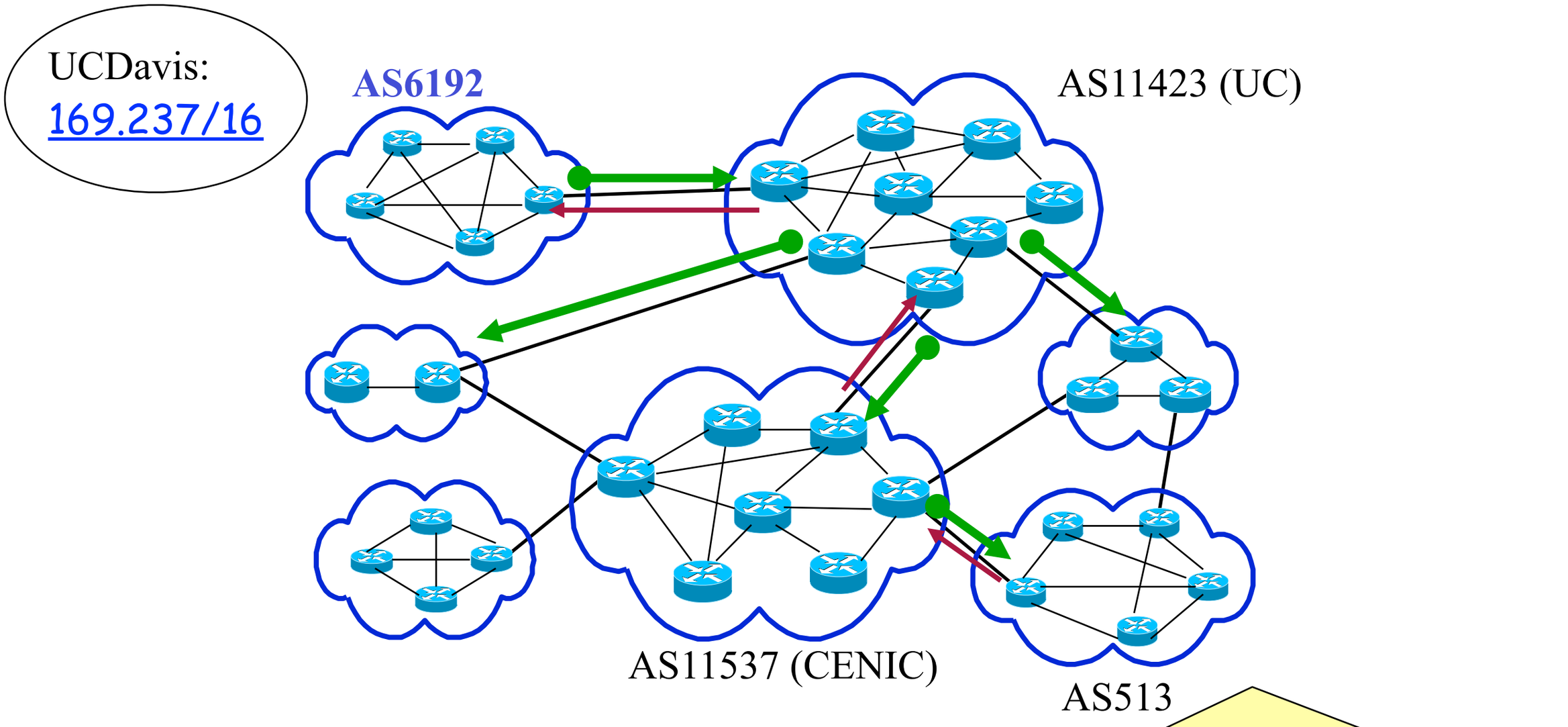
CE 817 - Advanced Network Security
Routing Security II

Lecture 21

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

Autonomous Systems (ASes)



an AS Path:

169.237/16 513→11537→11423→ 6192

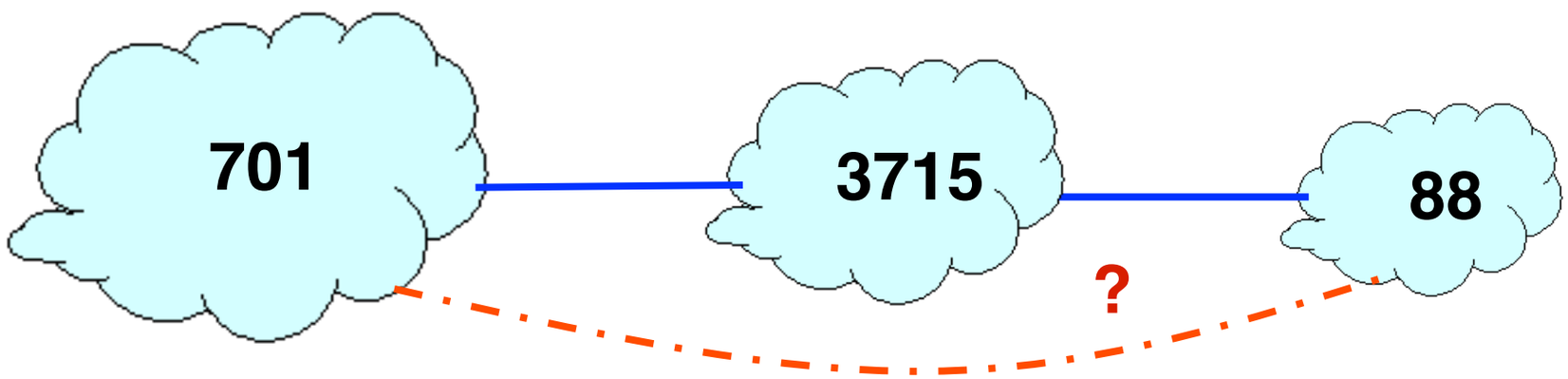
BGP Advertisement

- Given AS only advertises routes it considers good enough for itself
  - If there are multiple routes to the destination, it would choose the best one based on local policy
  - No obligation to advertise routes it does not like
    - This is how an AS implements a no transit policy

BGP AS Path

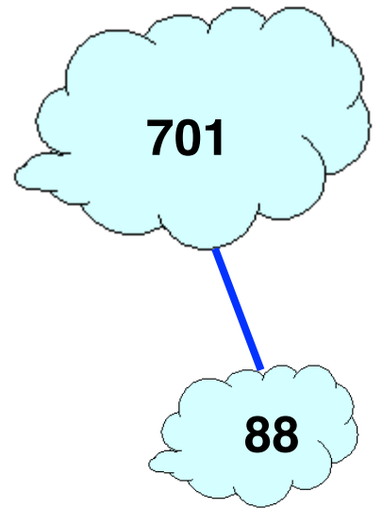
Bogus AS Paths

- Remove ASes from the AS path
  - E.g., turn “701 -> 3715 -> 88” into “701 -> 88”
- Motivations
  - Make the AS path look shorter than it is
  - Attract sources that normally try to avoid AS 3715
  - Help AS 88 look like it is closer to the Internet’s core
- Who can tell that this AS path is a lie?
  - Maybe AS 88 *does* connect to AS 701 directly



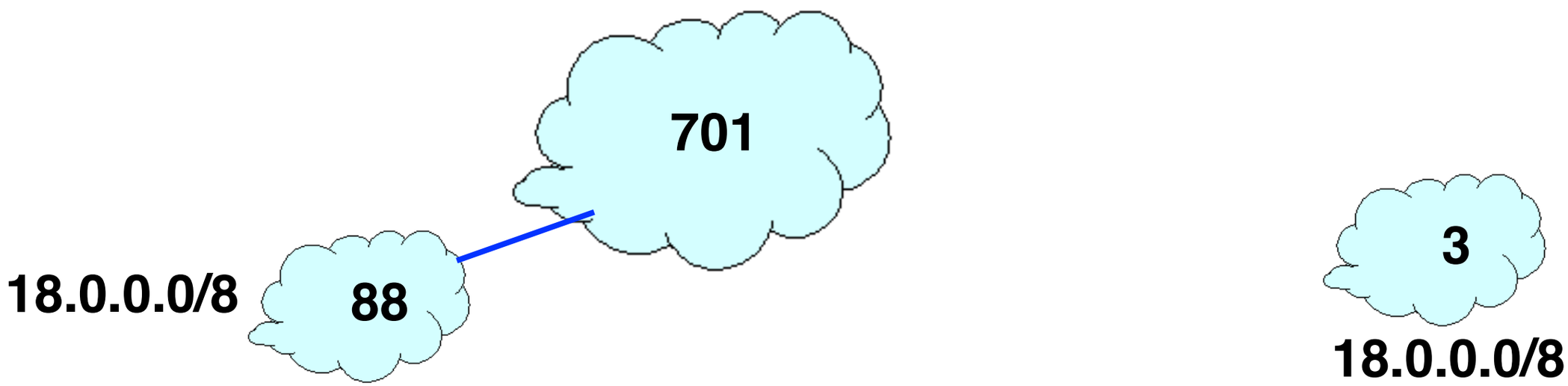
Bogus AS Paths

- Add ASes to the path
  - E.g., turn “701 88” into “701 3715 88”
- Motivations
  - Trigger loop detection in AS 3715
    - Denial-of-service attack on AS 3715
    - Or, blocking unwanted traffic coming from AS 3715!
  - Make your AS look like it has richer connectivity
- Who can tell the AS path is a lie?
  - AS 3715 could, if it verifying the path
  - AS 88 could, but would it really care as long as it received data traffic meant for it?



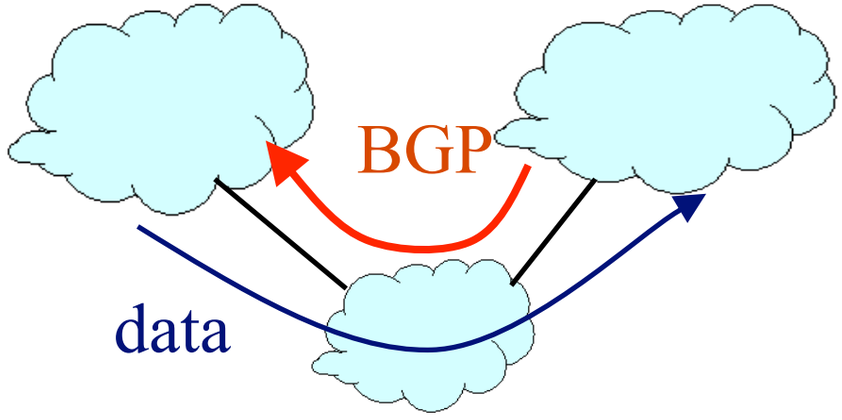
Bogus AS Paths

- Adds AS hop(s) at the end of the path
  - E.g., turns “701 88” into “701 88 3”
- Motivations
  - Evade detection for a bogus route
  - E.g., by adding the legitimate AS to the end
- Hard to tell that the AS path is bogus…
  - Even if other ASes filter based on prefix ownership



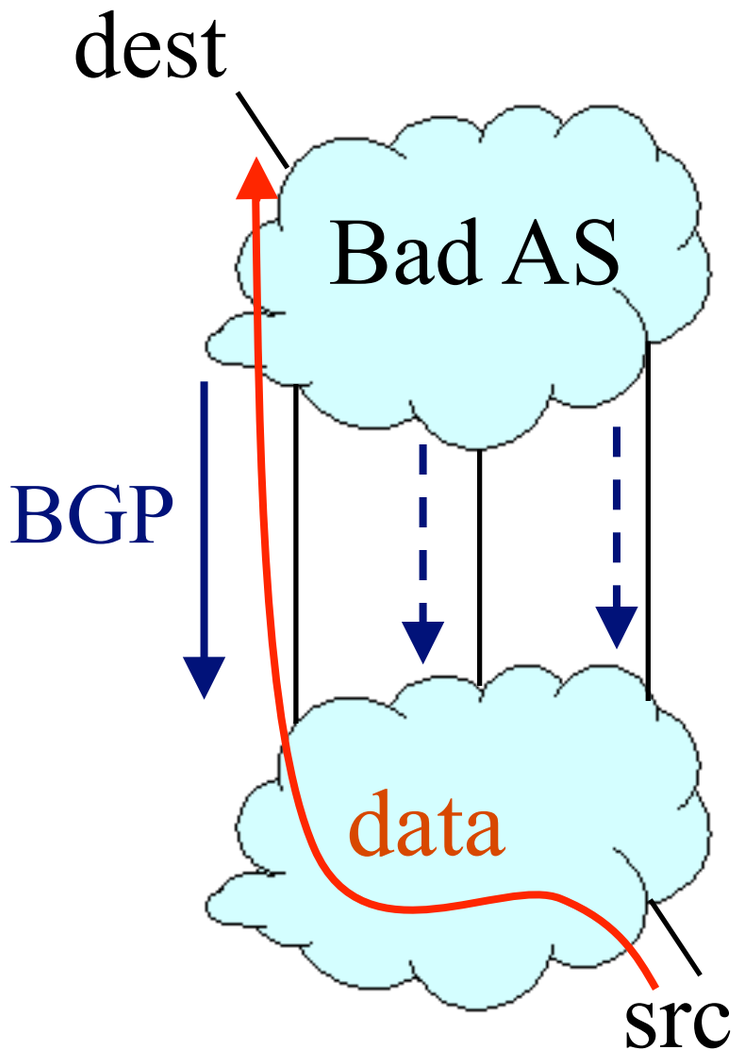
Invalid Paths

- AS exports a route it shouldn’t
  - AS path is a valid sequence, but violated policy
- Example: customer misconfiguration
  - Exports routes from one provider to another
- … interacts with provider policy
  - Provider prefers customer routes
  - … so picks these as the best route
- … leading the dire consequences
  - Directing all Internet traffic through customer
- Main defense
  - Filtering routes based on prefixes and AS path



Missing/Inconsistent Routes

- Peers require consistent export
  - Prefix advertised at all peering points
  - Prefix advertised with same AS path length
- Reasons for violating the policy
  - Trick neighbor into “cold potato”
  - Configuration mistake
- Main defense
  - Analyzing BGP updates
  - … or data traffic
  - … for signs of inconsistency



BGP Security Today

- Applying best common practices (BCPs)
  - Securing the session (authentication, encryption)
  - Filtering routes by prefix and AS path
  - Packet filters to block unexpected control traffic
- This is not good enough
  - Depends on vigilant application of BCPs
    - … and not making configuration mistakes!
  - Doesn’t address fundamental problems
    - Can’t tell who owns the 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

Proposed Enhancements to BGP

S-BGP Secure Version of BGP

- Address attestations
  - Claim the right to originate a prefix
  - Signed and distributed out-of-band
  - Checked through delegation chain from ICANN
- Route attestations
  - Distributed as an attribute in BGP update message
  - Signed by each AS as route traverses the network
  - Signature signs previously attached signatures
- S-BGP can validate
  - AS path indicates the order ASes were traversed
  - No intermediate ASes were added or removed

S-BGP Deployment Challenges

- Complete, accurate registries
  - E.g., of prefix ownership
- Public Key Infrastructure
  - To know the public key for any given AS
- Cryptographic operations
  - E.g., digital signatures on BGP messages
- Need to perform operations quickly
  - To avoid delaying response to routing changes
- Difficulty of incremental deployment
  - Hard to have a “holiday” to deploy S-BGP

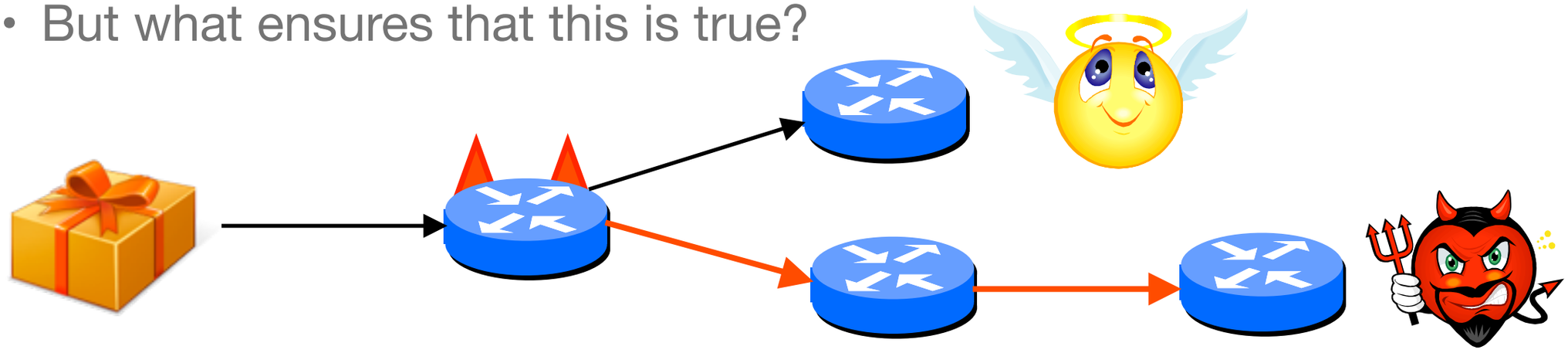
Incrementally Deployable Schemes

- Monitoring BGP update messages
  - Use past history as an implicit registry
  - E.g., AS that announces each address block
  - E.g., AS-level edges and paths
- Out-of-band detection mechanism
  - Generate reports and alerts
  - Internet Alert Registry: http://iar.cs.unm.edu/
  - Prefix Hijack Alert System: http://phas.netsec.colostate.edu/
- Soft response to suspicious routes
  - Prefer routes that agree with the past
  - Delay adoption of unfamiliar routes when possible
  - Some (e.g., misconfiguration) will disappear on their own

What About Packet Forwarding?

Control Plane Vs. Data Plane

- Control plane
  - BGP is a routing protocol
  - BGP security concerns validity of routing messages
  - I.e., did the BGP message follow the sequence of ASes listed in the AS-path attribute
- Data plane
  - Routers forward data packets
  - Supposedly along the path chosen in the control plane
  - But what ensures that this is true?



Data-Plane Attacks, Part 1

- Drop packets in the data plane
  - While still sending the routing announcements
- Easier to evade detection
  - Especially if you only drop some packets
  - Like, oh, say, BitTorrent or Skype traffic
- Even easier if you just slow down some traffic
  - How different are normal congestion and an attack?
  - Especially if you let ping/traceroute packets through?

Data-Plane Attacks, Part 2

- Send packets in a different direction
  - Disagreeing with the routing announcements
- Direct packets to a different destination
  - E.g., one the adversary controls
- What to do at that bogus destination?
  - Impersonate the legitimate destination (e.g., to perform identity theft, or promulgate false information)
  - Snoop on the traffic and forward along to real destination
- How to detect?
  - Traceroute? Longer than usual delays?
  - End-to-end checks, like site certificate or encryption?

Fortunately, Data-Plane Attacks are Harder

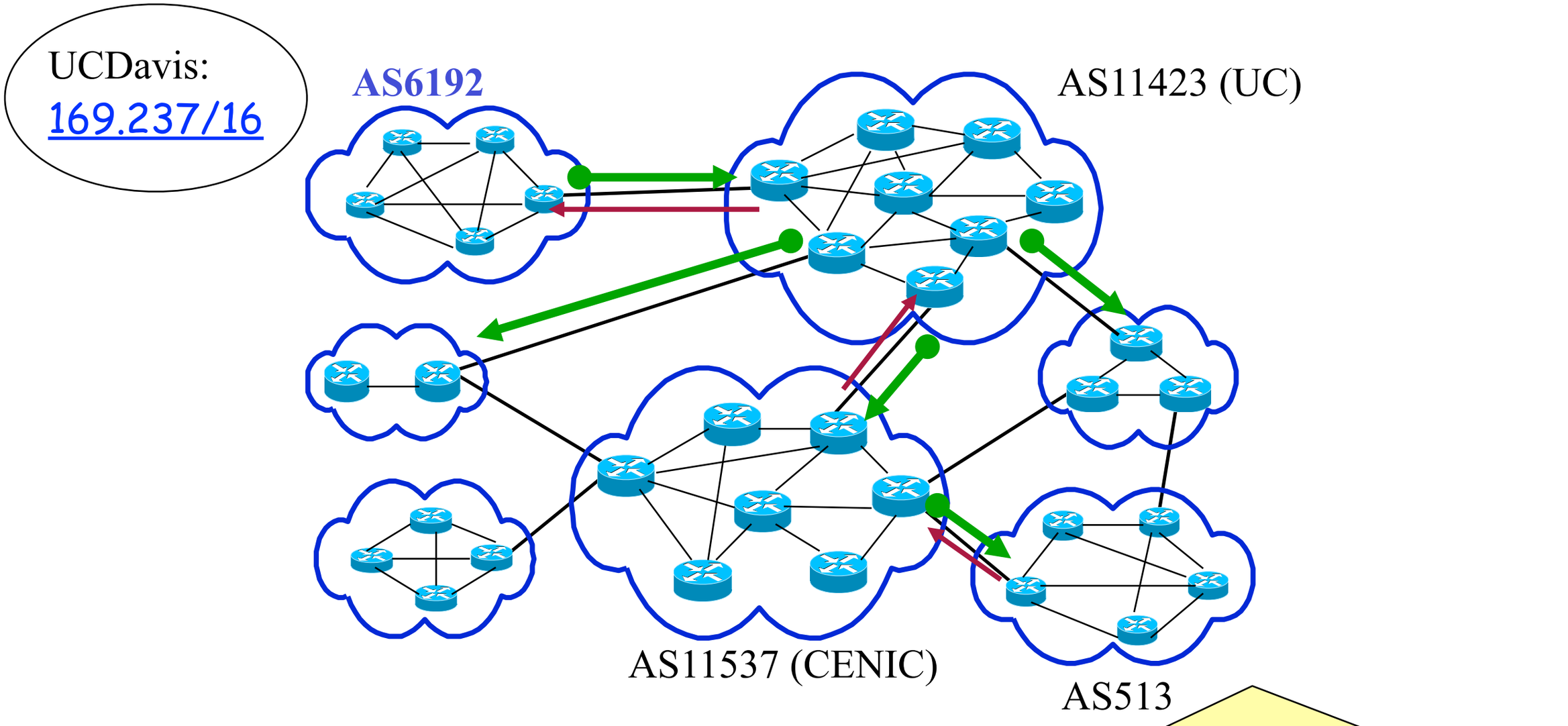
- Adversary must control a router along the path
  - So that the traffic flows through him
- How to get control a router
  - Buy access to a compromised router online
  - Guess the password
  - Exploit known router vulnerabilities
  - Insider attack (disgruntled network operator)
- Malice vs. greed
  - Malice: gain control of someone else's router
  - Greed: Verizon DSL blocks Skype to gently encourage me to pick up my landline phone to use Verizon long distance $ervice

Visual-based Anomaly Detection for BGP Origin AS Change (OASC) Events, Soon-Tee Teoh, Kwan-Liu Ma, S. Felix Wu, Dan Massey, Xiao-Liang Zhao, Dan Pei, Lan Wang, Lixia Zhang, Randy Bush, DSOM 2003.

Elisha: the long-term goal

- Monitoring and management of a large-scale complex system that we do not fully understand its behavior.
- Integration of human and machine intelligence to adaptively develop the domain knowledge for the target system.
- Knowledge Acquisition via Visualization
  - cognitive pattern matching
  - event correlation and explanation
- Elisha: open source available
  - http://www.cs.ucdavis.edu/~wu/Elisha/
  - Linux/Windows

Autonomous Systems (ASes)

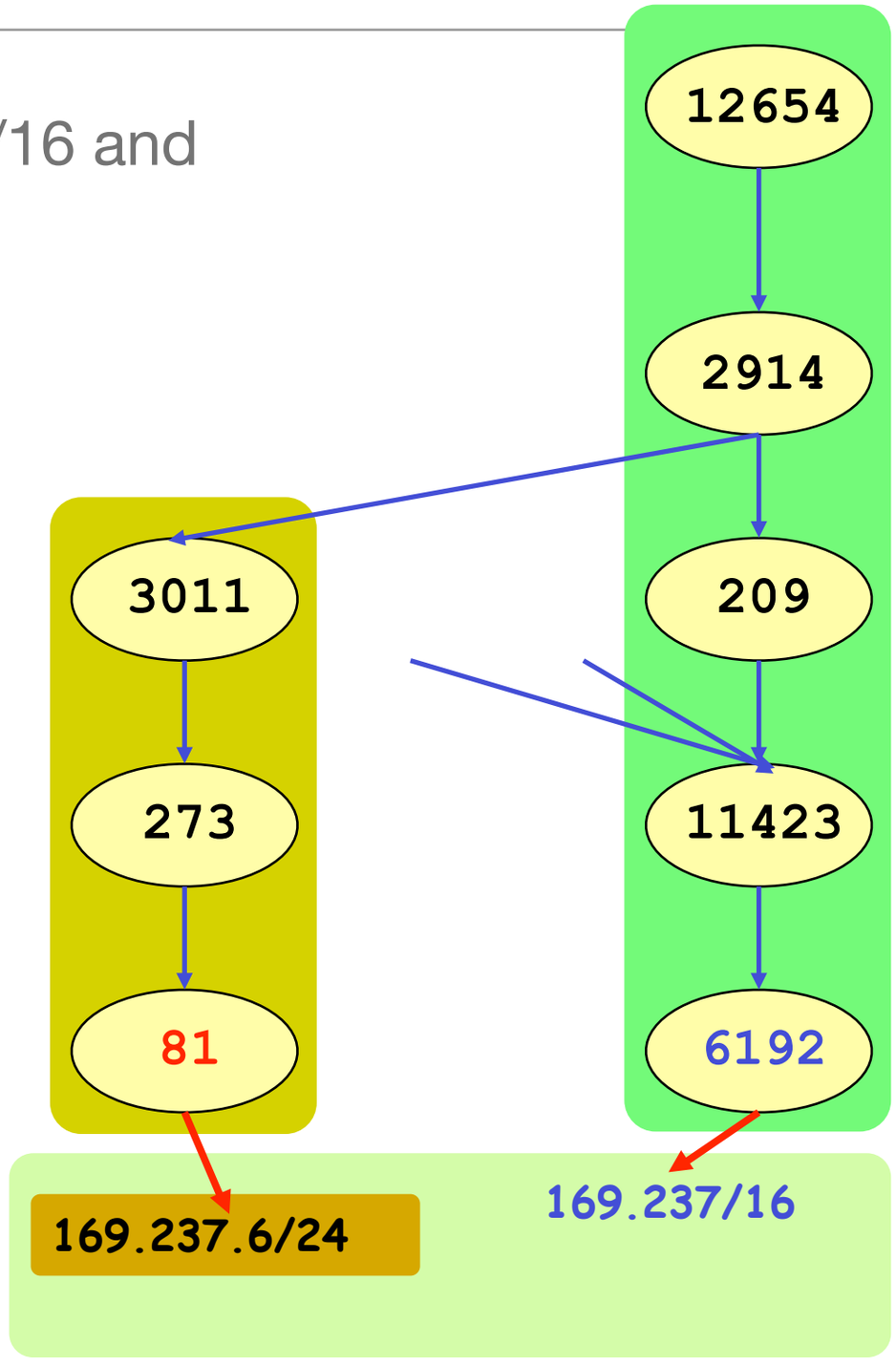


Origin AS in an AS Path

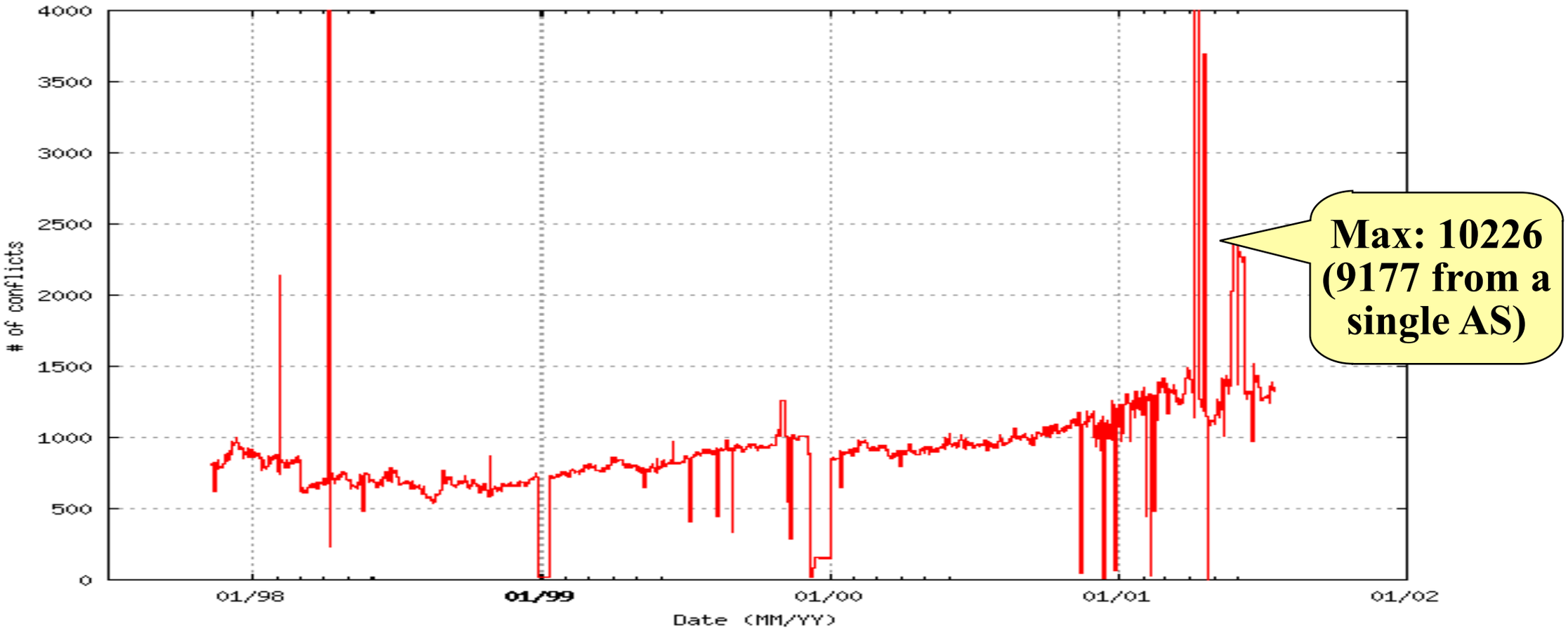
- UCDavis (AS-6192) owns 169.237/16 and AS-6192 is the origin AS
- AS Path: 513-> 11537 -> 11423 -> 6192
  - **12654 13129 6461 3356 11423 6192**
  - **12654 9177 3320 209 11423 6192**
  - **12654 4608 1221 4637 11423 6192**
  - **12654 777 2497 209 11423 6192**
  - **12654 3257 3356 11423 6192**
  - **12654 1103 11537 11423 6192**
  - **12654 3333 3356 11423 6192**
  - **12654 7018 209 11423 6192**
  - **12654 2914 209 11423 6192**
  - **12654 3549 209 11423 6192**

Origin AS Changes (OASC)

- Ownership: UCDavis (AS-6192) owns 169.237/16 and AS-6192 is the origin AS
- Current
  - AS Path: 2914 -> 209 -> 11423 -> 6192
  - for prefix: 169.237/16
- New
  - AS Path: 2914 -> 3011 -> 273 -> 81
  - for prefix: 169.237.6/24
  - Punching a hole on the address space
- Which route path to use?
- Legitimate or not??



BGP OASC Events



year	Median number	increase rate	#BGP table entries	increase rate
1998	683		52000	
1999	810.5	18.7%	60000	15.40%
2000	951	17.3%	80000	33.30%
2001	1294	34.8%	109000	36%

Data

- Oregon Route Views data
  - Peering with 54 BGP routers and 43 different ASes
- Overall 38225 OASC events observed
  - Over 1279 days

Visual-based Anomaly Detection

- “Visual” Anomalies
  - Something catches your eyes…

- Mental/Cognitive “long-term” profile or normal behavior
  - We build the “long-term” profile in your mind.
  - Human experts can incorporate “domain knowledge” about the target system/protocol.

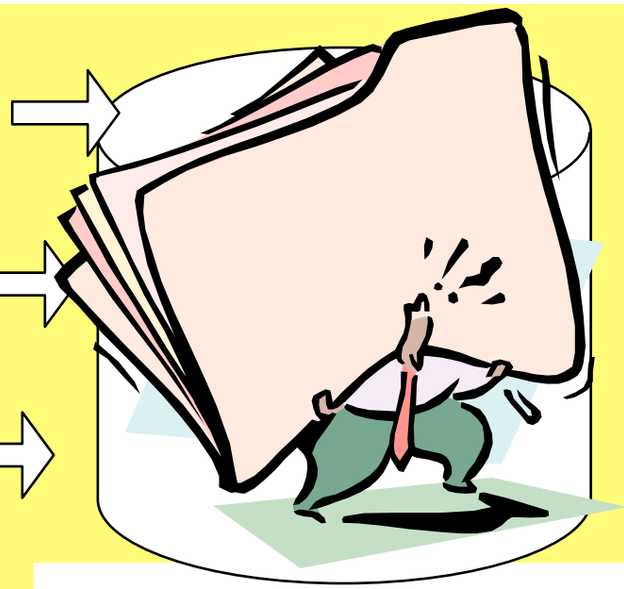
Visual-based Anomaly Detection

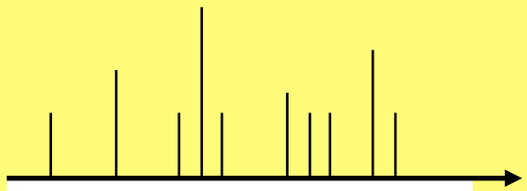
Information Visualization Toolkit

update

decay

clean



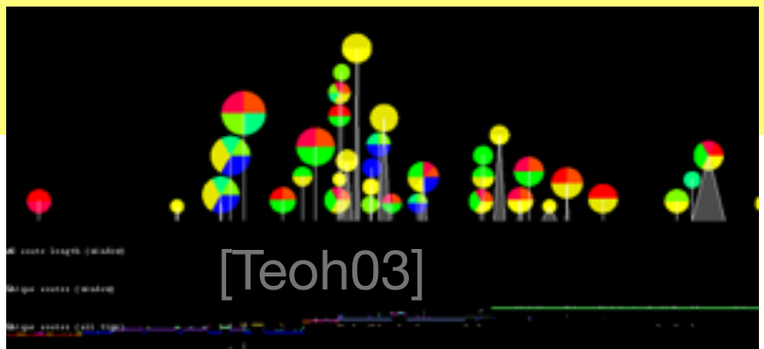


raw events

cognitive profile

cognitively identify the deviation

alarm identification



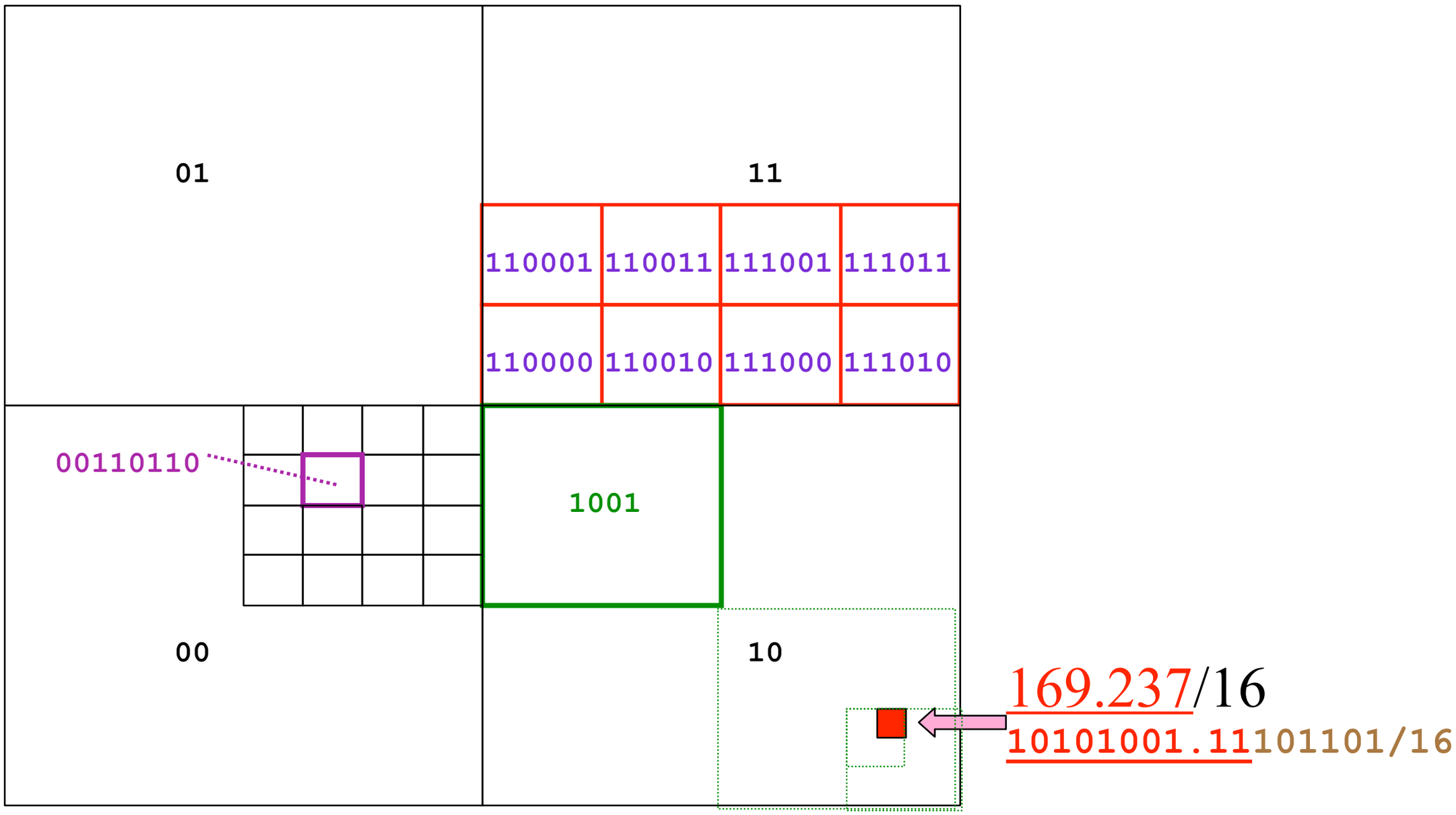
[Teoh03]

ELISHA/OASC

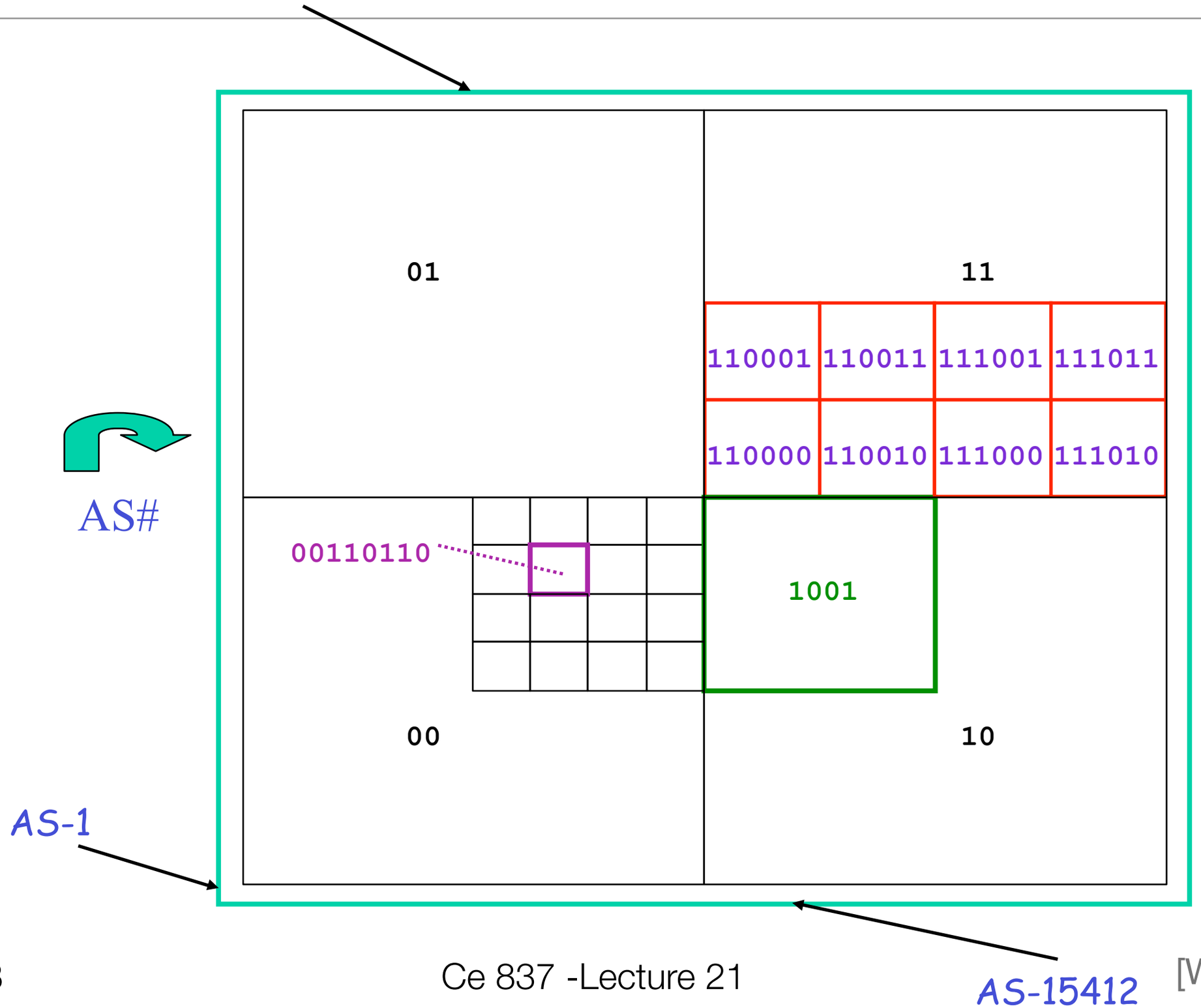
- Events:
  - Low level events: BGP Route Updates
  - High level events: OASC
    - Still 1000+ per day and max 10226 per day for the whole Internet

- Information to represent visually:
  - IP address blocks
  - Origin AS in BGP Update Messages
  - Different Types of OASC Events

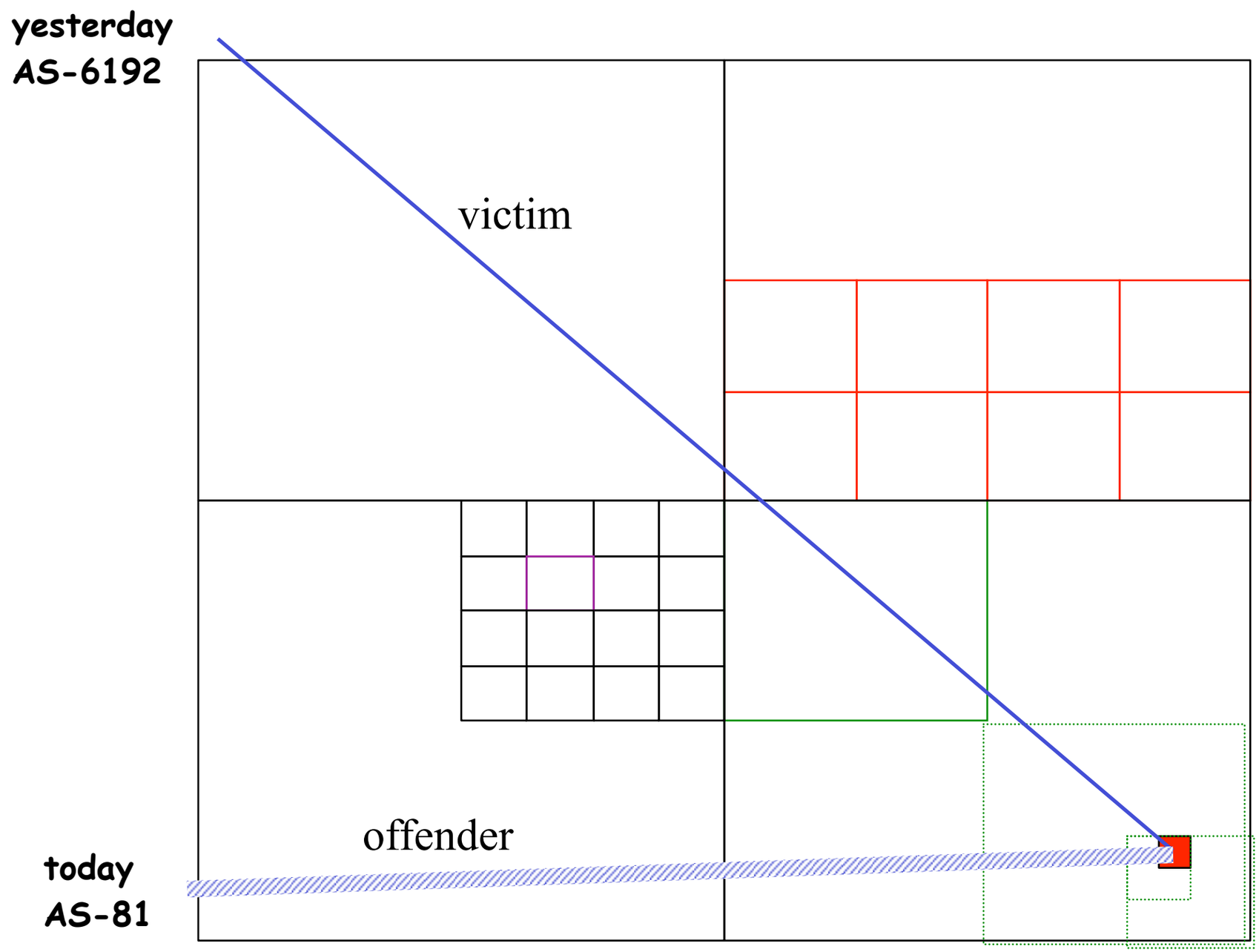
Quad-Tree Representation of IP Address Prefixes



AS# Representation



AS81 punched a “hole” on 169.237/16

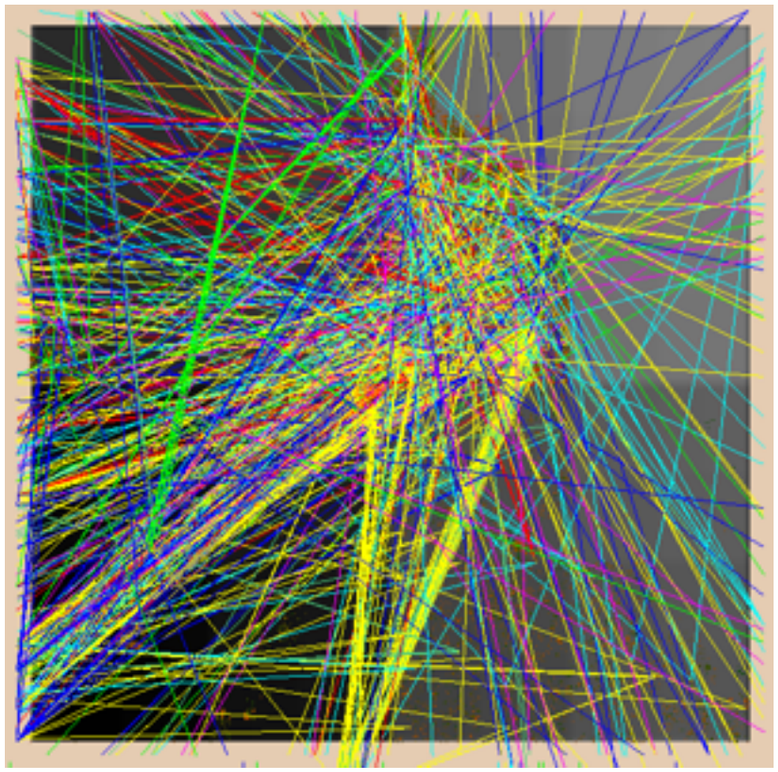


yesterday
169.237/16

today
169.237/16
169.237.6/24

8 OASC Event Types

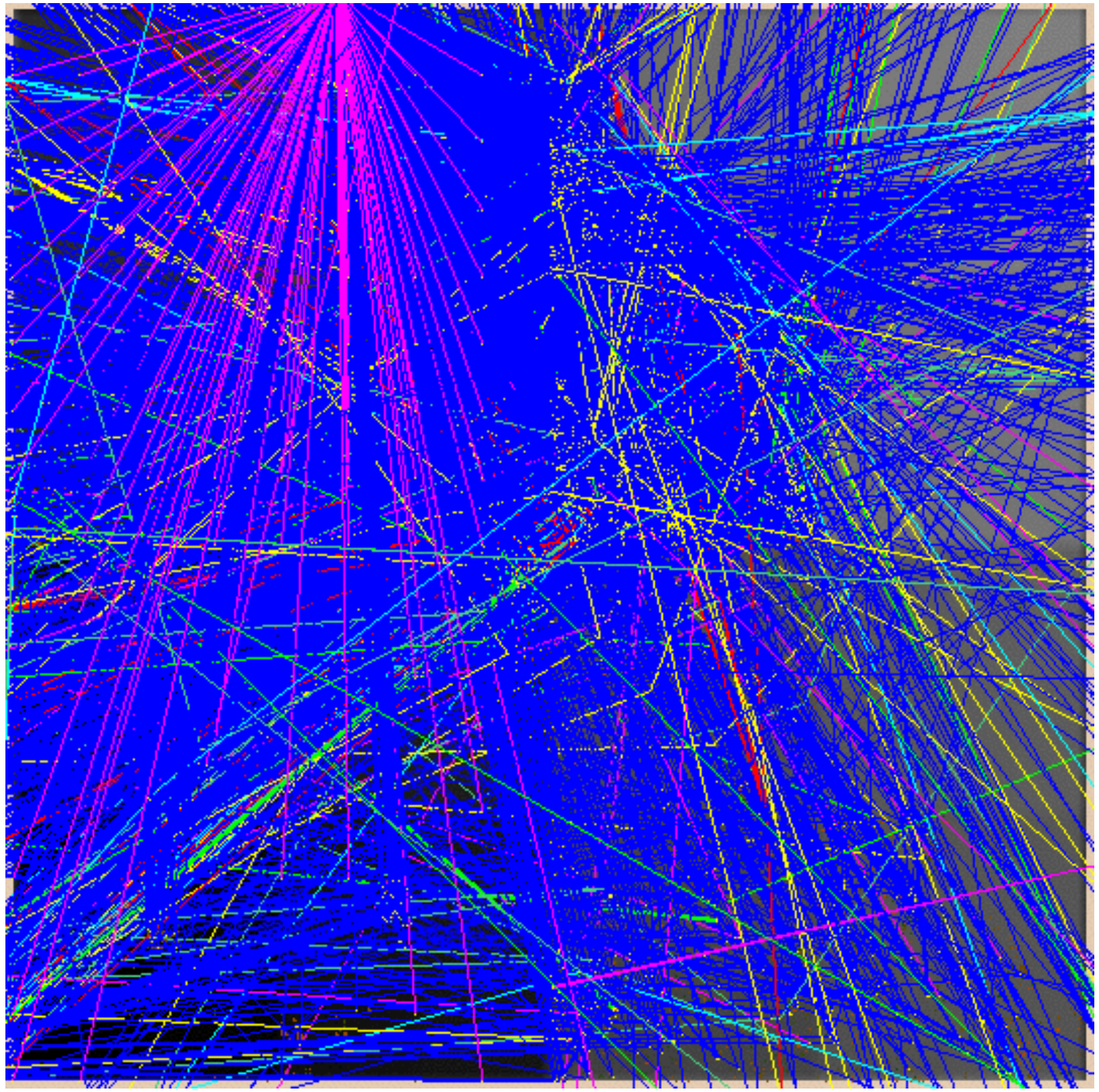
- Using different colors to represent types of OASC events
- **H type** : AS punches a hole on prefix addresses belonging to others
- **B type**: An AS announces a more specific prefix out of a larger block it already owns.
- O type: An AS announces a prefix previously not owned
  - **OS involving SOAS**
  - **OM involving MOAS**
- C type: An AS announces a prefix previously owned by another AS.
  - **CSS, CSM, CMS, CMM**
  - S=SOAS, M=MOAS



[Wu07]

August 14, 2000

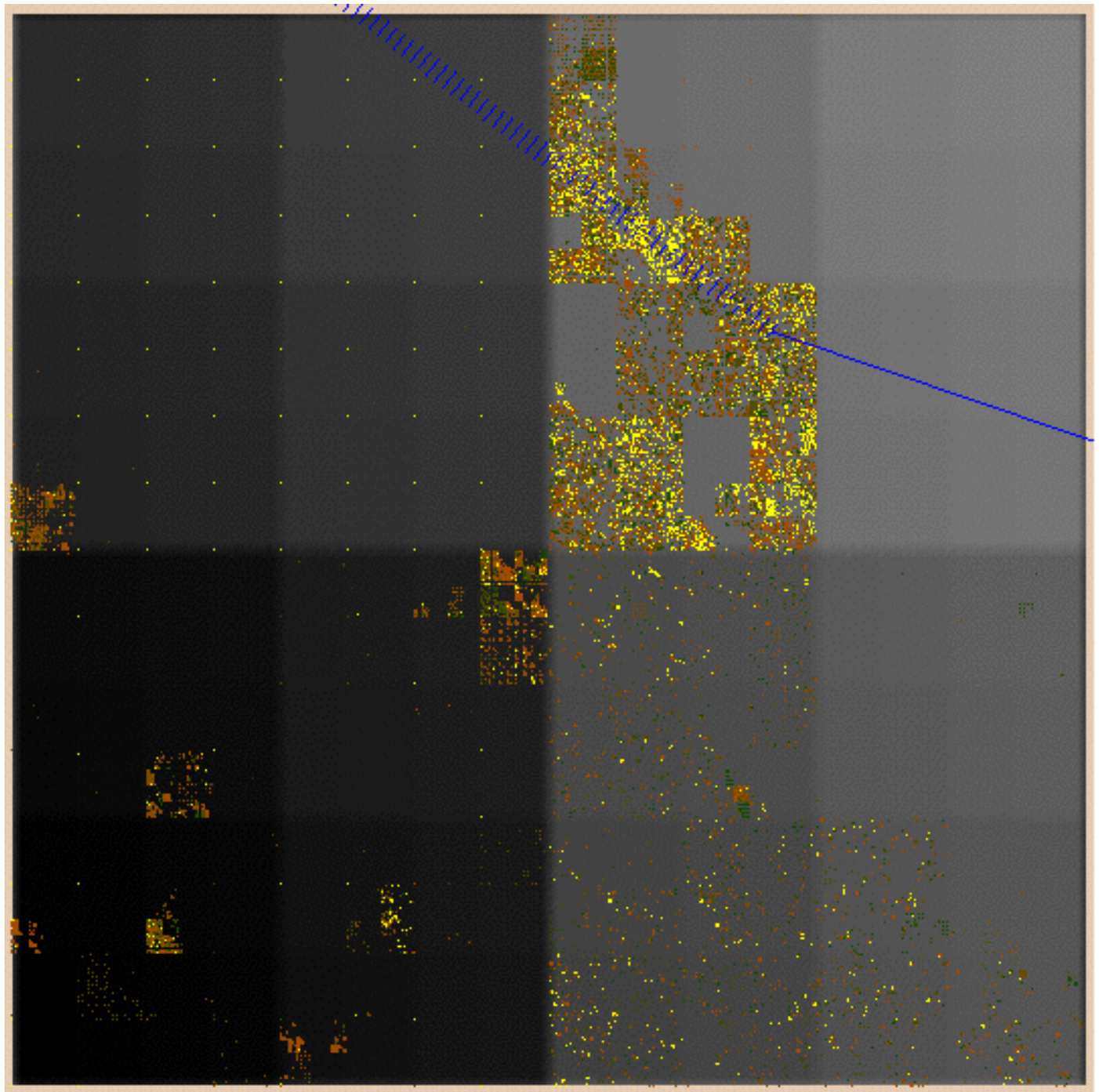
- A lot of blue lines (**H type**) :
  - AS punches a hole on prefix addresses belonging to others



[Teoh03]

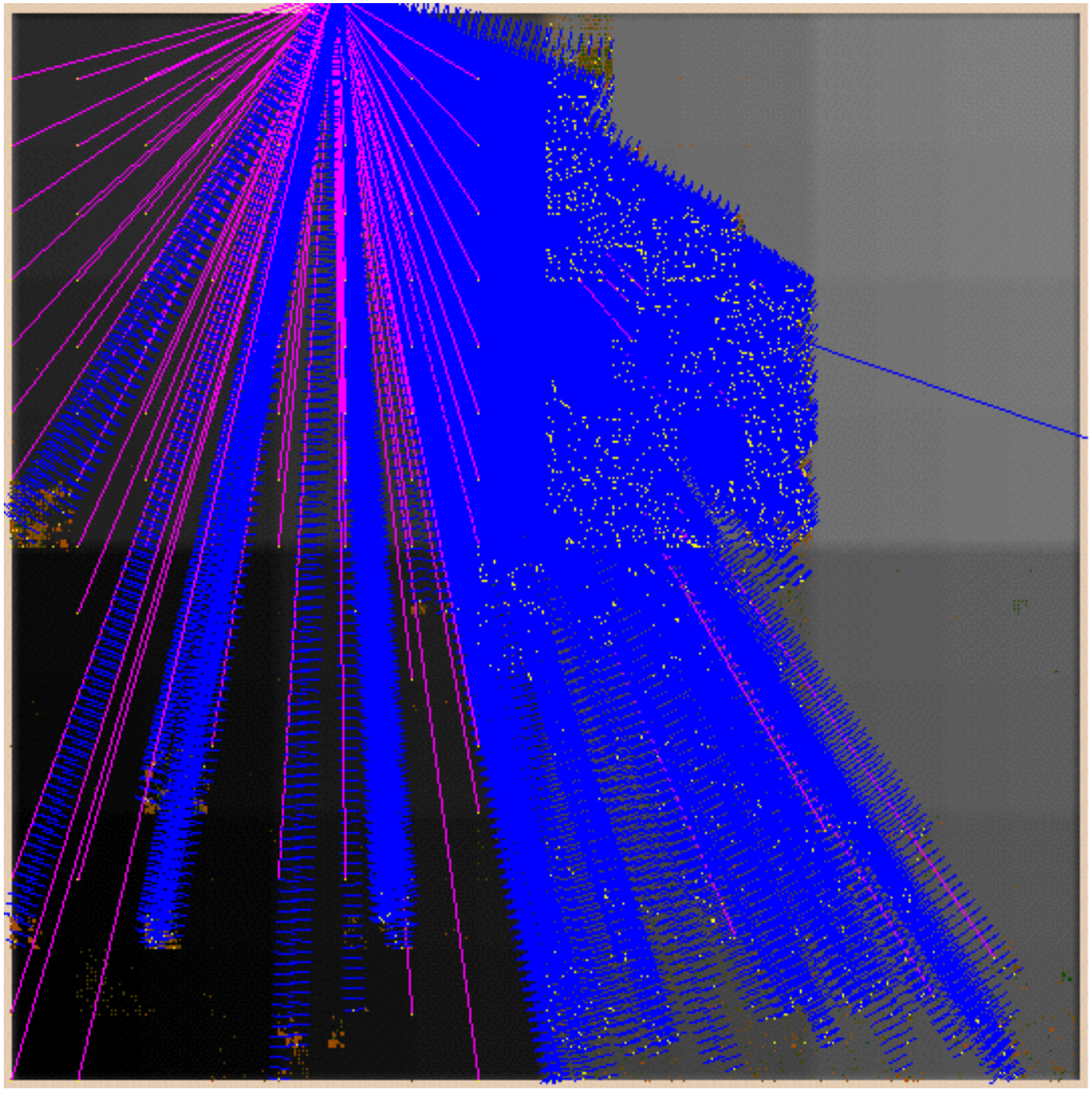
August 14, 2000

- Looking at AS 11724
  - 207.50.48.0/21
  - victim
- AS 7777
  - 207.50.53.251/32
  - Punching a hole
- Yellow pixel:
  - OASC occurred today
- Brown to Green pixel:
  - Change occurred on previous days



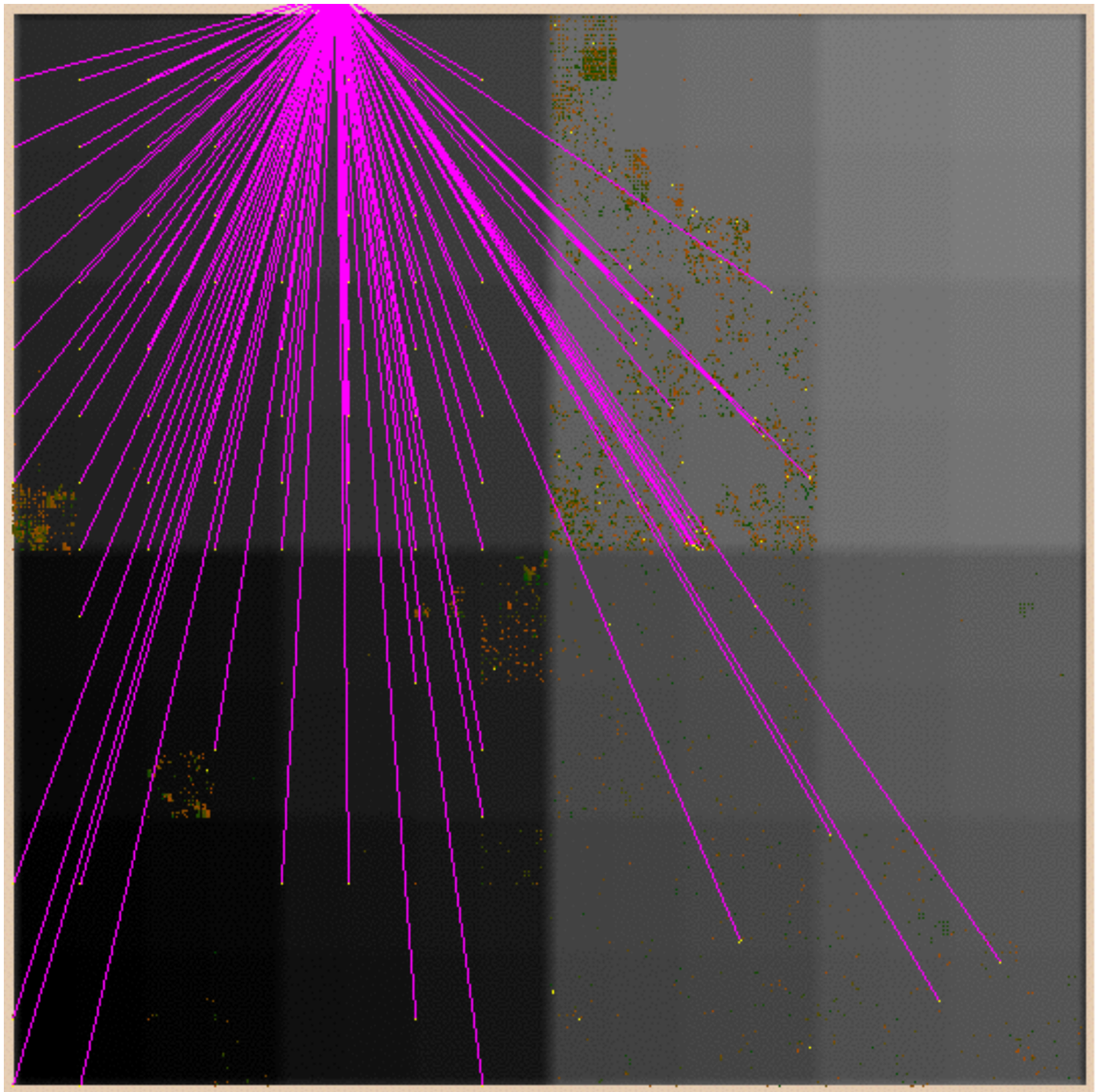
August 14, 2000

- Select OASC events related to AS 7777
- What are the pink links?



August 14, 2000

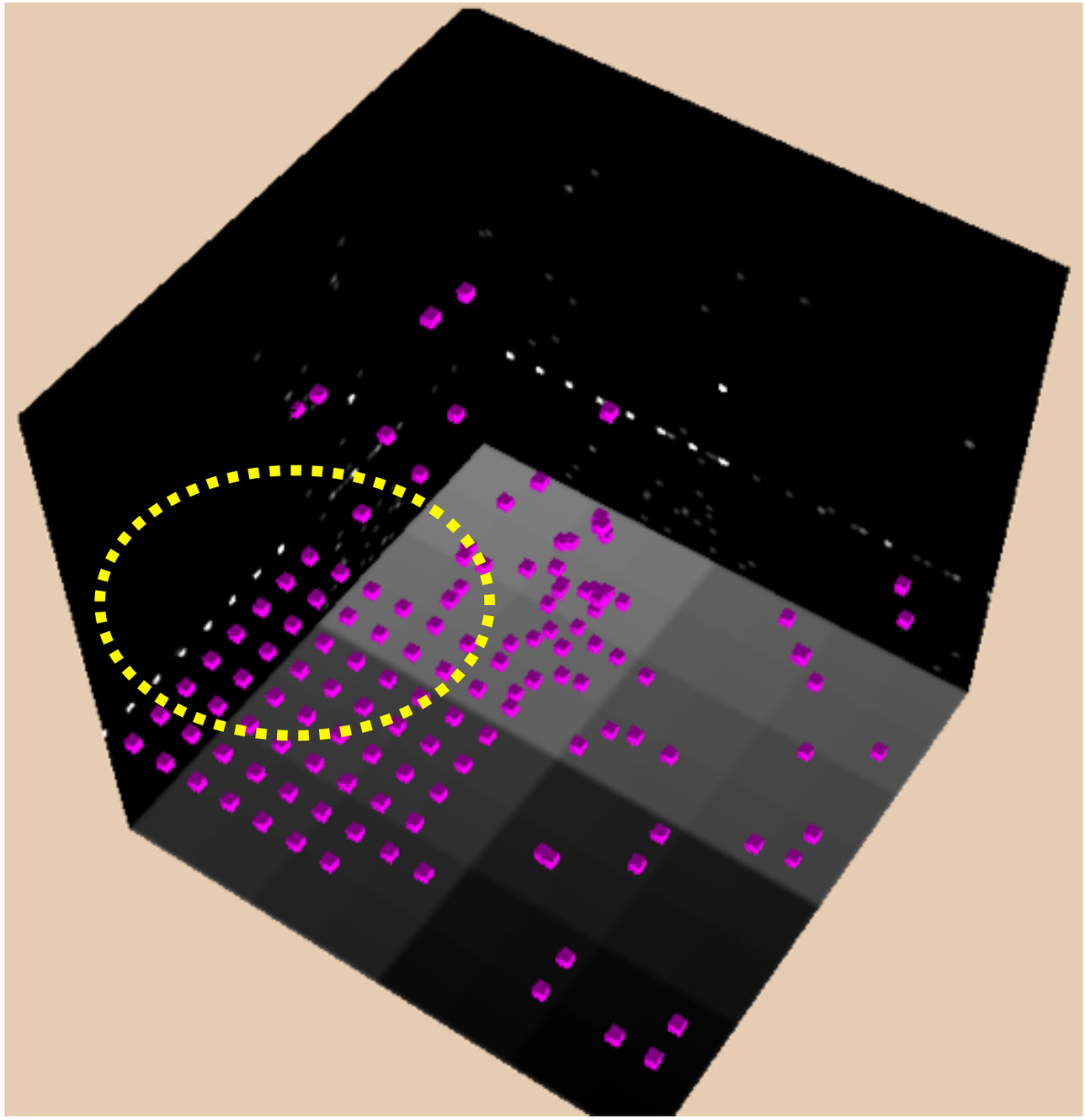
- O type: An AS announces a prefix previously not owned
  - **OS involving SOAS**
- There seems to be a pattern



[Teoh03]

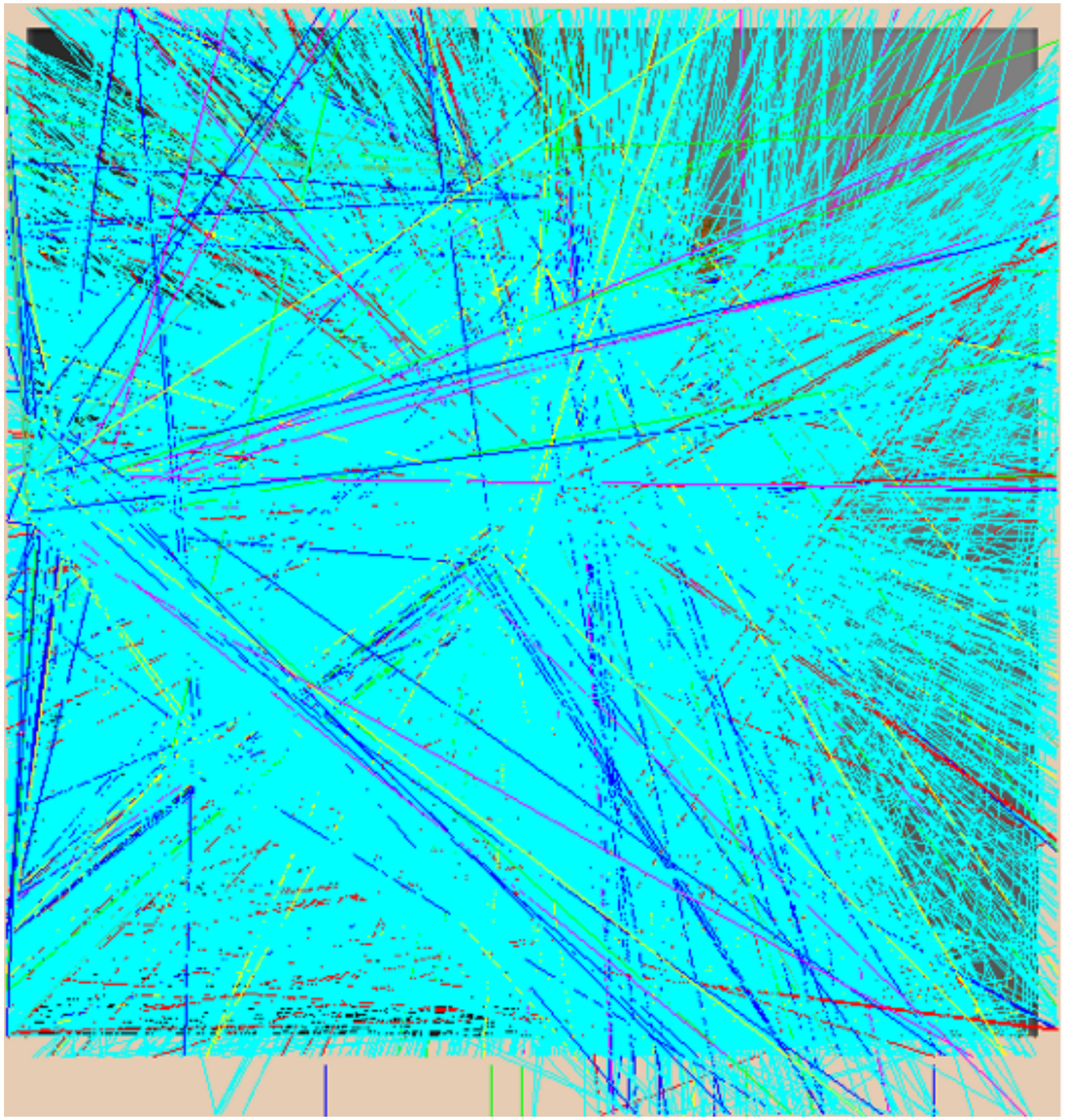
August 14, 2000

- 3D plot
- AS 7777 is advertising prefixes forming a grid in the unused address space.
- Announcing 65.0.0.0/8 to 126.0.0.0/8 + other addresses.
- Can you automate the pink grid detection?



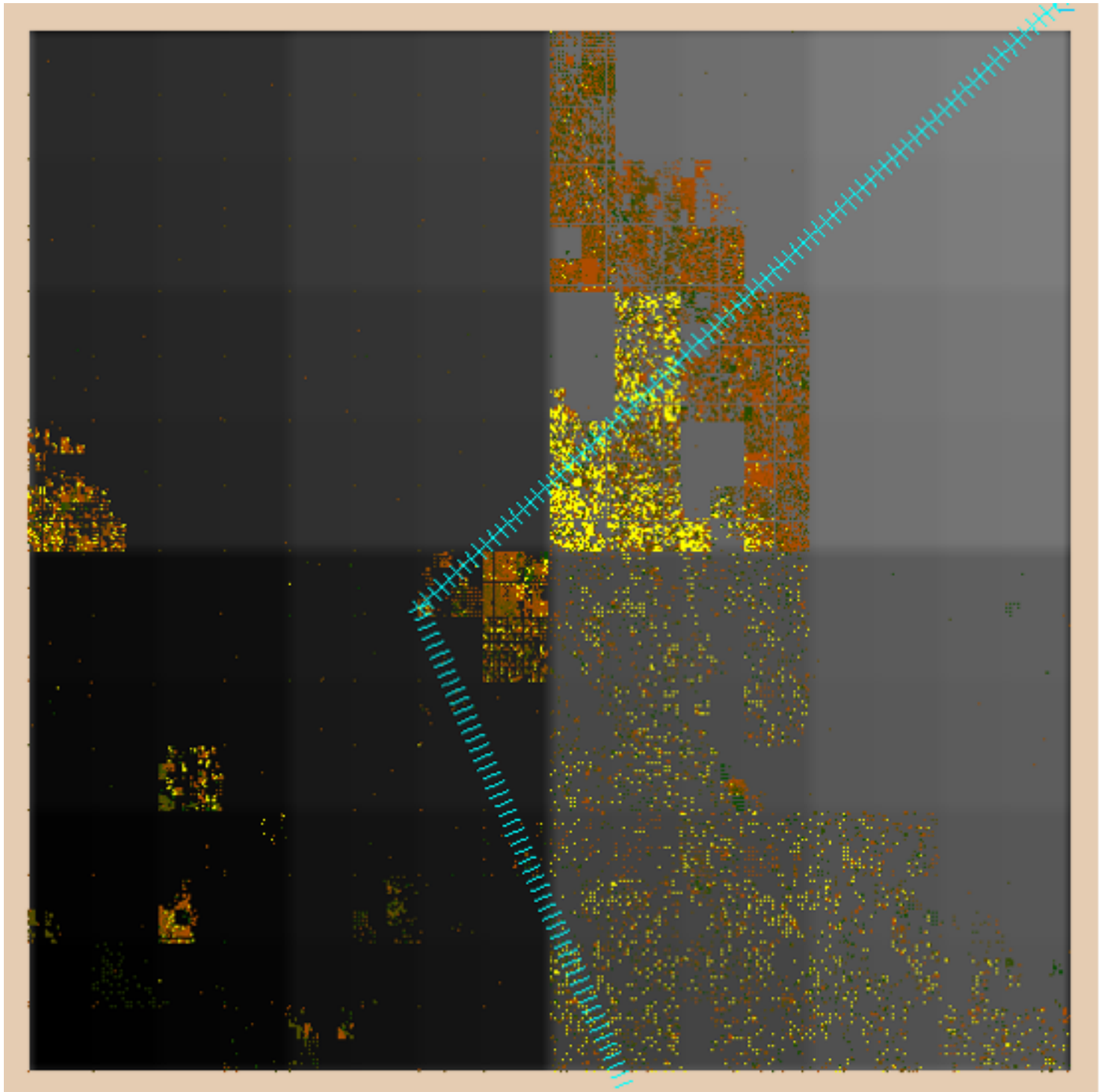
April 6, 2001

- Unusual amount of skyblue
- C type: An AS announces a prefix previously owned by another AS.
  - **CSM**
- Prefix claimed by one AS before, now by multiple ASs
- Small amount is fine
  - i.e. multi-homing



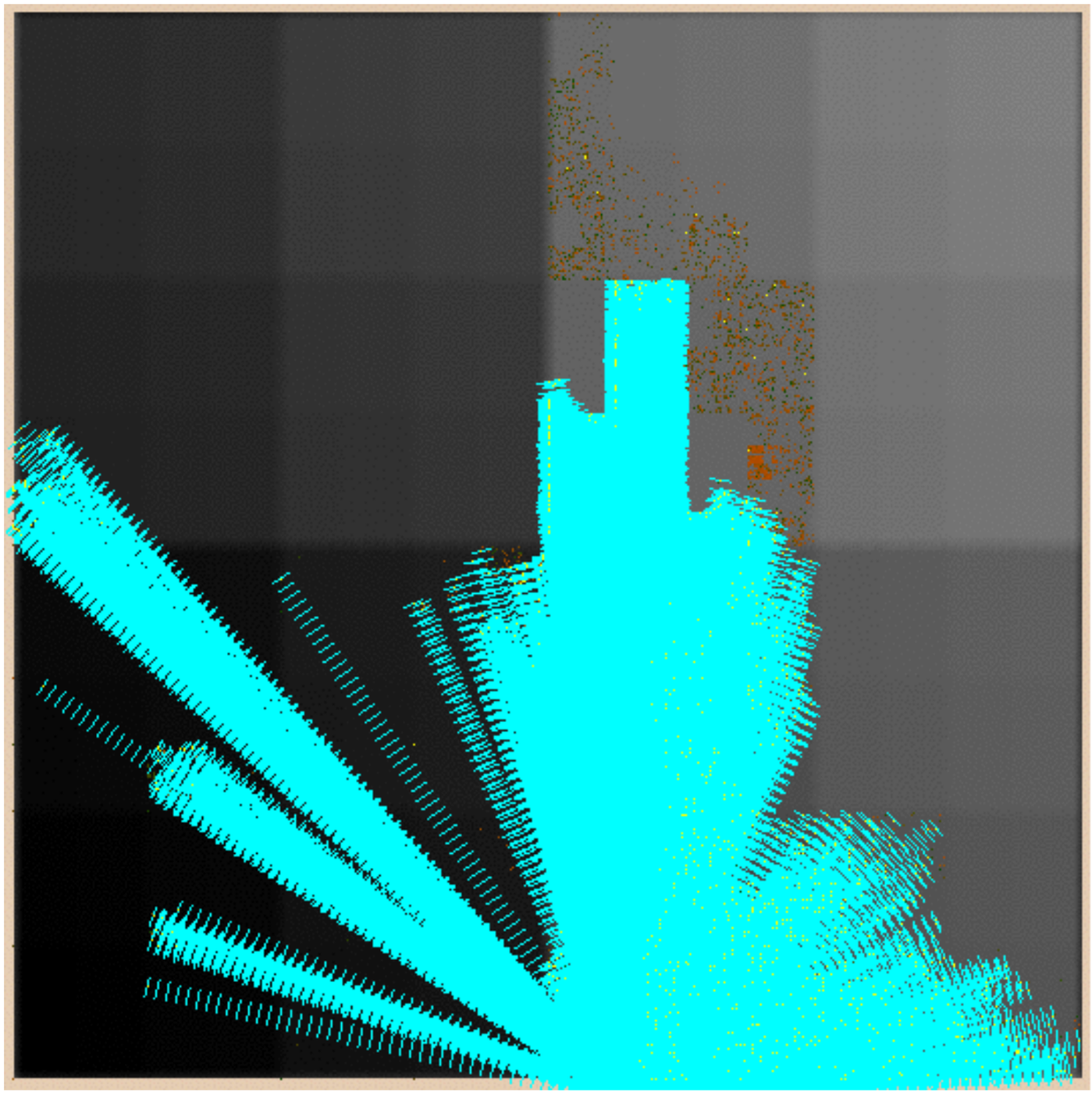
April 6, 2001

- New
  - AS 15412
- Old
  - AS 10132



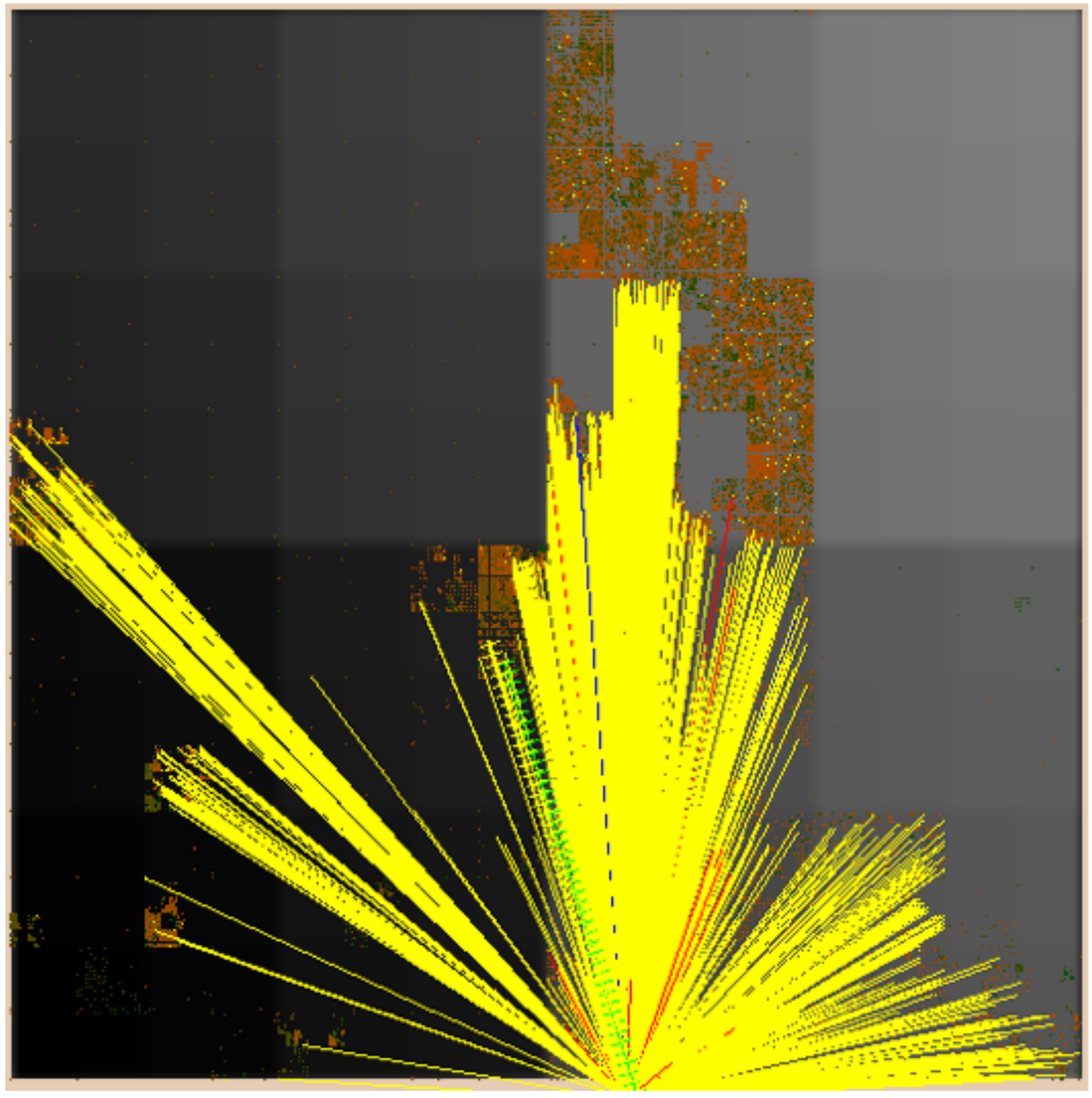
April 6, 2001

- Looking at AS 15412



April 7-12, 2001

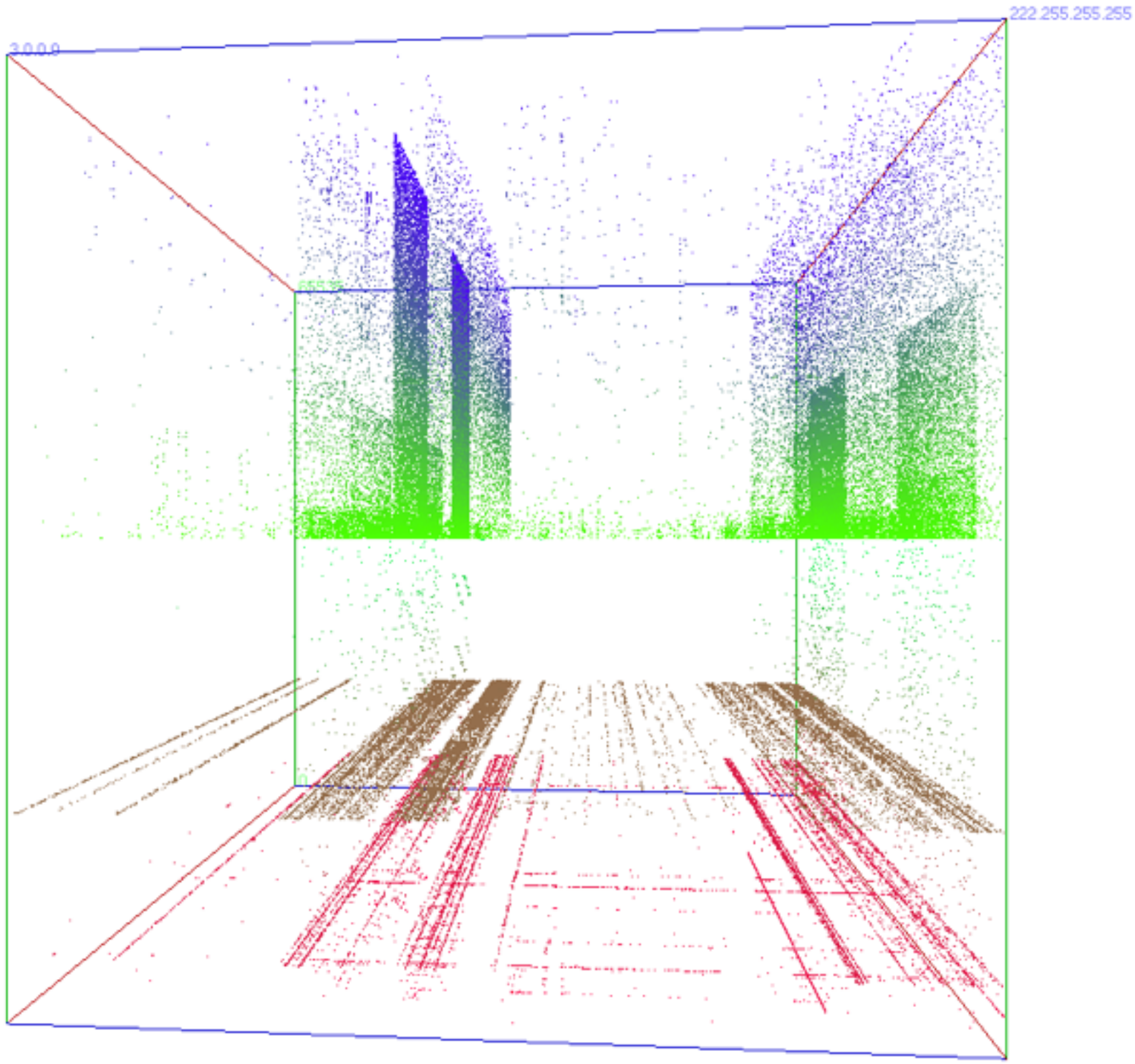
- Admin corrected the mistake
  - Announcements were withdrawn
- C type: An AS announces a prefix previously owned by another AS.
  - **CMS**



MonCube


65535
5000
1024
0
Dest. Port
Source IP
(Internet)
Destination IP

MonCube



Acknowledgments/References

- [Wu07] ecs 236, Intrusion Detection, S. Felix Wu, UC Davis, Winter 2007.
- [Rex05] COS 461, Computer Networks, Jennifer Rex, Princeton University, Spring 2005.
- [Peterson07] Computer Networks: A Systems Approach (Fourth Edition), by Larry L. Peterson, Bruce S. Davie, March 2007.
- [Teoh03] Visual-based Anomaly Detection for BGP Origin AS Change (OASC), Soon-Tee Teoh, Kwan-Liu Ma, S. Felix Wu, Dan Massey, Xiao-Liang Zhao, Dan Pei, Lan Wang, Lixia Zhang, Randy Bush, Presentation at DSOM, Germany, 2003.