Characterizing Large-scale Routing Anomalies: A Case Study of the China Telecom Incident

Rahul Hiran[1], Niklas Carlsson[1], Phillipa Gill[2]

[1] Linköping University, Sweden

[2]University of Toronto, Canada

19th March2013

LiU EXPANDING REALITY

China Telecom incident

Forbes · New Posts +26 posts this hour · Most Popular Google's Driverless Car · Lists Business Of Basketball

0 Share 0 Tweet 0 Share

Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.
+ Follow (647)

SECURITY | 11/19/2010 @ 12:06PM | 4,685 views

China Hijacks 15% Of Internet Traffic? More Like .015%

Internet Traffic from U.S. Government Websites Was Redirected Via Chinese Networks

By Joshua Rhett Miller / Published November 16, 2010 / FoxNews.com

The Telegraph

HOME NEWS WORLD SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFE

USA Asia China Europe Middle East Australasia Africa South America Central Asia

HOME » NEWS » WORLD NEWS » ASIA » CHINA

China 'hijacks' 15 per cent of world's internet traffic

China "hijacked" 15 per cent of the world's internet traffic for 18 minutes earlier this year, including highly sensitive email exchanges between senior US government and military figures, a report to the US Congress said.

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › Technology › Internet

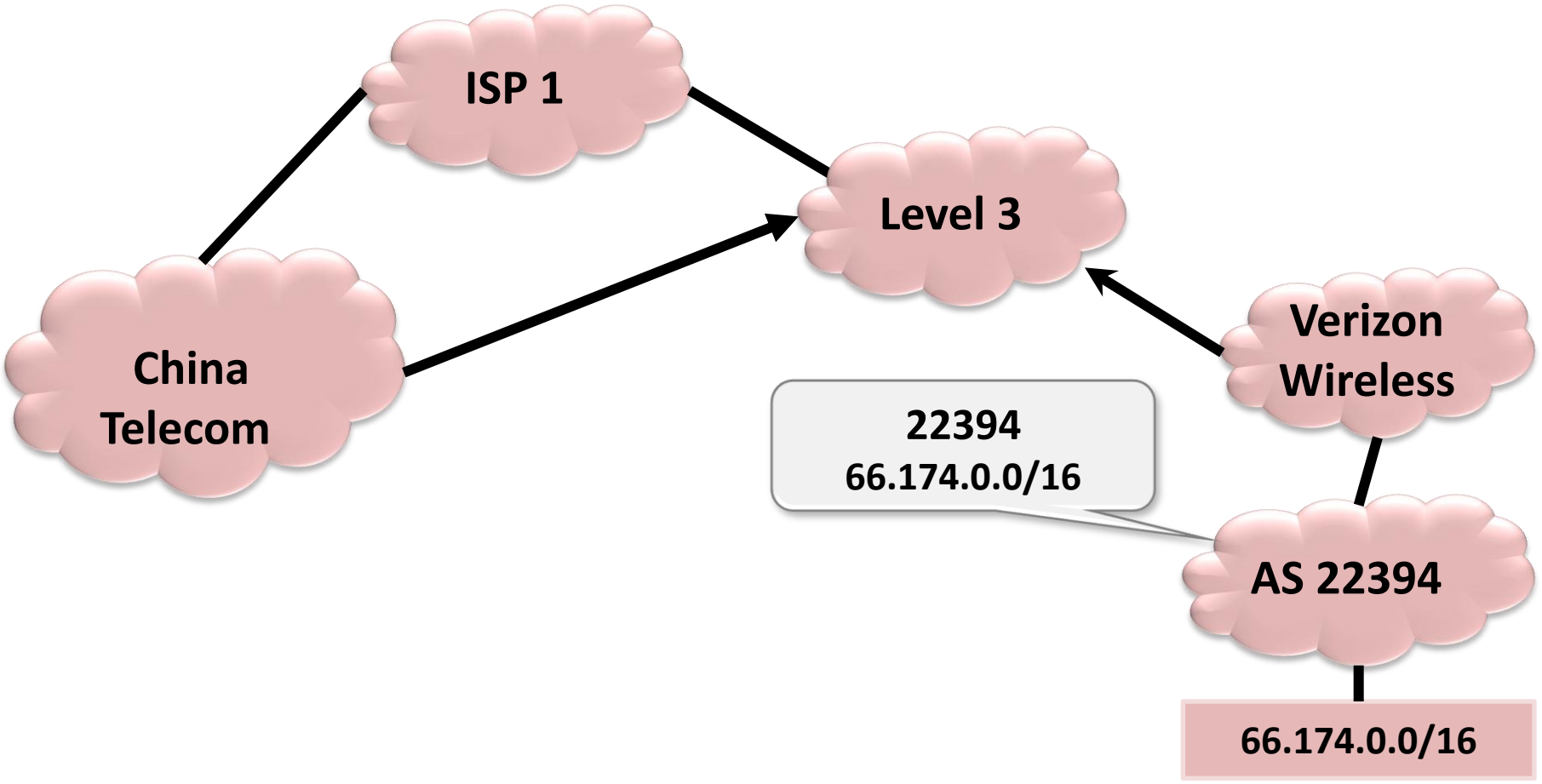
China denies 'hijacking' internet traffic

US report claims Chinese telecoms company had access to 15% of global traffic, including military emails, for 18 minutes

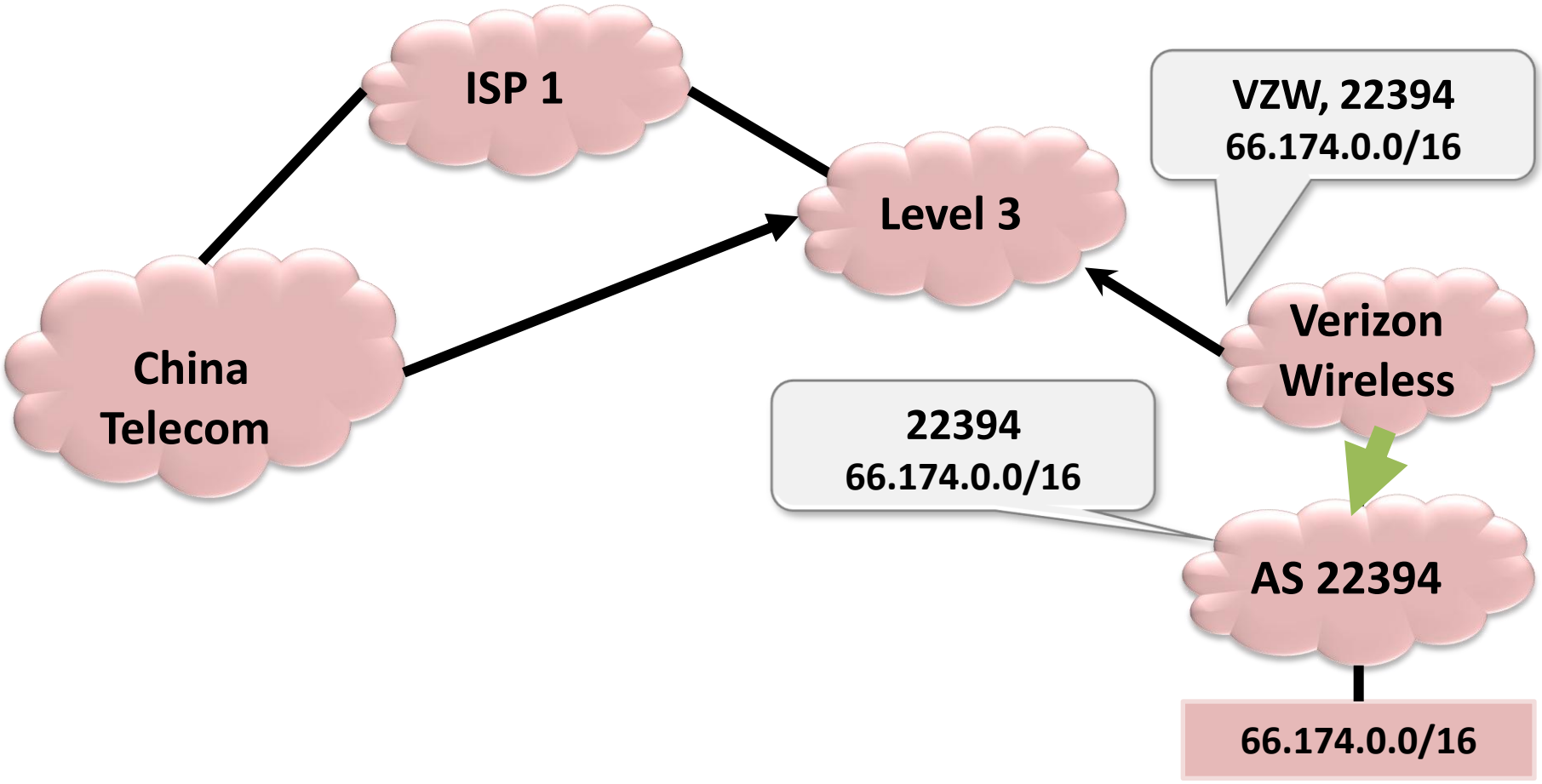
China Telecom incident

- The incident occurred on 8th April 2010
- The congress report, 2010 in USA mentions the incident
- Questions about what was done with the data, attack or accident
- We characterize this incident using only publicly available data (e.g., Routeviews and iPlane)

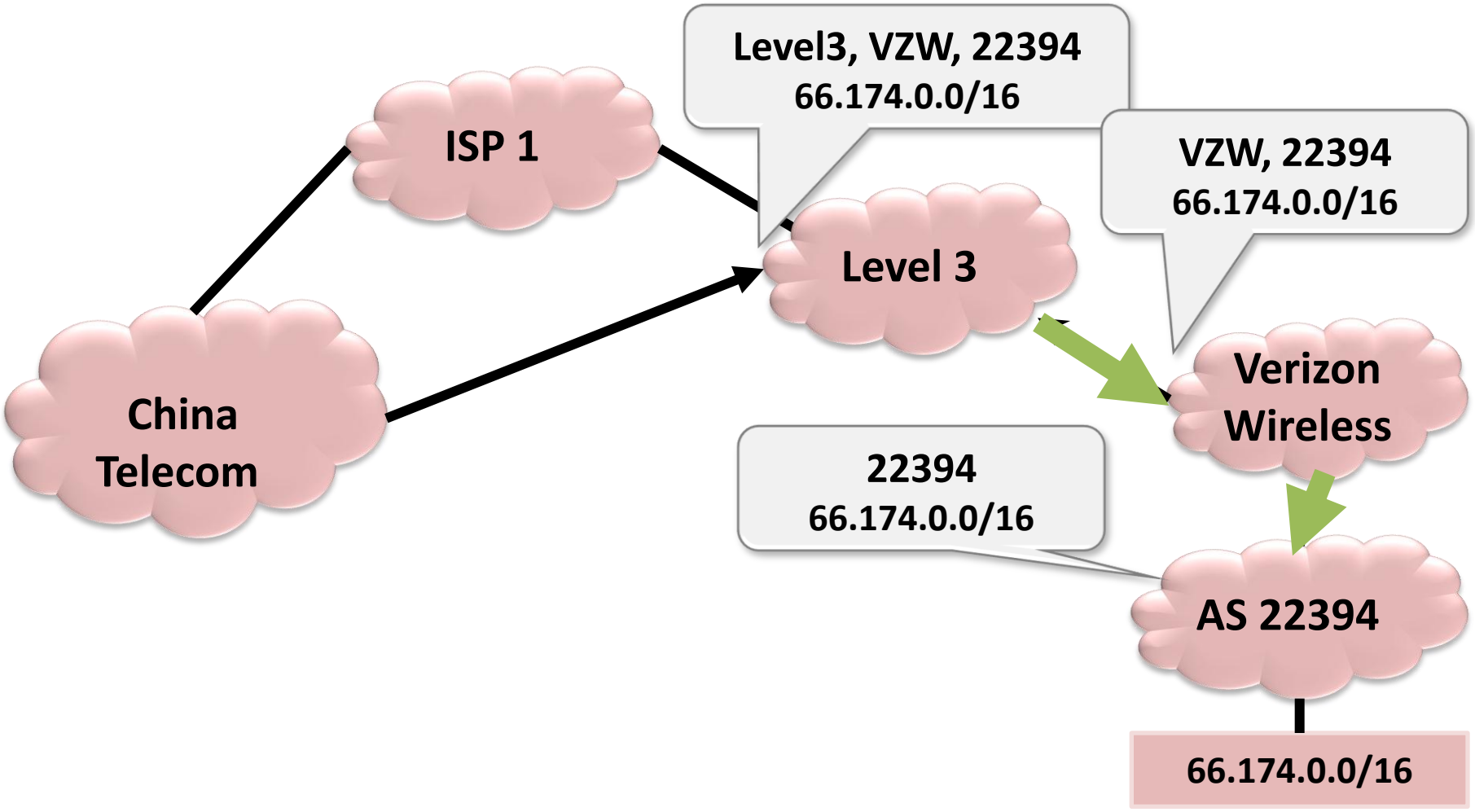
BGP (Border Gateway Protocol) refresher



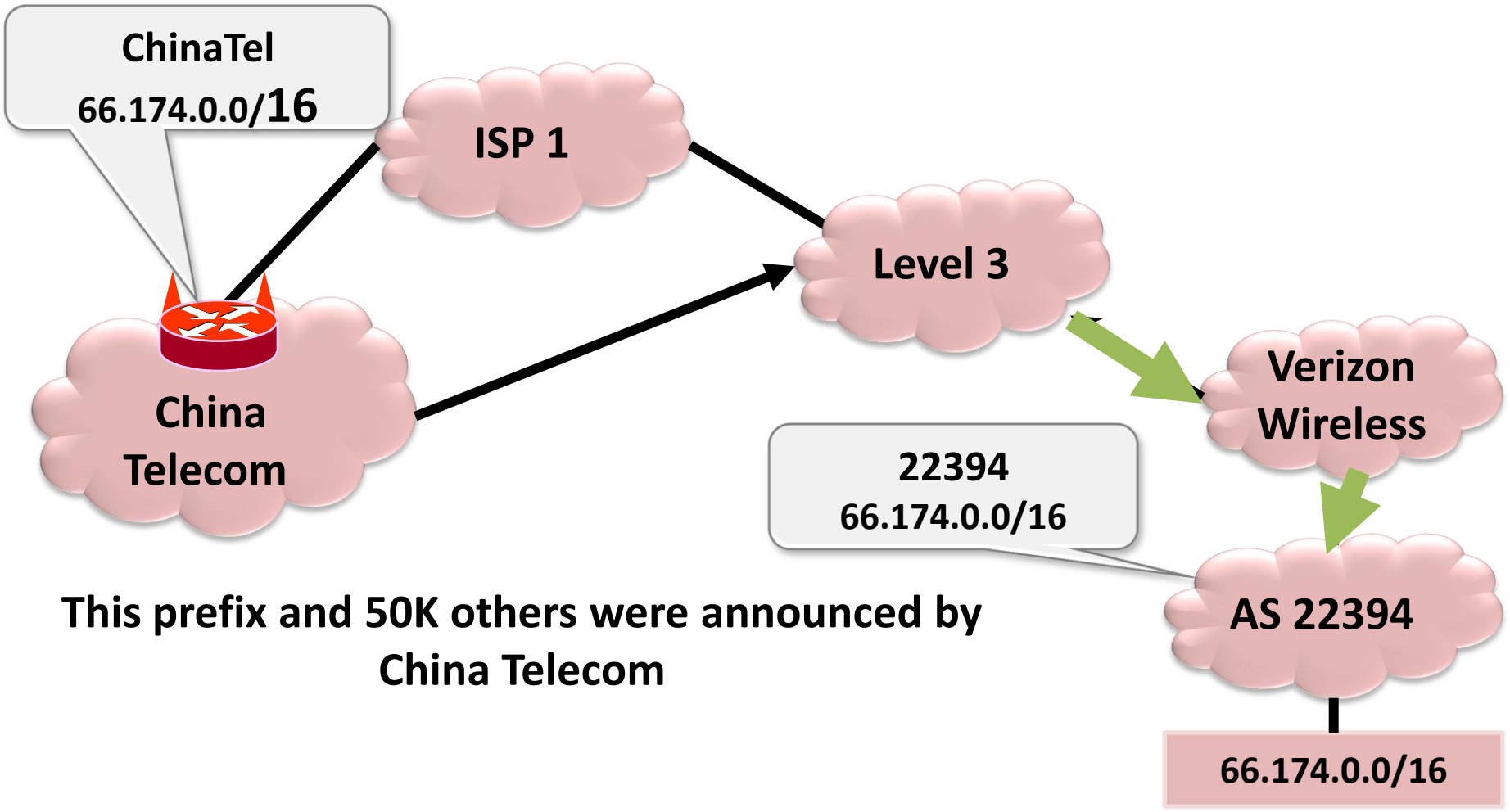
BGP (Border Gateway Protocol) refresher



BGP (Border Gateway Protocol) refresher

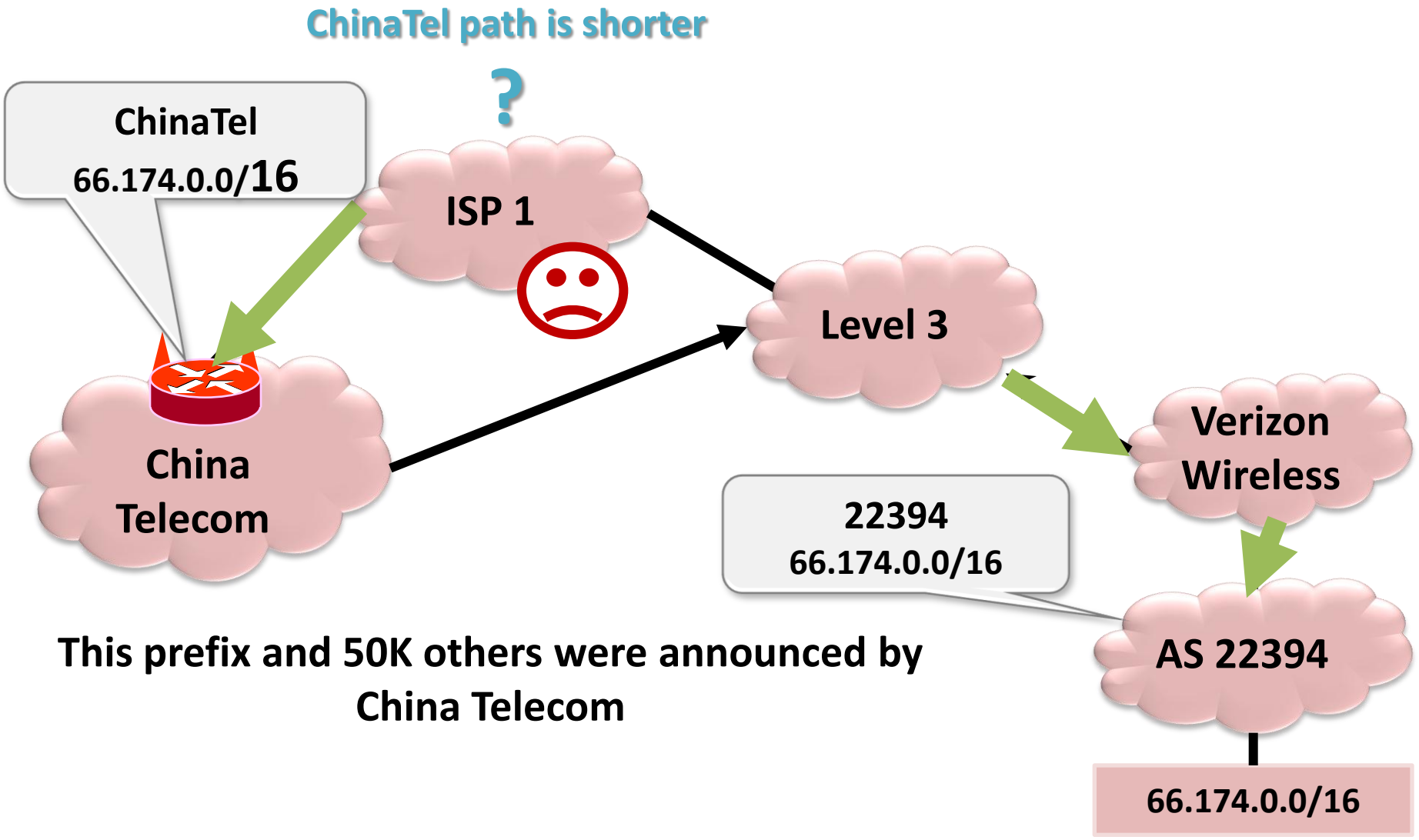


BGP (Border Gateway Protocol) refresher



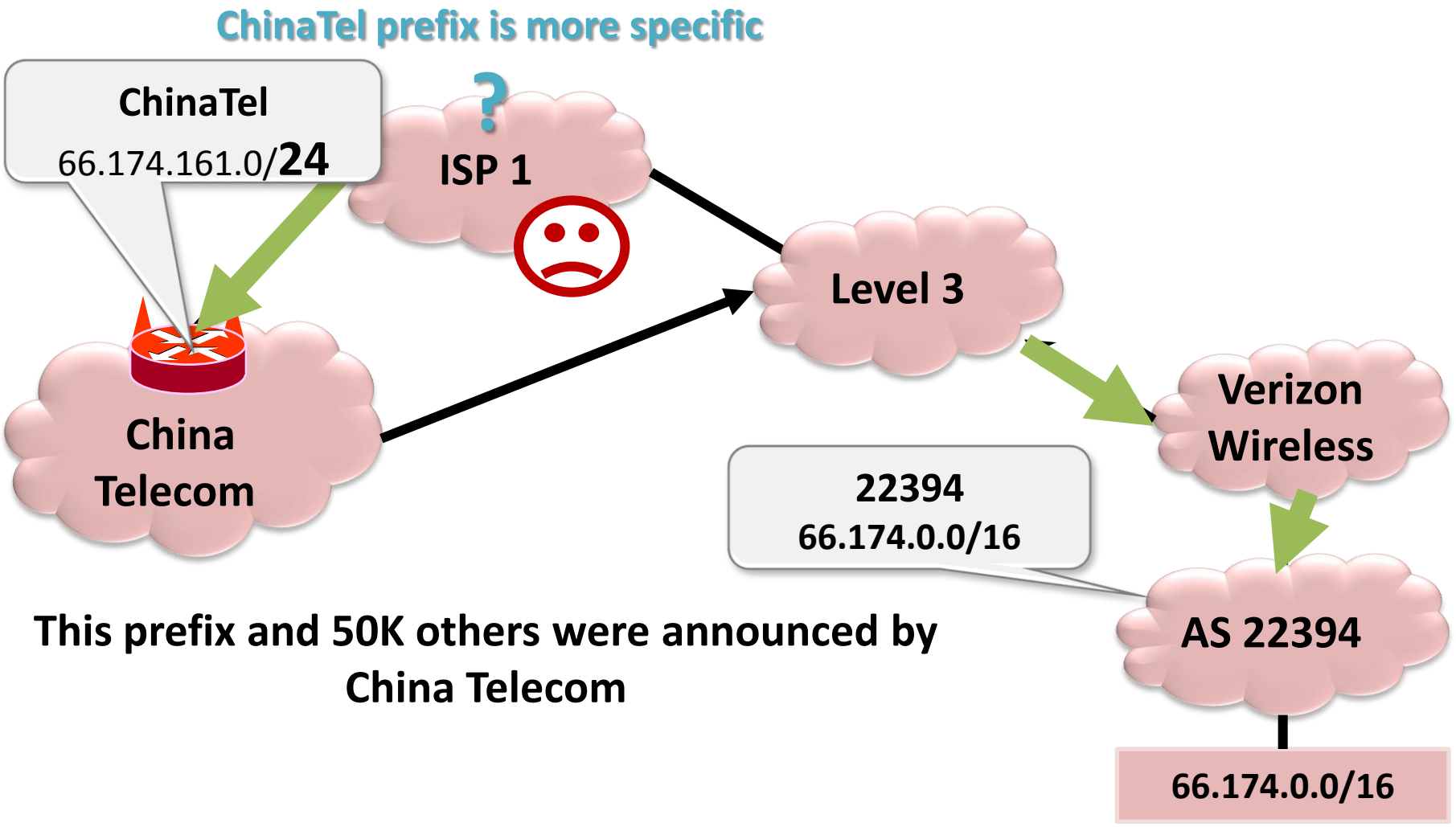
This prefix and 50K others were announced by China Telecom

BGP (Border Gateway Protocol) refresher

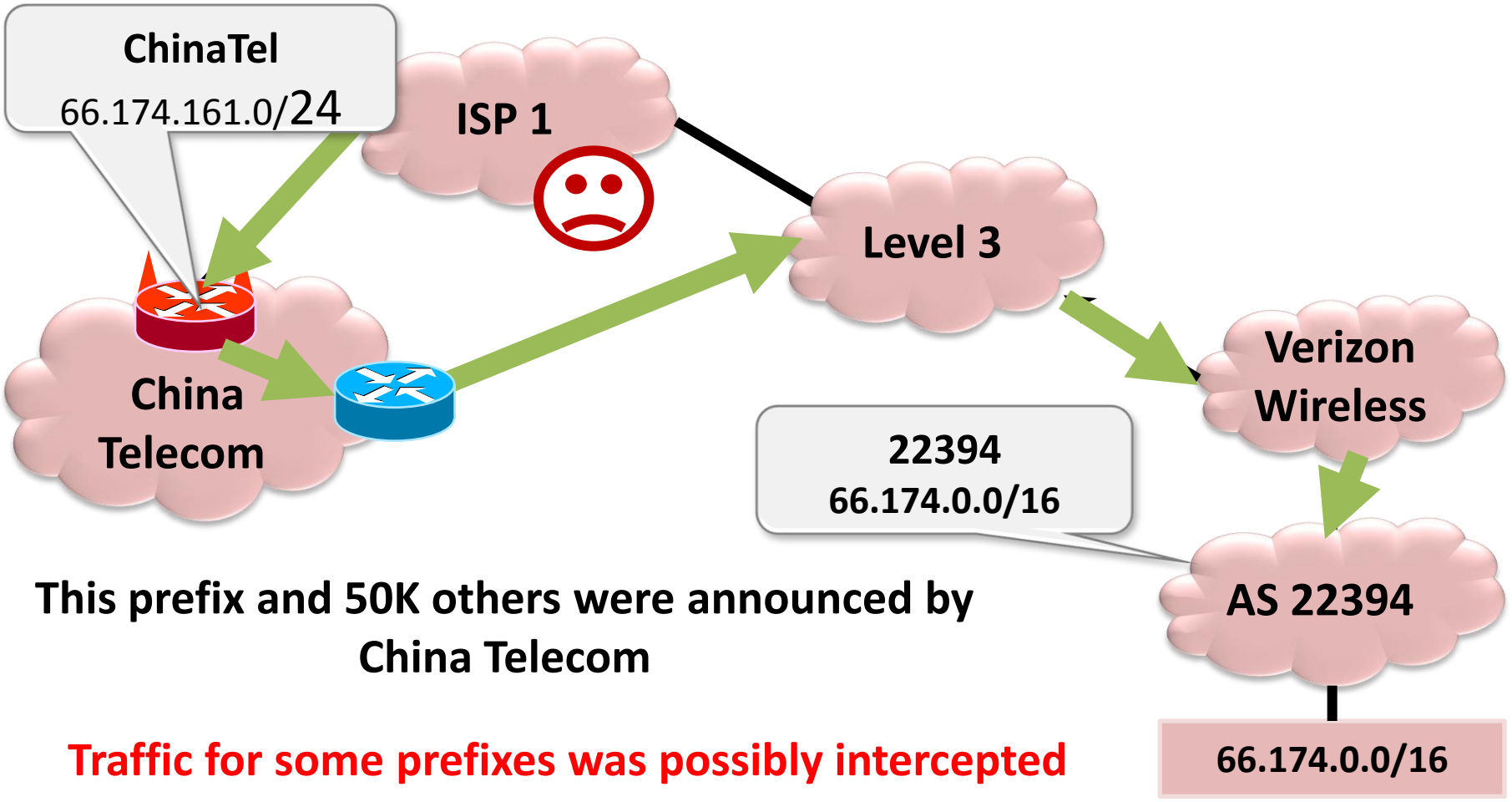


This prefix and 50K others were announced by China Telecom

BGP (Border Gateway Protocol) refresher



BGP (Border Gateway Protocol) refresher

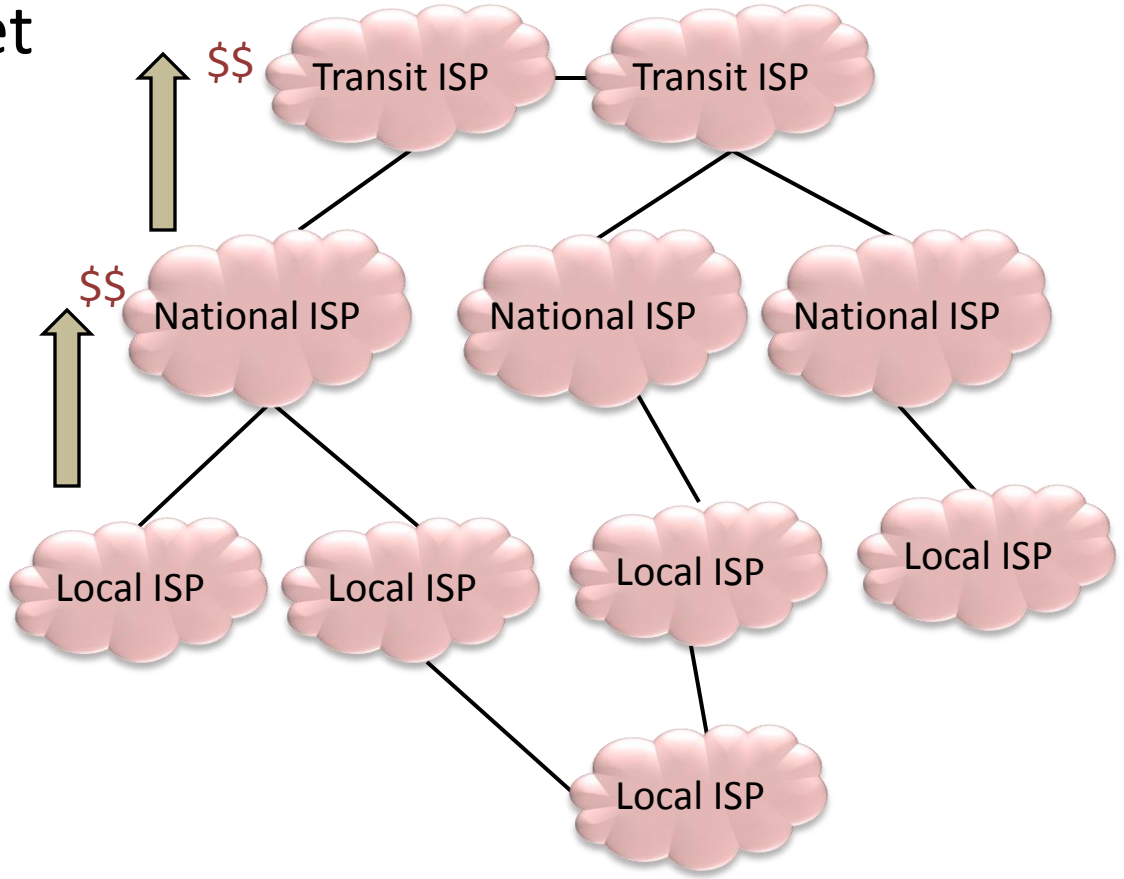


This prefix and 50K others were announced by China Telecom

Traffic for some prefixes was possibly intercepted

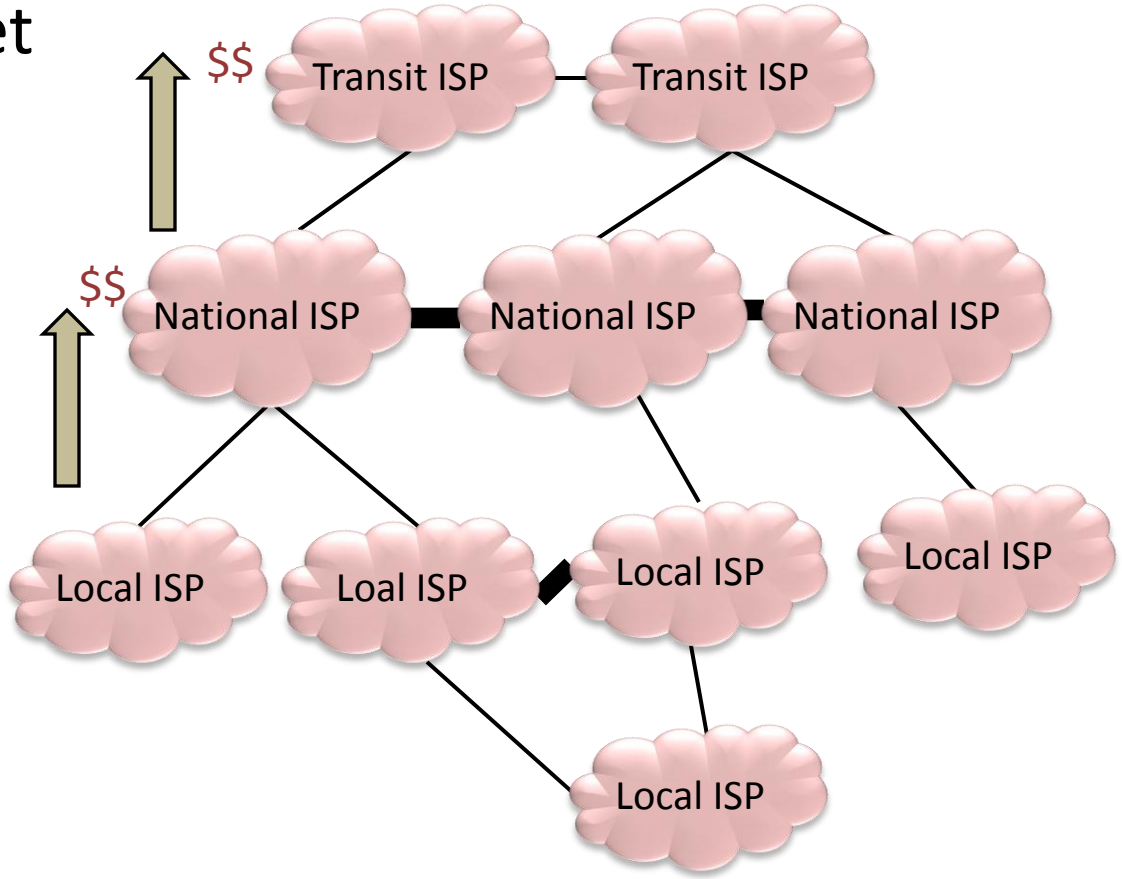
BGP routing policies: Business relationships

- Heirarchical Internet structure



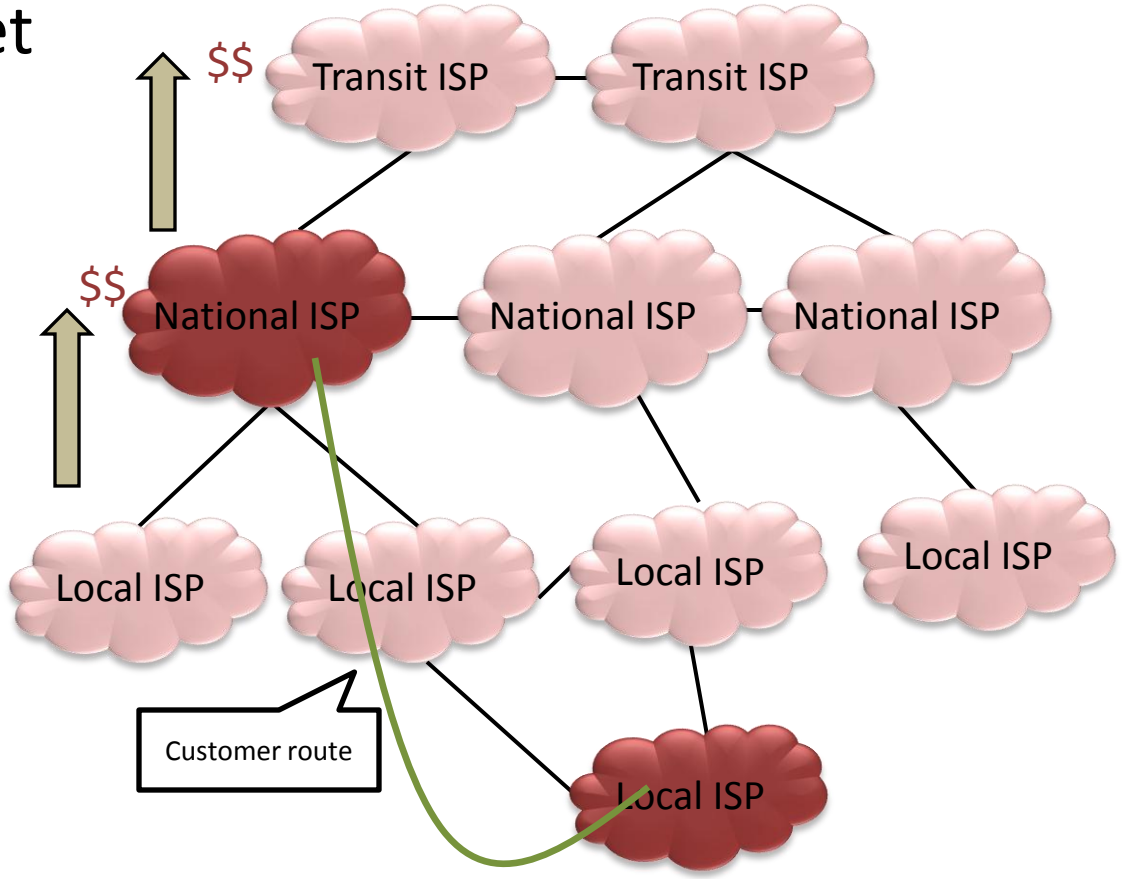
BGP routing policies: Business relationships

- Heirarchical Internet structure
- Different relationships
  - Customer-Provider
  - Peer-Peer



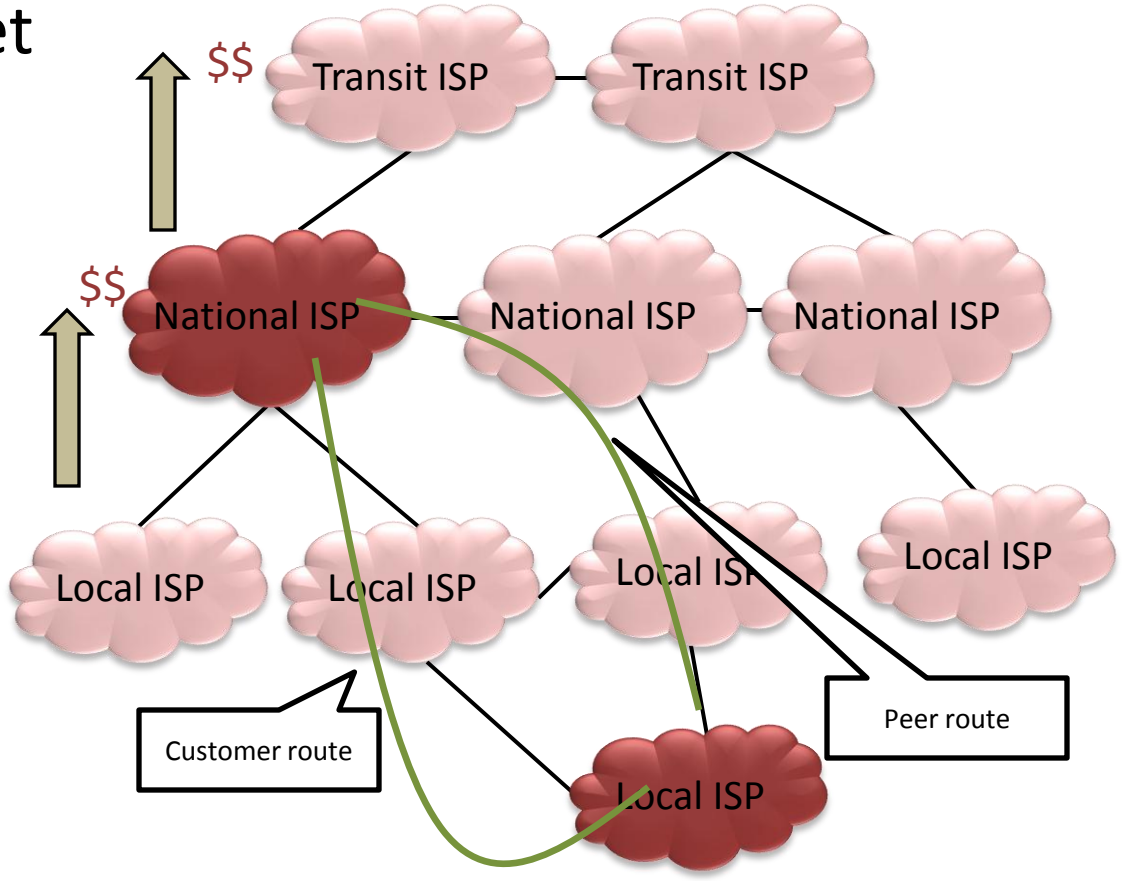
BGP routing policies: Business relationships

- Heirarchical Internet structure
- Different relationships
  - Customer-Provider
  - Peer-Peer



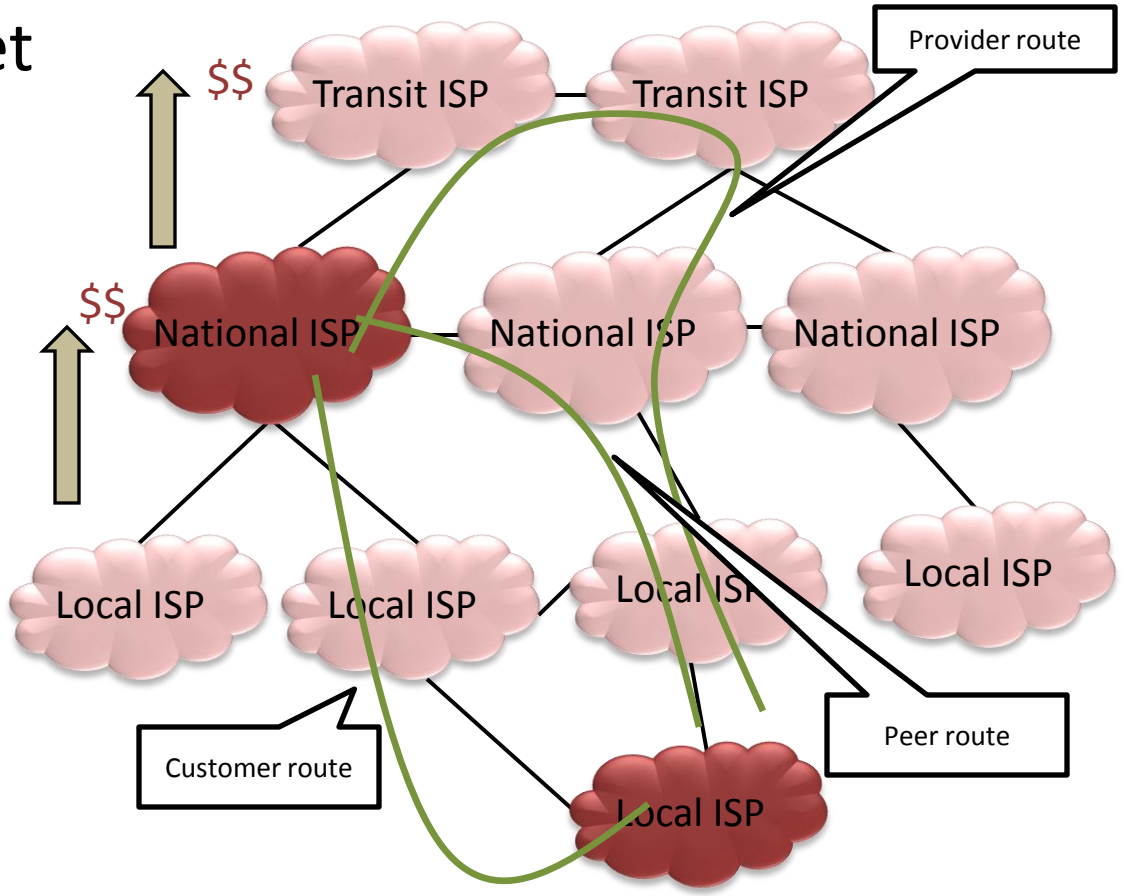
BGP routing policies: Business relationships

- Heirarchical Internet structure
- Different relationships
  - Customer-Provider
  - Peer-Peer



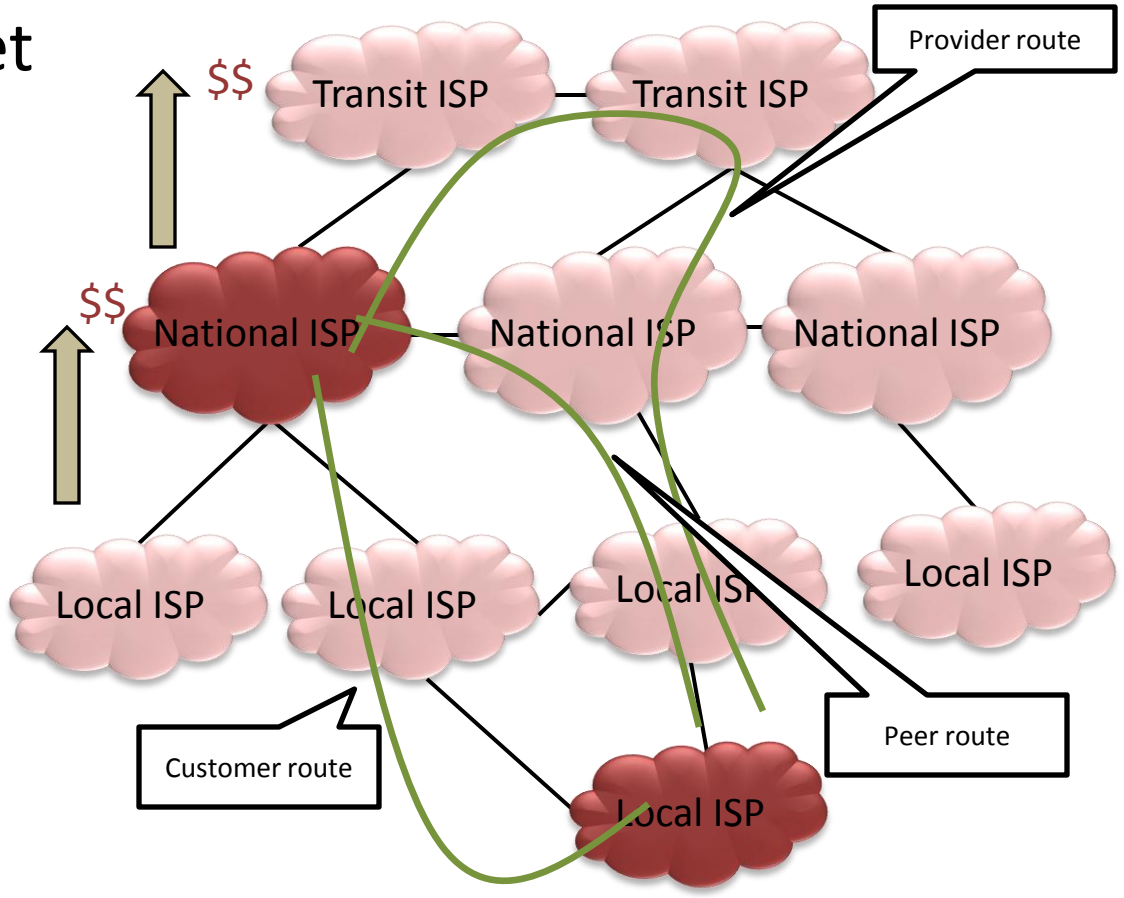
BGP routing policies: Business relationships

- Heirarchical Internet structure
- Different relationships
  - Customer-Provider
  - Peer-Peer



BGP routing policies: Business relationships

- Heirarchical Internet structure
- Different relationships
  - Customer-Provider
  - Peer-Peer
- Preference order
  - Customer route (high)
  - Peer route
  - Provider route (low)

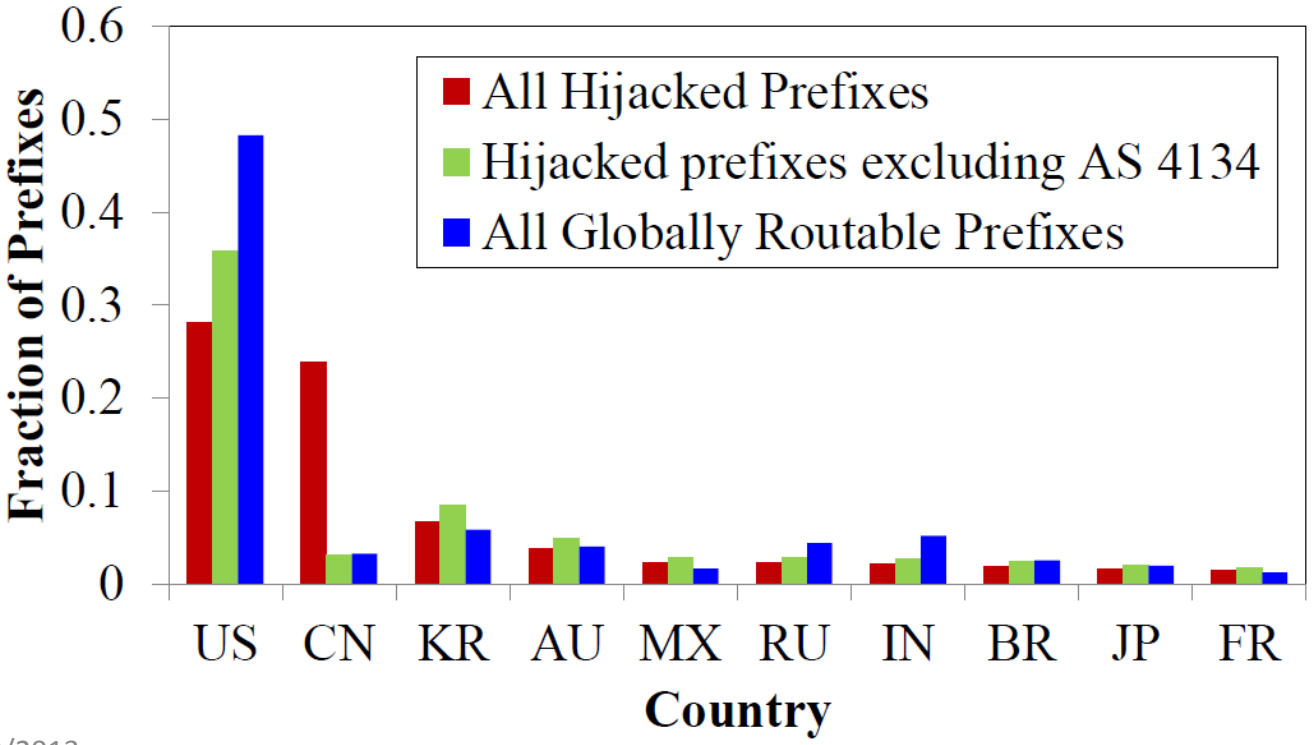


Analysis outline

- Prefix hijack analysis
  - Country-based analysis
- Subprefix hijack analysis
- Interception analysis
  - Reasons for interception

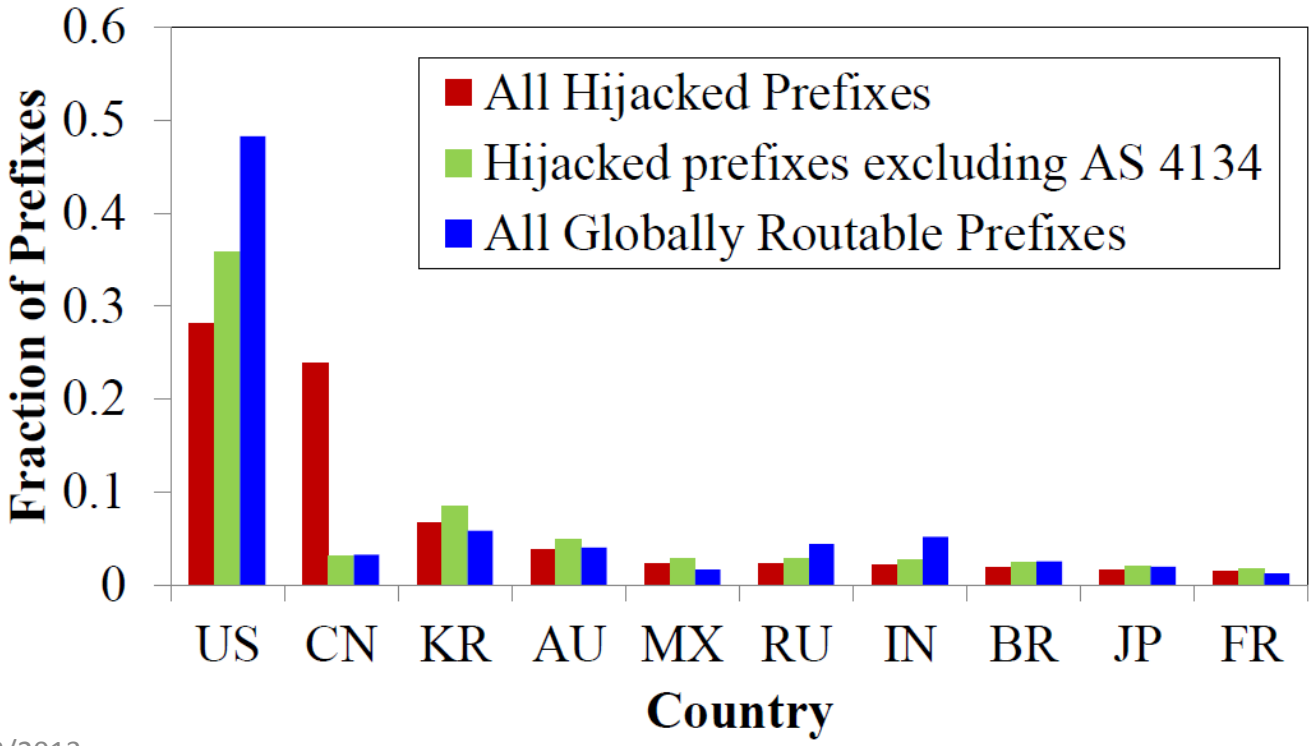
Country-based analysis

- Was any country targeted?
- Geographic distribution of prefixes



Country-based analysis

Distribution of hijacked prefixes do not deviate from global distribution of prefixes



Subprefix hijack analysis

- 21% (9,082) prefixes longer than existing prefixes at all six Routeviews monitors
- 95% of this prefixes belong to China Telecom
- <1% (86) prefixes subprefix hijacked excluding the top-3 ASes in table

Subprefix Hijacks	
Prefixes	Organization
8,614	China Telecom (AS 4134)
371	China Educ/Research (AS 4538)
11	China Telecom (AS 38283)
9	Telecom Holding (AS 34590)
4	Cisco Systems (AS 109)

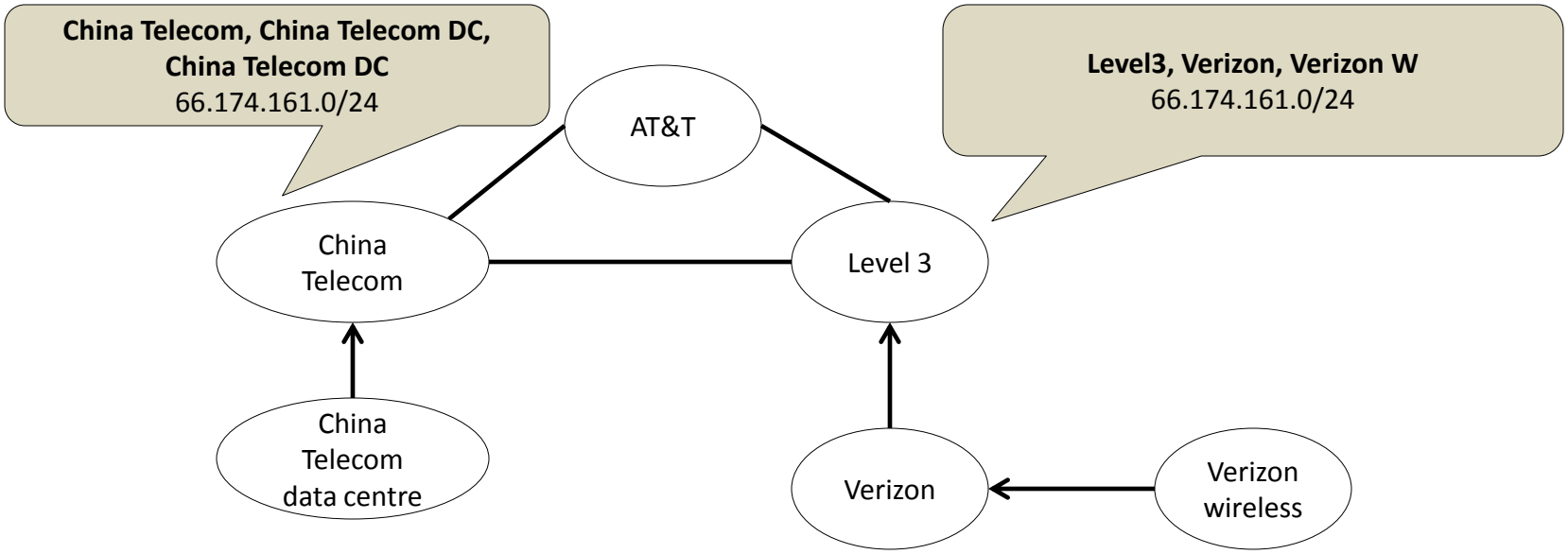
Subprefix hijack analysis

No evidence for intentional subprefix hijacking

Subprefix Hijacks	
Prefixes	Organization
8,614	China Telecom (AS 4134)
371	China Educ/Research (AS 4538)
11	China Telecom (AS 38283)
9	Telecom Holding (AS 34590)
4	Cisco Systems (AS 109)

How did interception occur?

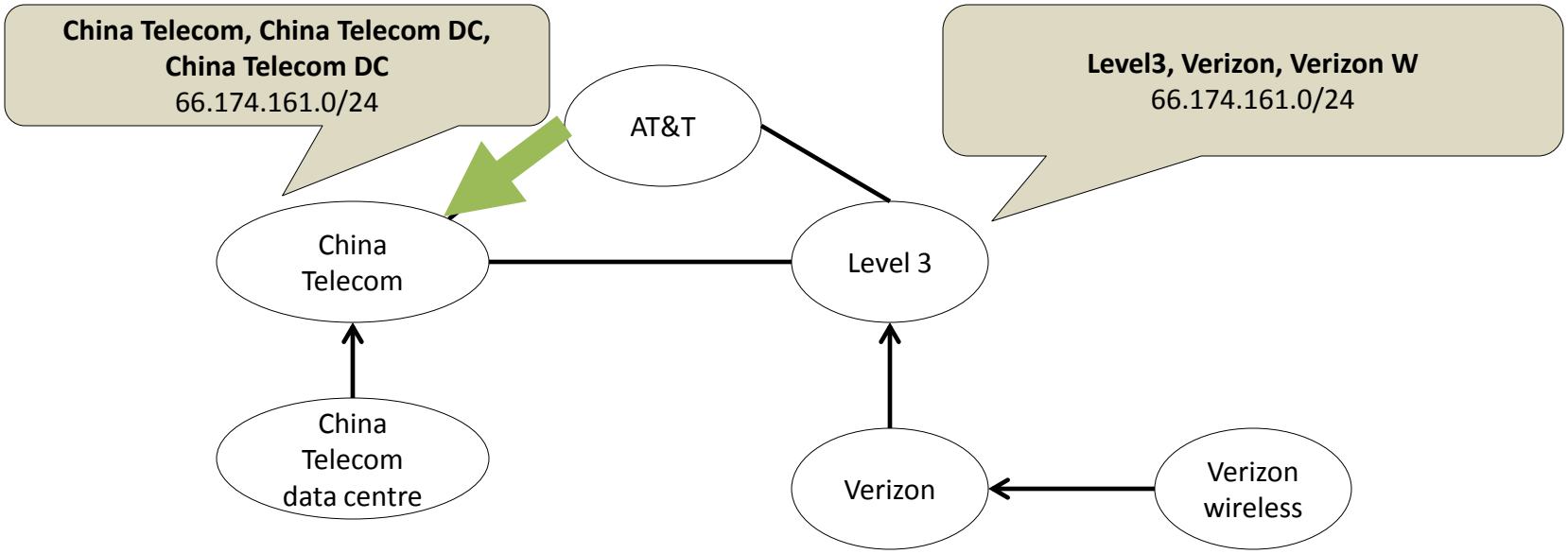
Two required routing decisions for traffic interception:



How did interception occur?

Two required routing decisions for traffic interception:

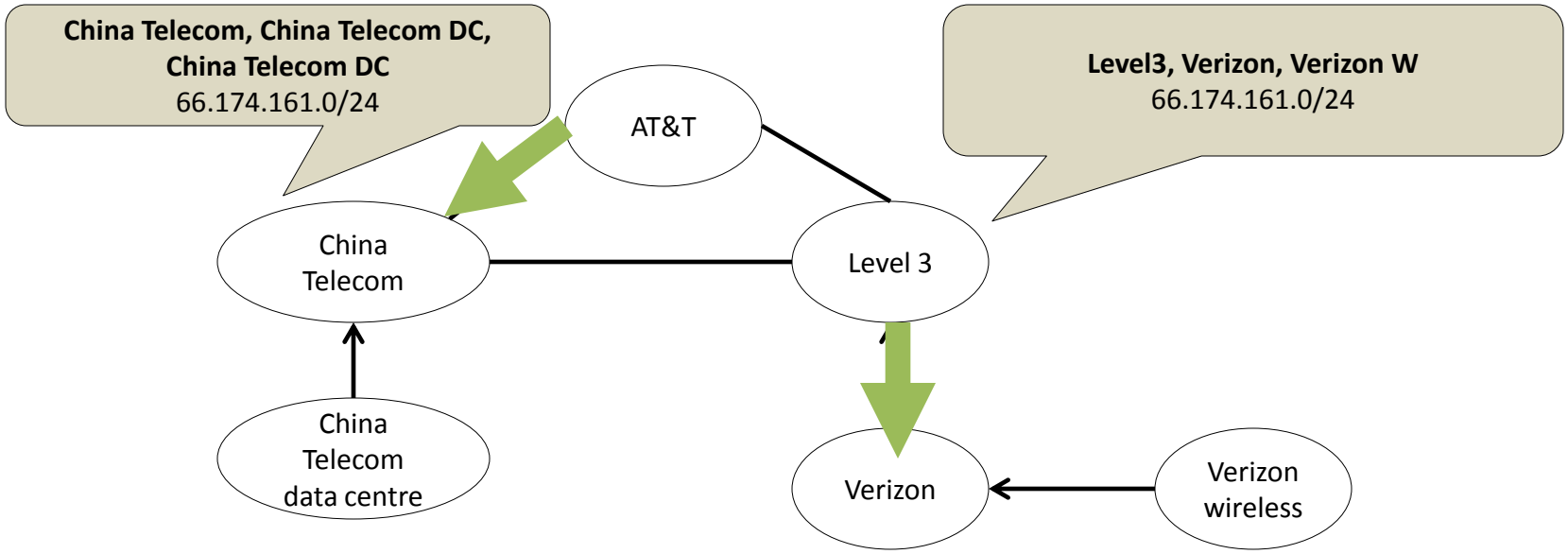
1. A neighbor routes to China Telecom for hijacked prefix



How did interception occur?

Two required routing decisions for traffic interception:

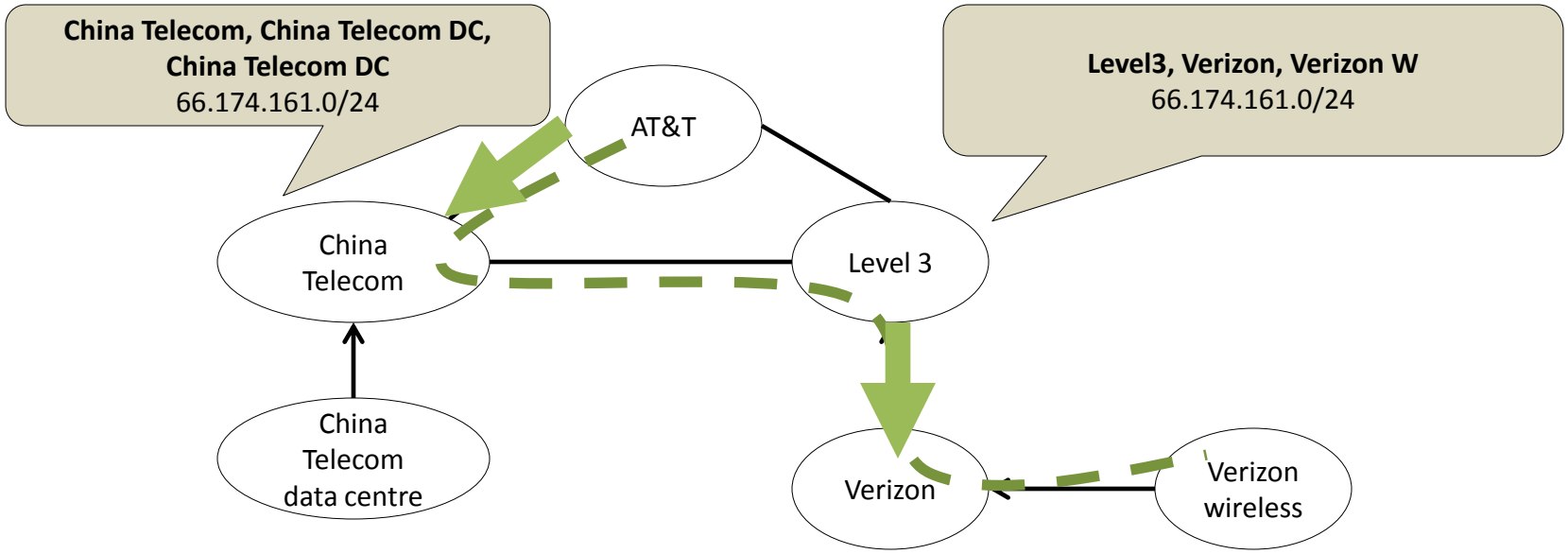
1. A neighbor routes to China Telecom for hijacked prefix
2. Another neighbor does not do so



How did interception occur?

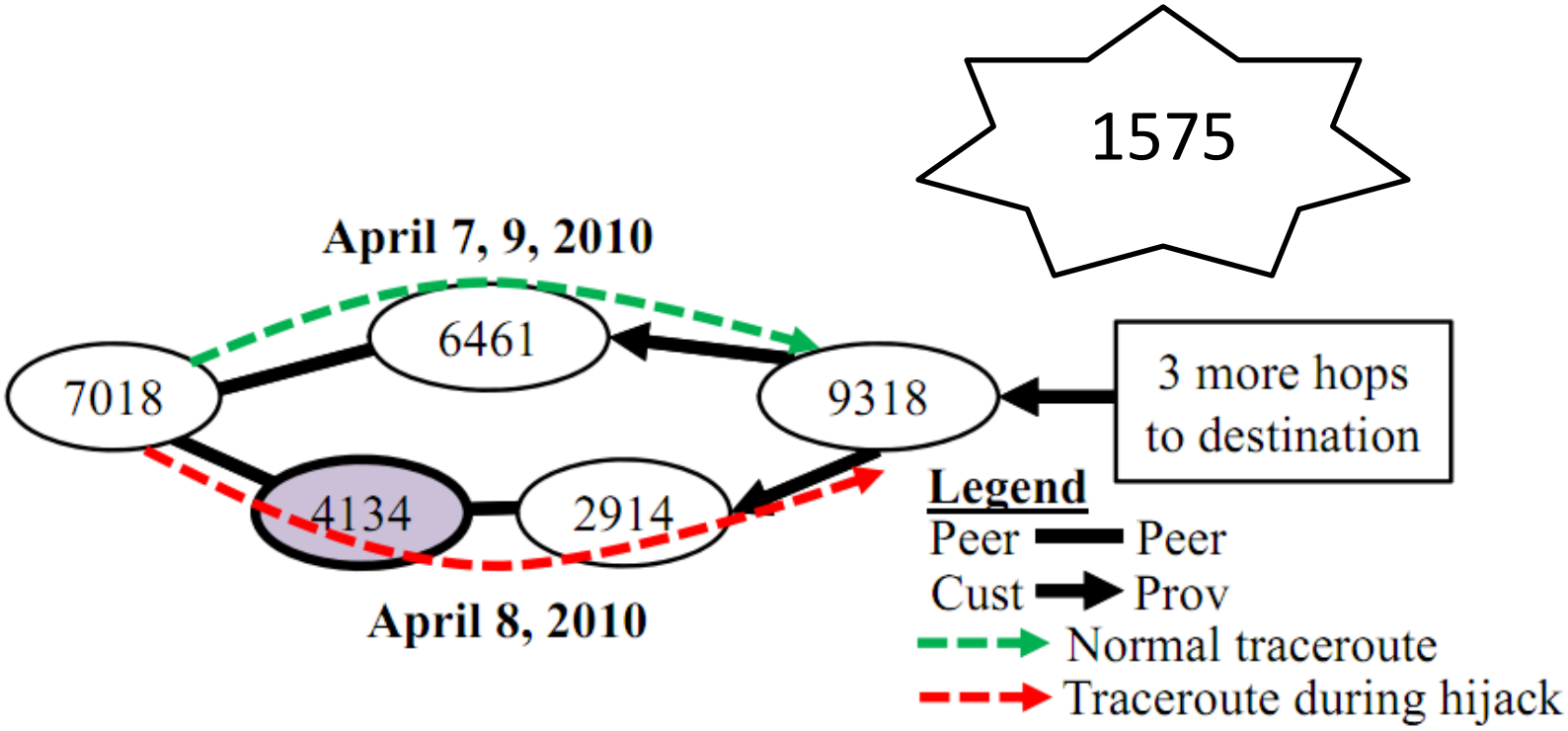
Two required routing decisions for traffic interception:

1. A neighbor routes to China Telecom for hijacked prefix
2. Another neighbor does not do so



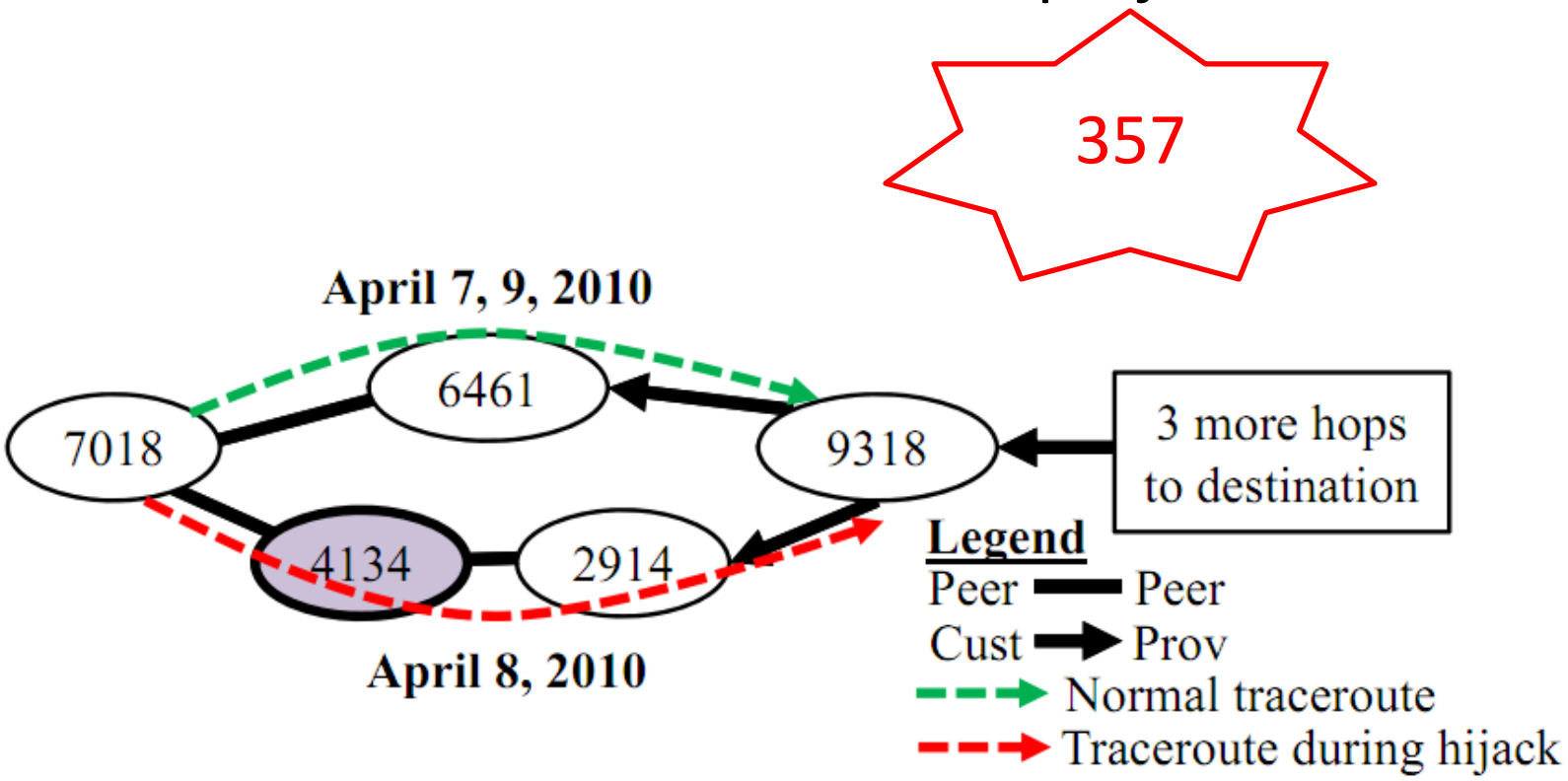
Interception analysis

- Identification of interception instances
- Used traceroute data from iPlane project



Interception analysis

- Identification of interception instances
- Used traceroute data from iPlane project



Interception analysis

Reasons for neighbors not choosing 4134

Reason	# of traceroutes	% of traceroutes
Had a customer path	139	39%
Had a shorter path	193	54%
Had an equally good path	18	5%
Other	7	2%

Interception analysis:

Reasons for neighbors not choosing 4134

Reason	# of traceroutes	% of traceroutes
Had a customer path	139	39%
Had a shorter path	193	54%
Had an equally good path	18	5%
Other	7	2%

- Routing policies and business relationships resulted in interception
- Accidental interception possible

Conclusion and discussion

- Characterized the China Telecom incident
  - Accidental interception possible
  - Sheds light on properties of announced prefixes
  - Supports the conclusion that incident was a leak of random prefixes
  - However, it does not rule out malicious intent
- Our study highlights
  - Challenges of diagnosing routing incidents
  - Importance of public and rich available data

Linköping University

expanding reality

Questions?

Rahul Hiran

rahul.hiran@liu.se