PCH
Packet Clearing House

AS-Path Analysis

Testing Claims of "Tier 1" Status and Examining BGP Routing Anomalies

Version 1.2

September, 2006

Gaurab Raj Upadhaya

Bill Woodcock

Vijay Adhikari

PCH
Packet Clearing House

Background

Autonomous systems which claim “tier-1” status differentiate themselves from others by claiming that they do not receive transit from any other autonomous system.

PCH
Packet Clearing House

Background

Autonomous systems which do not receive transit may reach other ASes by selling transit to them or by peering with them.

Background

All AS-paths take one of two forms: One in which the “center” is an AS which provides transit to two down-stream ASes:

Dupont buys Sprint sells SBC sells Fry’s

Background

All AS-paths take one of two forms:
Or one in which the “center” is a peering session between two ASes, each of which provides transit to one down-stream AS:

PCH buys Verio peers Sprint sells SBC sells Fry’s

PCH
Packet Clearing House

Proposition

Since there can exist no more than one peering session in any AS-path,
No more than two ASNs can make a legitimate claim to “tier-1” status with respect to any valid AS-path.

PCH
Packet Clearing House

Seed-list to test

For an arbitrary starting-point to test our proposition, we took the intersection of the lists of most commonly-occurring transit ASes from a number of routers:

701	UUNet / MCI	1239	Sprint
3356	Level 3	2914	NTT / Verio
7018	AT&T	6461	MFN
209	Qwest	2828	XO Communications
3549	Global Crossing	6461	SAVVIS

PCH
Packet Clearing House

Adding a Candidate

Adding ATDN (AOL Transit Data Network) to our list yields no additional observed anomalies. Thus they're probably fairly "tier-1."

PCH
Packet Clearing House

Adding a Candidate

The arbitrary method by which we seeded our list does not find content providers, only transit providers.

ATDN is reputed to be “tier-1” so we can test our proposition by adding them, and checking to see whether this yields additional anomalies...

Packet Clearing House

Testing the Proposition

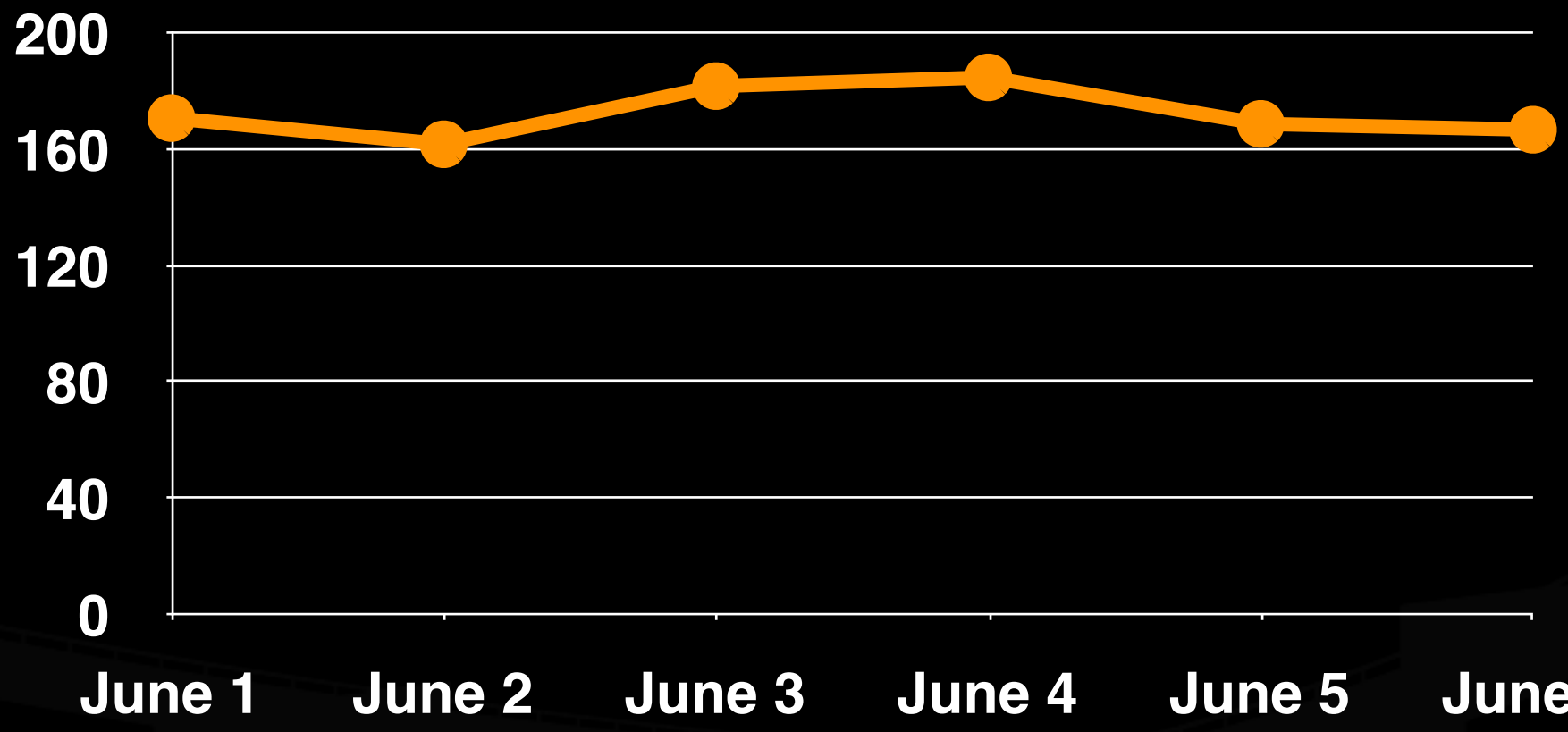
We find anomalous cases, in which three or more ASNs from our test list occur in the same AS-path:

65.215.36.0/24

3549	6221	3356	701	22907
Global Crossing	Cybersites	Level 3	UUNET	

Leaked Routes

(more than 2 Tier1 ASNs)



PCH
Packet Clearing House

More Anomalies

Inconsistent ASNs

Non-contiguous Repeats

Private ASNs

Unallocated ASNs

PCH
Packet Clearing House

Inconsistent Prefix Announcements

Examples

12.33.218.0/24

Announced by more than 1 ASNs:

22057, 23181

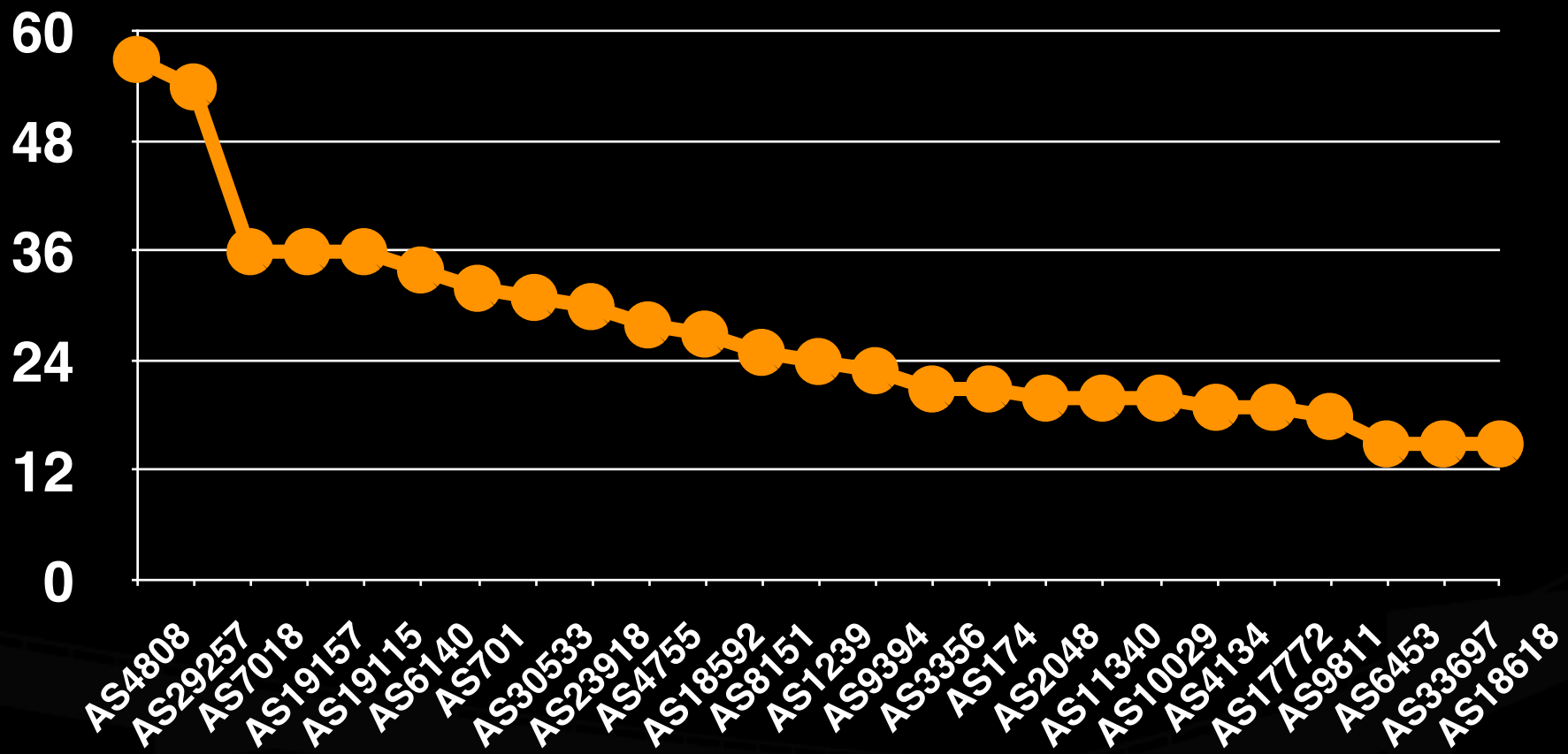
12.64.255.0/24

Announced by more than 1 ASNs:

4264, 17228, 17229, 17233

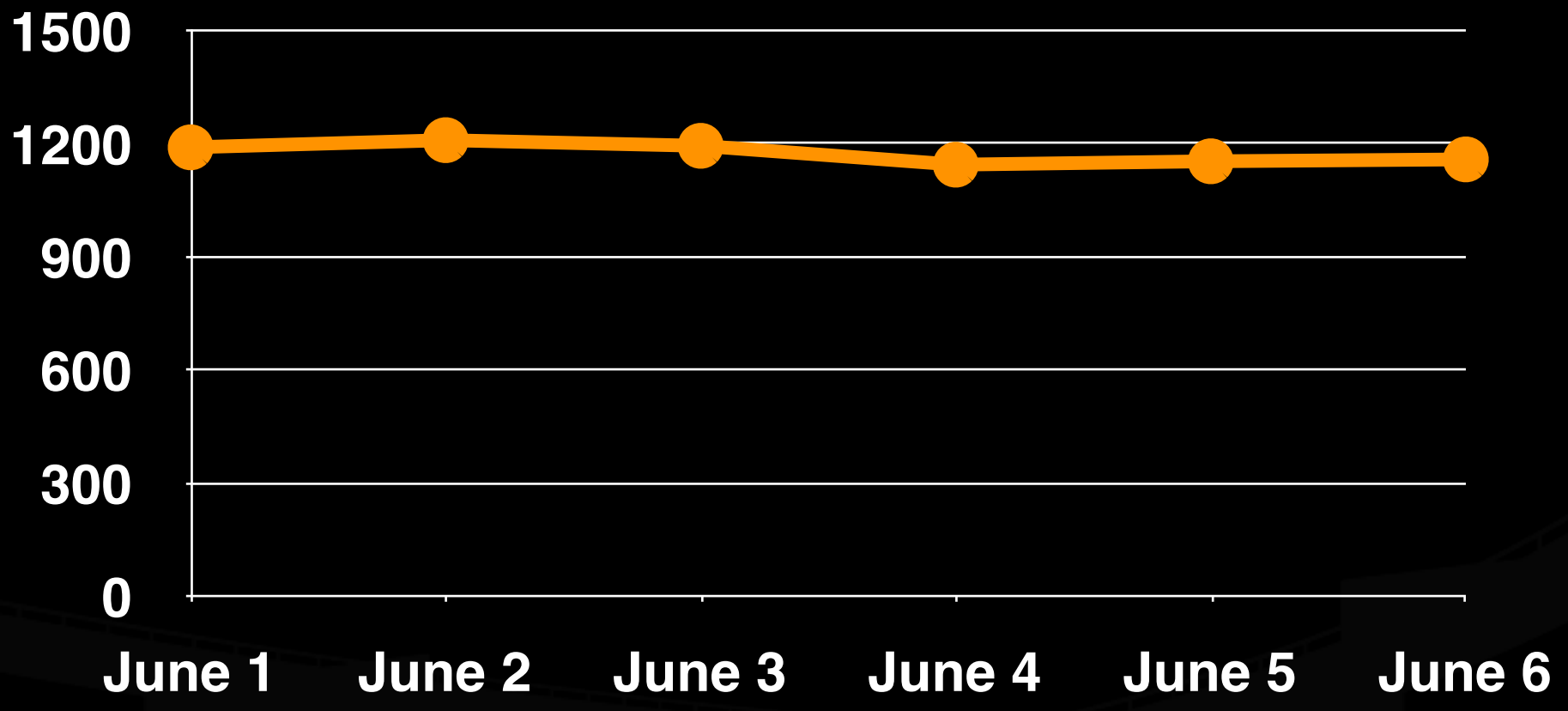
Packet Clearing House

Inconsistent Prefix Announcements



Packet Clearing House

Inconsistent Prefix Announcements



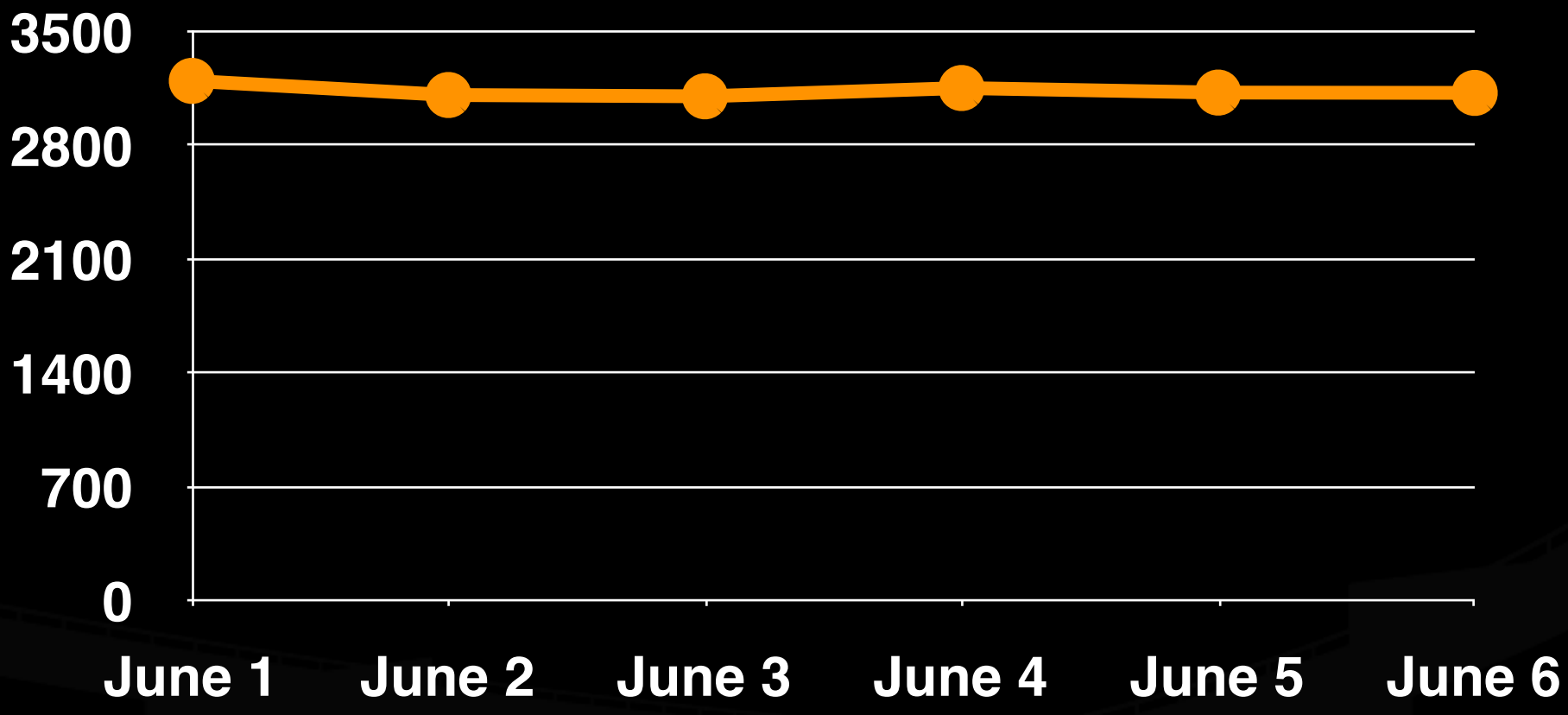
Non-contiguous Repeats

Examples:

1299 7018 12163 12163 12162 12163 12163 12163 12163
7018 65000 65001 7018 1239 4648 2764 9837 9476
11608 13768 21548 21548 21548 21548 7018 21548 36231

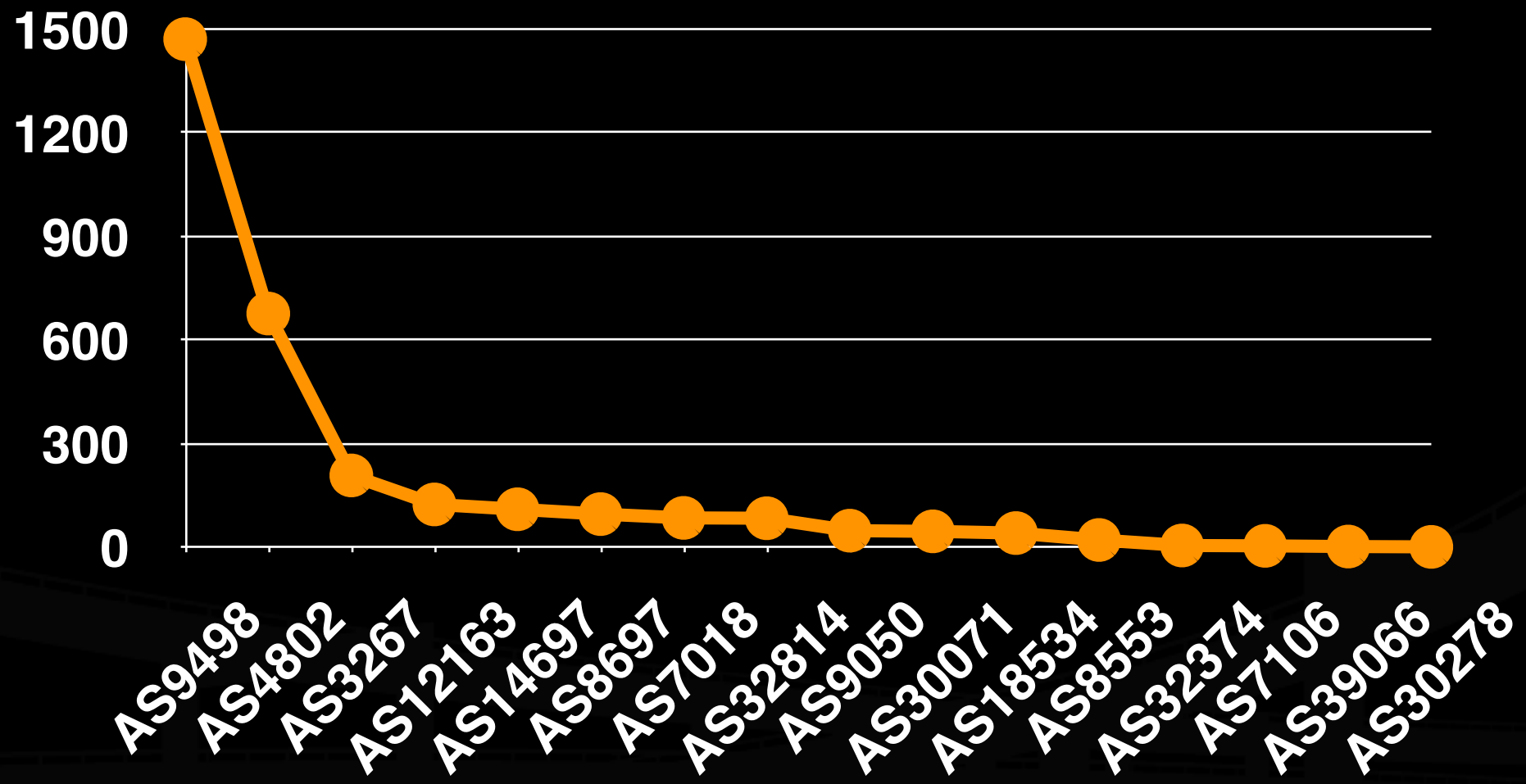
PCH
Packet Clearing House

Non-contiguous Repeats



PCH
Packet Clearing House

Non-contiguous Repeats



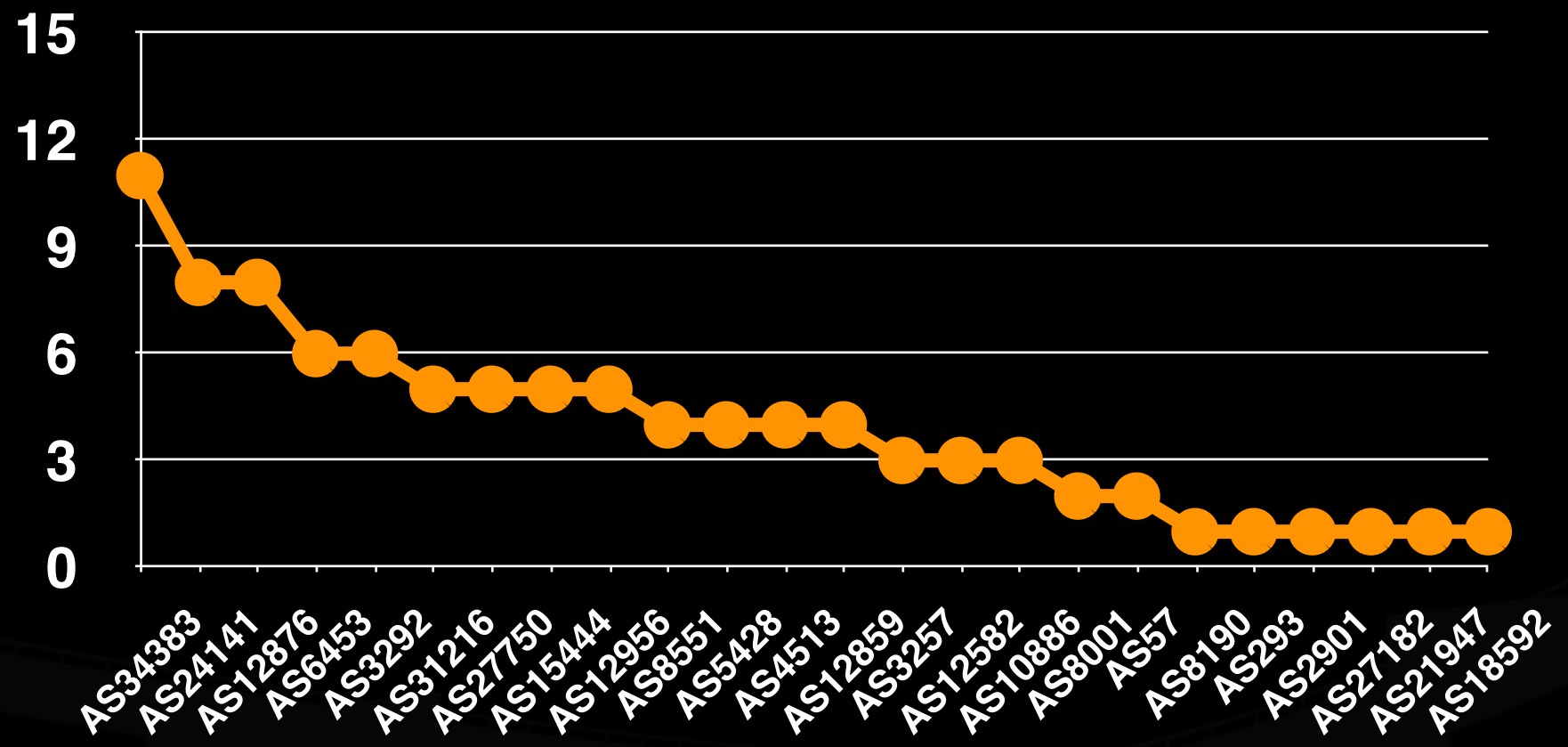
Packet Clearing House

Private AS Number Leak

7018 65000 65001 7018 1239 4648 2764 9837 9476
14608 19029 2516 65000 4134

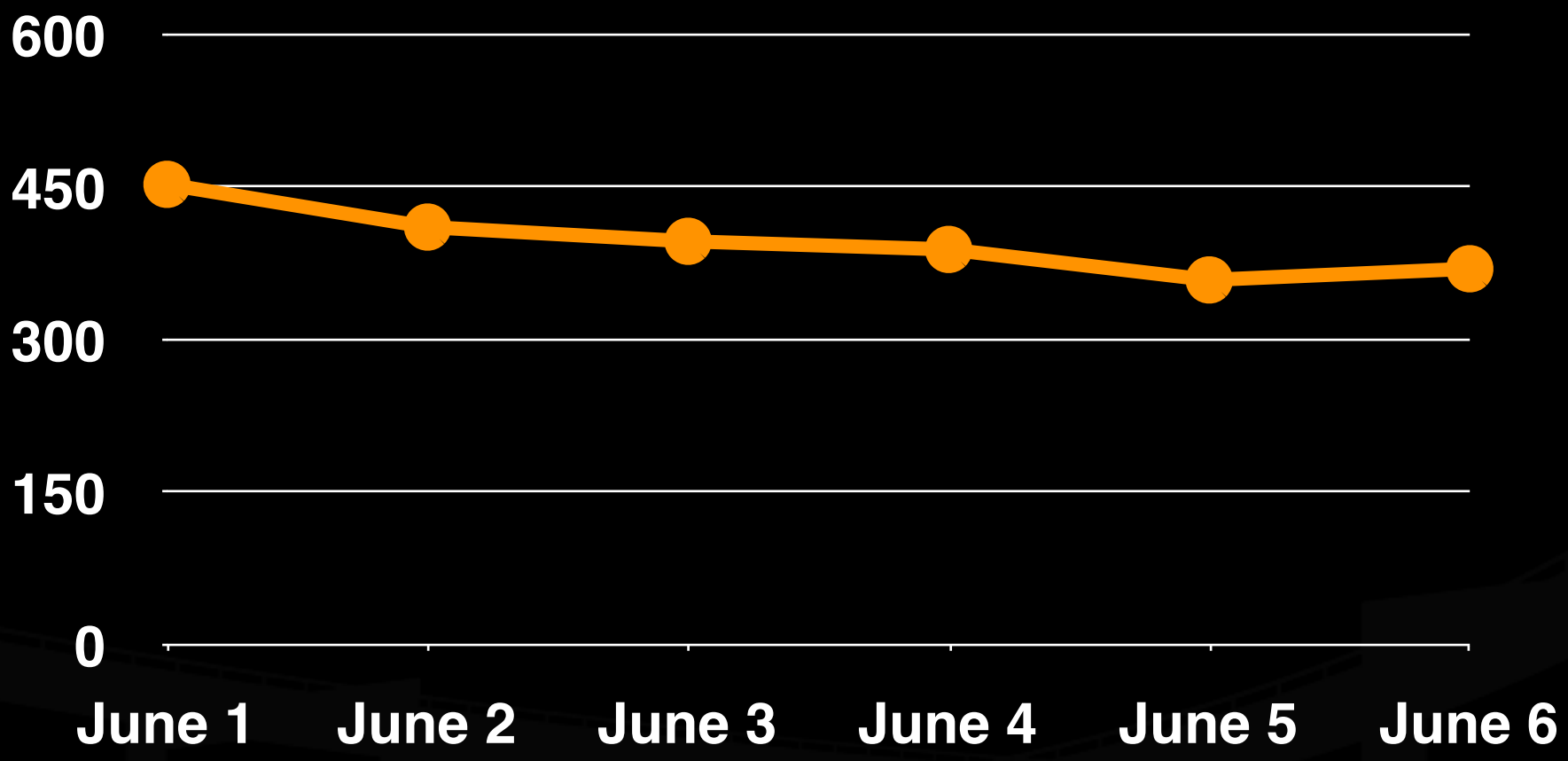
Packet Clearing House

Private AS Number Leak



PCH
Packet Clearing House

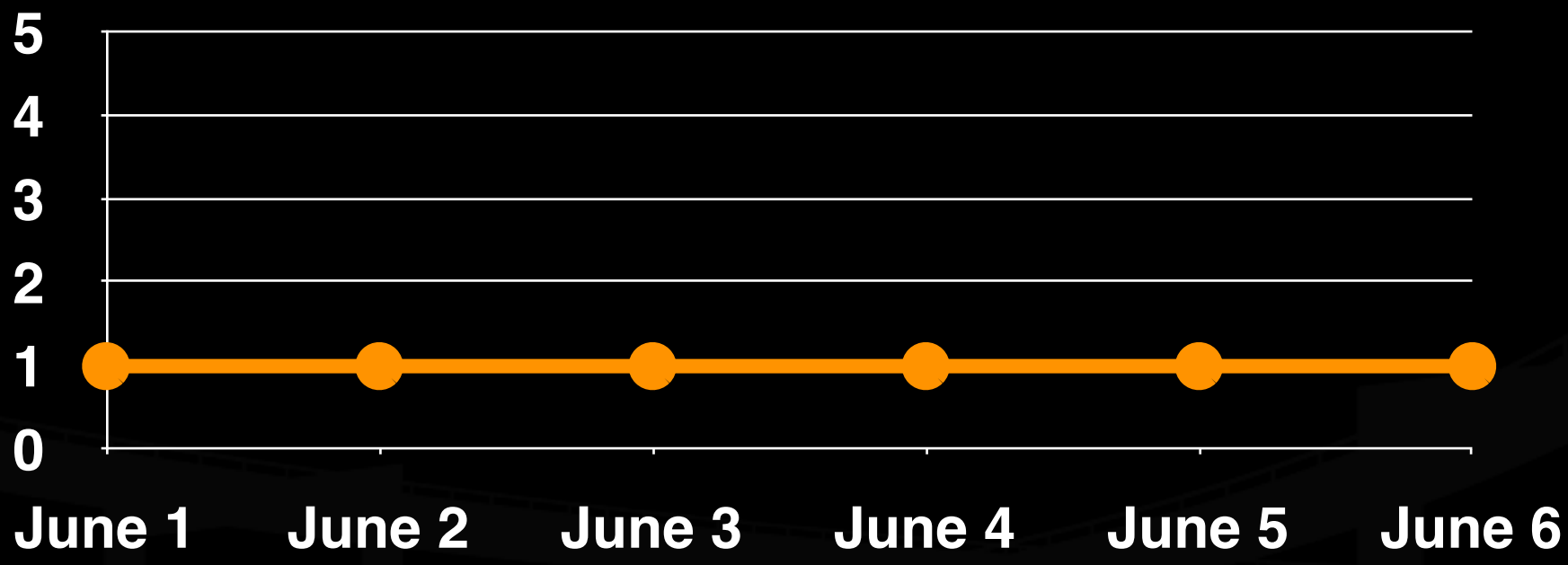
Private AS Number Leak



Using and Leaking Unallocated ASN

24587 is the only ASN leaking an unallocated ASN

81.17.39.128/27 3333 24587 64500



‘X’ relationships

Contrary to our assumption on ISP relationship, we see quite a few ‘X’ relationship

e.g

7660 / 2516 \ 7473 \ 9498 X 9730 X 9498 \ 17913

8001 / 7018 \ 9498 X 9730 X 9498 \ 17625

Where, AS9498 & AS9730 are two parts of same company

5650 / 7018 \ 12069 X 23269

5650 ? 22773 \ 23269 \ 12069

Where, it’s very likely that 23269 is leaking routes

PCH
Packet Clearing House

X Relationship

Where two ASNs announce each other routes

Use iterative parsing of the routing table data from multiple sources

Additional cross-checks

- Assume the top 10 ASNs as not buying from anyone
- Look at peer routes collected on PCH routers
- Regional full routes in 4 locations around the world from our own routers and by others.

Packet Clearing House

Deciphering X Relationships

Using Whois is sometimes useful

```
aut-num:    AS10310
as-name:    Yahoo-prod
descr:      Yahoo, Inc. production AS

aut-num:    AS26085
as-name:    Yahoo-SC5
descr:      Yahoo SC5 datacenter
```

sometimes it's not:

```
aut-num:        AS35324
import:         from AS35391 accept ANY
export:         to AS35391 announce ANY

aut-num:        AS35391
import:         from AS35324 accept ANY
export:         to AS35324 announce ANY
```

Packet Clearing House

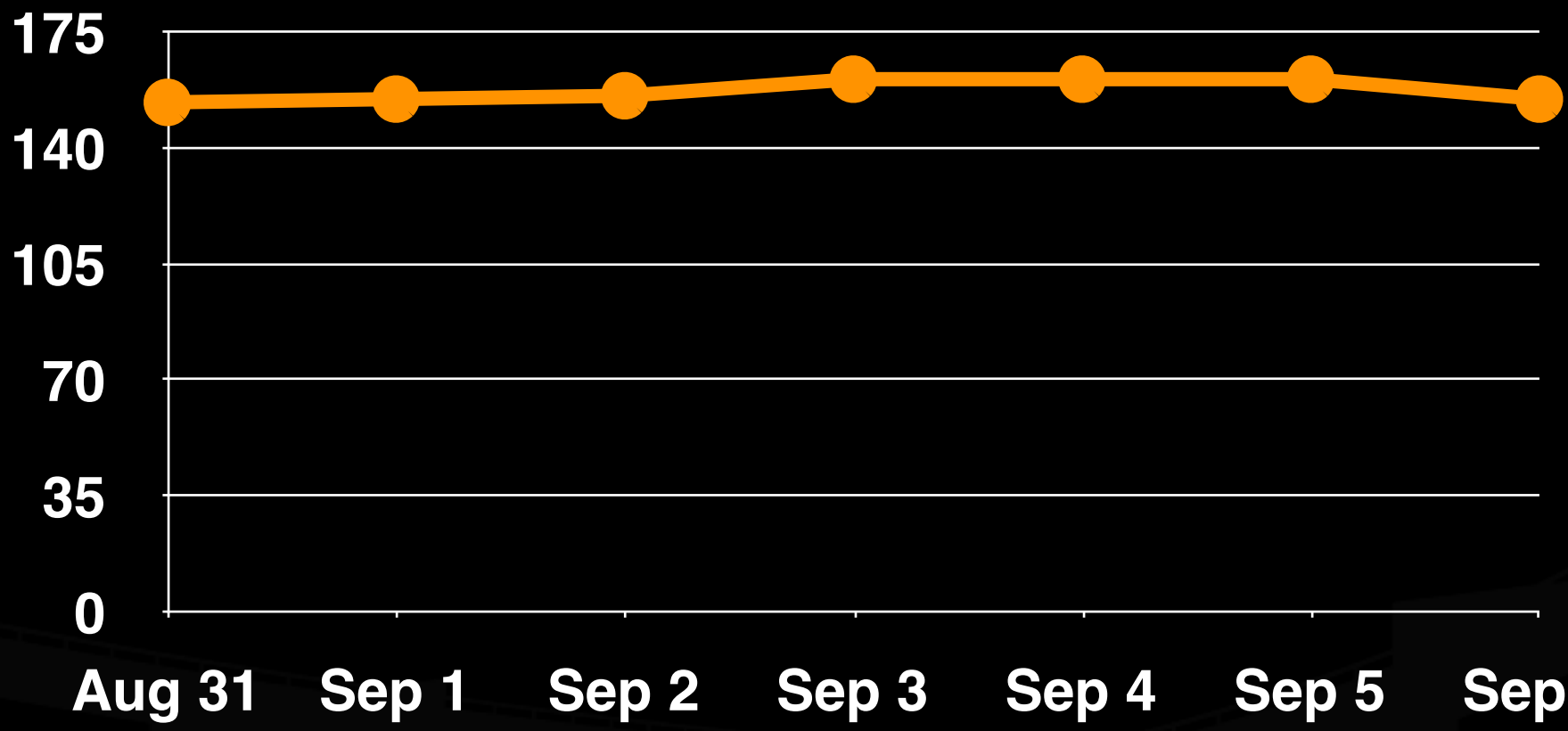
Deciphering X Relationships

Some AS-PATH are difficult to explain

Best Guess here : ANC is leaking Routes, but how Tiscali comes between ANC and CNC is difficult to imagine - both topologically and geographically

Packet Clearing House

X - Relationship count



PCH
Packet Clearing House

Plan

Setup a e-mail mechanism to report possible route-leaks to ASNs

Setup a web front end so that operators can check against possible route leaks by peers and customers

More extensive cross check mechanism, against historical and archived data

PCH
Packet Clearing House

Thanks, and Questions?

Copies of this presentation can be found
in PDF and QuickTime formats at:

http:// www.pch.net / resources / papers / bgp-aspath-analysis

Gaurab Raj Upadhaya
Vijay Kumar Adhikari
Bill Woodcock

bgp-anomalies@pch.net