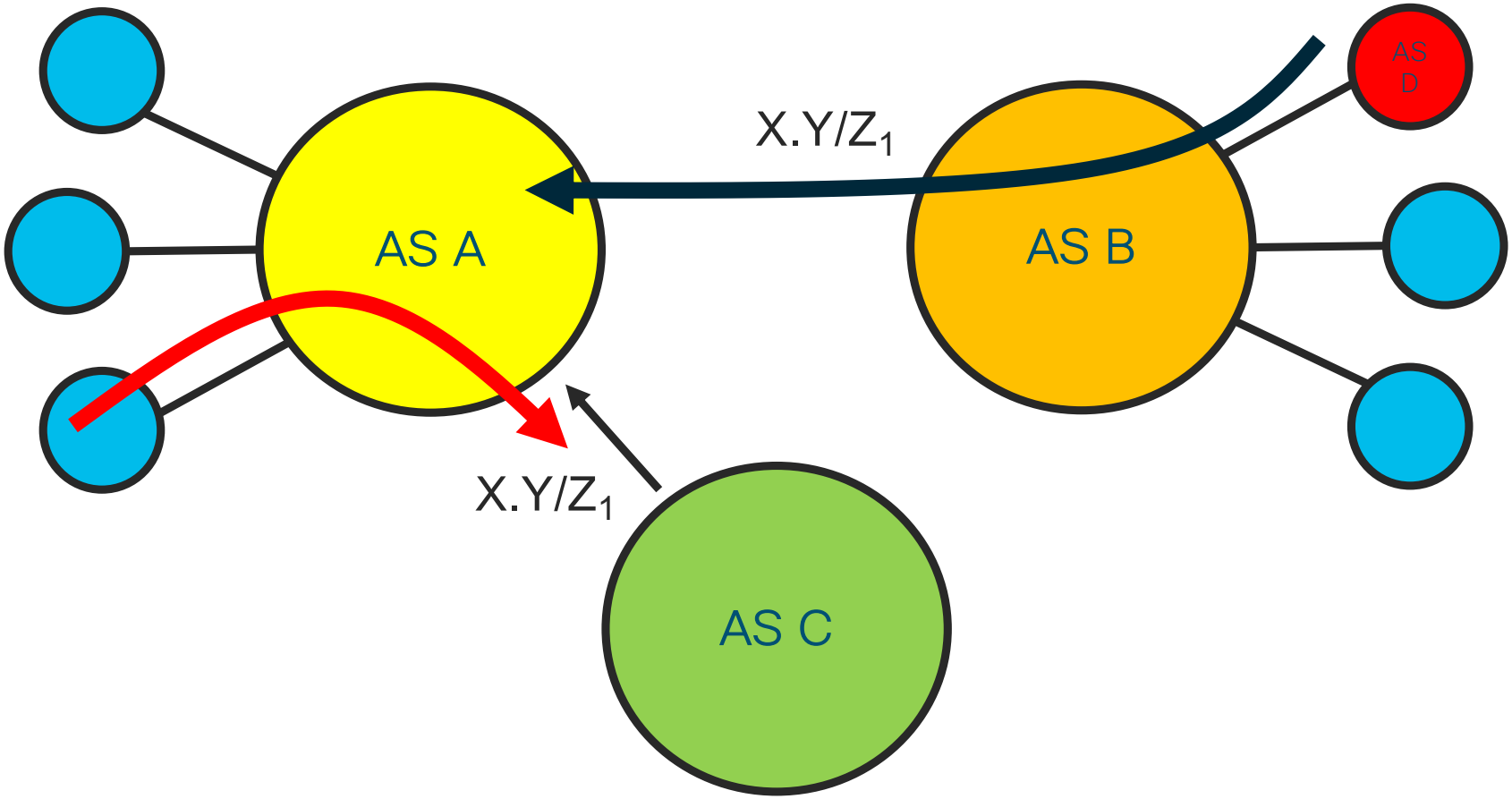


Example: “Local” BGP hijacking



If B is A’s customer, B will prefer D path

Example: “Local” BGP hijacking



If B is A’s provider, A will prefer C path

BGP route hijacking - Detection

Detecting BGP route hijacking:

- Bogus AS path
- AS Origin Change
- Sub Prefix Advertisement
- Change in IP Time-to-Live (TTL)
- Change in Round-Trip-Time (RTT)
- Requires many points of data collection

Layered Approach for Mitigating Route Hijack

- Implement BGP peering BCPs
- Mutually Agreed Norms for Routing Security (MANRS)
  - https://www.manrs.org/isps/
- Implement Route Hijack detection Mechanisms

BGP Peering BCPs

BGP Control Plane:

- Implement Generalized TTL Security Mechanism (GTSM) (RFC5082)
- Implement TCP Authentication Option (TCP-AO)
  - Baseline MD5 and also stronger auth option in IOS-XR 6.5.1
- Control-plane policing per-peer (default in IOS-XR)
- Limit BGP control-plane to only configured peers
- Implement BGP ingress and egress prefix-filtering
- Implement BGP ingress and egress AS-path filtering
- Implement BGP prefix-limit per peer

BGP Peering BCPs

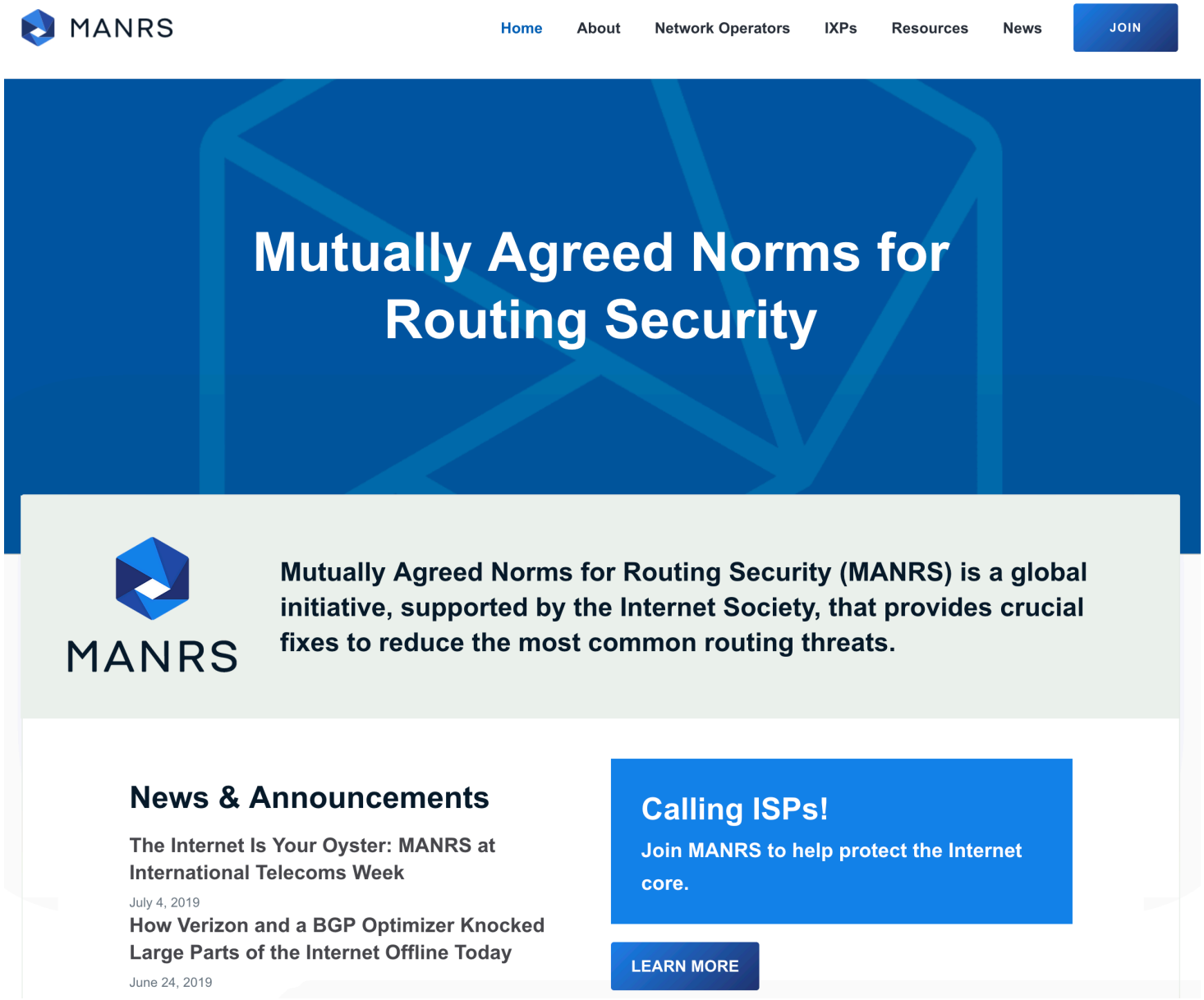
Data Plane:

- Reset QoS Headers (e.g. IP Prec, DSCP, EXP) on inbound traffic
- Ingress and Egress Data-plane filtering
- If feasible, whitelist your own IP space at edge

- Automation is key in maintaining accuracy
- Review BCP 84, 194 and BCP 38 if you are transit service provider

MANRS

- Provides BCOP guidance to ease deployment of measures and is targeted at stub networks and small providers.
- MANRS actions include:
  - Filtering
  - Anti–Spoofing
  - Coordination
  - Global Validation
- Provides Implementation Guidelines for MANRS actions
  - https://www.manrs.org/isps/guide/


MANRS
Home
About
Network Operators
IXPs
Resources
News
JOIN
Mutually Agreed Norms for Routing Security
MANRS
Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.
News & Announcements
The Internet Is Your Oyster: MANRS at International Telecoms Week
July 4, 2019
How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today
June 24, 2019
Calling ISPs!
Join MANRS to help protect the Internet core.
LEARN MORE

Resources

These resources are available to assist in learning more about or becoming compliant with MANRS:

- **Implementation Guide for Network Operators**
  - PDF Version
- **Tutorials**
  - Module 1: Introduction to MANRS
  - Module 2: IRRs, RPKI, and PeeringDB
  - Module 3: Global Validation: Facilitating validation of routing information on a global scale
  - Module 4: Filtering: Preventing propagation of incorrect routing information
  - Module 5: Anti-Spoofing: Preventing traffic with spoofed source IP addresses
  - Module 6: Coordination: Global communication between network operators
- **Papers**
  - Internet Routing with MANRS
  - Routing Security for Policymakers
  - 451 Research MANRS Project Study Report

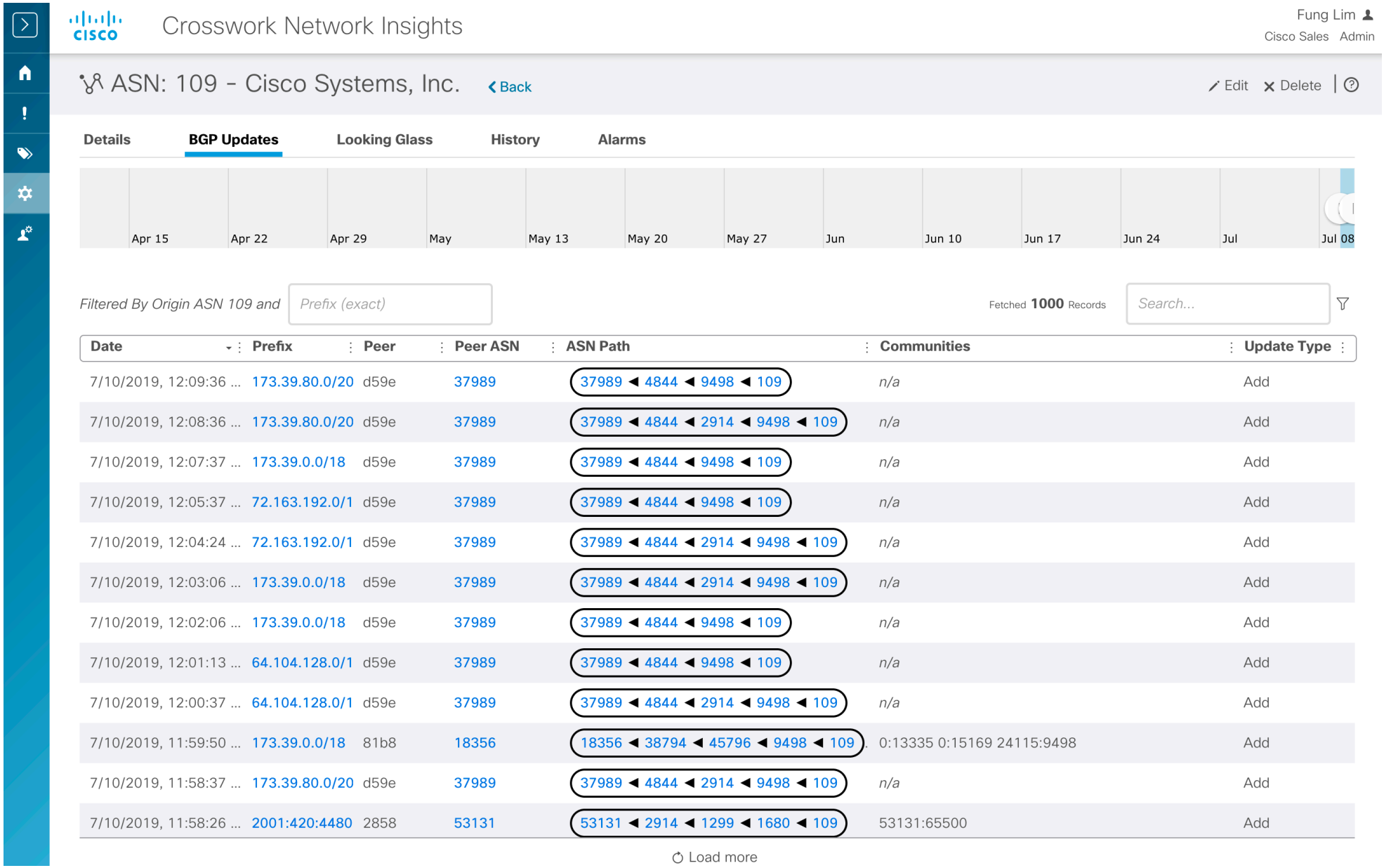
Route Hijack Detection Mechanisms

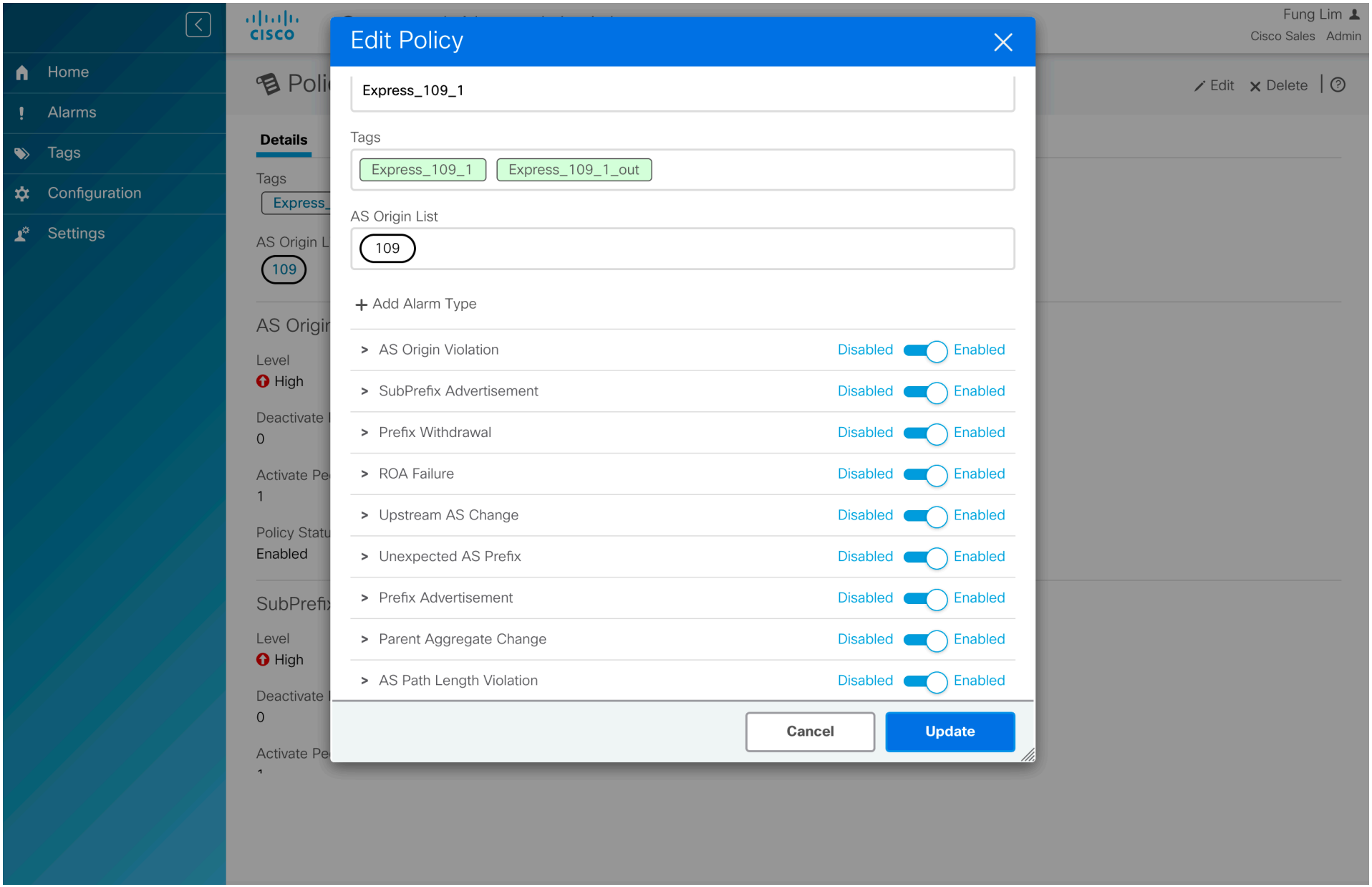
- Various Tools provide alerts, etc. for monitoring prefixes of interest
  - e.g. BGPstream
  - e.g. Cisco Crosswork Network Insights (CCNI) (previous BGPmon)
- Ensure that “interesting” prefixes are watched so that mitigation actions may be applied at the earliest opportunity.

BGPMON Now part of OpenDNS

BGPStream About Contact

Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
BGP Leak		*Origin AS:* TCISL Tata Communications, IN (AS 17908) *Leaker AS:* CHINATELECOM-CORE-WAN-CN2 China Telecom Next Generation Carrier Network, CN (AS 4809)	2019-07-09 12:34:43		More detail
Outage		WIRTEK, IT (AS 201602)	2019-07-09 12:14:00	2019-07-09 12:19:00	More detail
Outage		NET23-AS, HU (AS 30836)	2019-07-09 11:53:00	2019-07-09 11:56:00	More detail
Outage		RADIANT Radiant Communications Limited, BD (AS 38067)	2019-07-09 10:10:00	2019-07-09 10:25:00	More detail
Outage		DNIC-ASBLK-00306-00371 - DoD Network Information Center, US (AS 337)	2019-07-09 10:01:00	2019-07-09 10:05:00	More detail
Outage		DNIC-ASBLK-00306-00371 - DoD Network Information Center, US (AS 337)	2019-07-09 09:32:00	2019-07-09 09:39:00	More detail
Outage		VAD-SRL-AS1, MD (AS 202723)	2019-07-09 09:24:00		More detail
Outage		Super Cabo TV Caratinga Ltda, BR (AS 53050)	2019-07-09 08:59:00	2019-07-09 12:37:00	More detail


Crosswork Network Insights
Fung Lim
Cisco Sales Admin
ASN: 109 - Cisco Systems, Inc.
Back
Edit
Delete
Details
BGP Updates
Looking Glass
History
Alarms
Apr 15
Apr 22
Apr 29
May
May 13
May 20
May 27
Jun
Jun 10
Jun 17
Jun 24
Jul
Jul 08
Filtered By Origin ASN 109 and
Prefix (exact)
Fetched 1000 Records
Search...
Date
Prefix
Peer
Peer ASN
ASN Path
Communities
Update Type
7/10/2019, 12:09:36 ... 173.39.80.0/20 d59e 37989 37989 ◀ 4844 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:08:36 ... 173.39.80.0/20 d59e 37989 37989 ◀ 4844 ◀ 2914 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:07:37 ... 173.39.0.0/18 d59e 37989 37989 ◀ 4844 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:05:37 ... 72.163.192.0/1 d59e 37989 37989 ◀ 4844 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:04:24 ... 72.163.192.0/1 d59e 37989 37989 ◀ 4844 ◀ 2914 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:03:06 ... 173.39.0.0/18 d59e 37989 37989 ◀ 4844 ◀ 2914 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:02:06 ... 173.39.0.0/18 d59e 37989 37989 ◀ 4844 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:01:13 ... 64.104.128.0/1 d59e 37989 37989 ◀ 4844 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 12:00:37 ... 64.104.128.0/1 d59e 37989 37989 ◀ 4844 ◀ 2914 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 11:59:50 ... 173.39.0.0/18 81b8 18356 18356 ◀ 38794 ◀ 45796 ◀ 9498 ◀ 109 0:13335 0:15169 24115:9498 Add
7/10/2019, 11:58:37 ... 173.39.80.0/20 d59e 37989 37989 ◀ 4844 ◀ 2914 ◀ 9498 ◀ 109 n/a Add
7/10/2019, 11:58:26 ... 2001:420:4480 2858 53131 53131 ◀ 2914 ◀ 1299 ◀ 1680 ◀ 109 53131:65500 Add
Load more


Home
Alarms
Tags
Configuration
Settings
Fung Lim
Cisco Sales Admin
Edit
Delete
Details
Edit Policy
Express_109_1
Tags
Express_109_1
Express_109_1_out
AS Origin List
109
+ Add Alarm Type
> AS Origin Violation Disabled Enabled
> SubPrefix Advertisement Disabled Enabled
> Prefix Withdrawal Disabled Enabled
> ROA Failure Disabled Enabled
> Upstream AS Change Disabled Enabled
> Unexpected AS Prefix Disabled Enabled
> Prefix Advertisement Disabled Enabled
> Parent Aggregate Change Disabled Enabled
> AS Path Length Violation Disabled Enabled
Cancel
Update

Useful Tools/Resources

- MANRS
  - https://www.manrs.org/
- Service Provider Security Best Practices
  - http://www.cisco.com/security/sp
- SENKI
  - https://www.senki.org/
- BGPStream
  - https://bgpstream.com/

Thank you!


CISCO