Does Scale, Size, and Locality Matter? Evaluation of Collaborative BGP Security Mechanisms

Rahul Hiran, Niklas Carlsson, Nahid Shahmehri

Linköping University, Sweden

Routing attacks increasingly common

100.127.0.0/24	AS13489	EPM Telecomunicaciones S.A. E.S.P.,CO	100.64.0.0 - 100.127.255.255
102.2.88.0/22	AS38456	PACTEL-AS-AP Pacific Teleports. ,AU	102.0.0.0 - 102.255.255.255
103.6.108.0/22	AS55526	NOIDASOFTWARETECHNOLOGYPARK-IN NOIDA Software Technology Park Ltd,IN	103.6.108.0 - 103.6.111.255
103.9.108.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP	103.9.107.0 - 103.9.111.255
103.15.92.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP	103.15.92.0 - 103.15.95.255
103.18.76.0/22	AS18097	DCN D.C.N. Corporation,JP	103.18.76.0 - 103.18.83.255
103.18.248.0/22	AS18097	DCN D.C.N. Corporation,JP	103.18.248.0 - 103.18.251.255
103.19.0.0/22	AS18097	DCN D.C.N. Corporation,JP	103.19.0.0 - 103.19.3.255
103.20.100.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN	103.20.100.0 - 103.20.103.255
103.20.101.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN	103.20.100.0 - 103.20.103.255
103.21.4.0/22	AS12182	INTERNAP-2BLK - Internap Network Services Corporation,US	103.21.4.0 - 103.21.7.255
103.26.116.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.26.116.0 - 103.26.119.255
103.228.132.0/22	AS4826	VOCUS-BACKBONE-AS Vocus Connect International Backbone,AU	103.228.133.0 - 103.228.135.255
103.248.88.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP	103.248.88.0 - 103.248.91.255
103.248.220.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.248.220.0 - 103.248.223.255
103.249.8.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP	103.249.8.0 - 103.249.11.255
103.250.0.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.250.0.0 - 103.250.3.255
116.206.72.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255
116.206.85.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255
116.206.103.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255

Each day there are large numbers of bogus route announcements

- e.g., cidr-report.org

Among these we have seen many serious attacks ...

Routing attacks increasingly common

100.127.0.0/24	AS13489	EPM Telecomunicaciones S.A. E.S.P.,CO	100.64.0.0 - 100.127.255.255
102.2.88.0/22	AS38456	PACTEL-AS-AP Pacific Teleports. ,AU	102.0.0.0 - 102.255.255.255
103.6.108.0/22	AS55526	NOIDASOFTWARETECHNOLOGYPARK-IN NOIDA Software Technology Park Ltd,IN	103.6.108.0 - 103.6.111.255
103.9.108.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP	103.9.107.0 - 103.9.111.255
103.15.92.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP	103.15.92.0 - 103.15.95.255
103.18.76.0/22	AS18097	DCN D.C.N. Corporation,JP	103.18.76.0 - 103.18.83.255
103.18.248.0/22	AS18097	DCN D.C.N. Corporation,JP	103.18.248.0 - 103.18.251.255
103.19.0.0/22	AS18097	DCN D.C.N. Corporation,JP	103.19.0.0 - 103.19.3.255
103.20.100.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN	103.20.100.0 - 103.20.103.255
103.20.101.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN	103.20.100.0 - 103.20.103.255
103.21.4.0/22	AS12182	INTERNAP-2BLK - Internap Network Services Corporation,US	103.21.4.0 - 103.21.7.255
103.26.116.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.26.116.0 - 103.26.119.255
103.228.132.0/22	AS4826	VOCUS-BACKBONE-AS Vocus Connect International Backbone,AU	103.228.133.0 - 103.228.135.255
103.248.88.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP	103.248.88.0 - 103.248.91.255
103.248.220.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.248.220.0 - 103.248.223.255
103.249.8.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP	103.249.8.0 - 103.249.11.255
103.250.0.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP	103.250.0.0 - 103.250.3.255
116.206.72.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255
116.206.85.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255
116.206.103.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US	116.206.0.0 - 116.206.255.255

Each day there are large numbers of bogus route announcements

- e.g., cidr-report.org

Among these we have seen many serious attacks ...

Routing attacks increasingly common

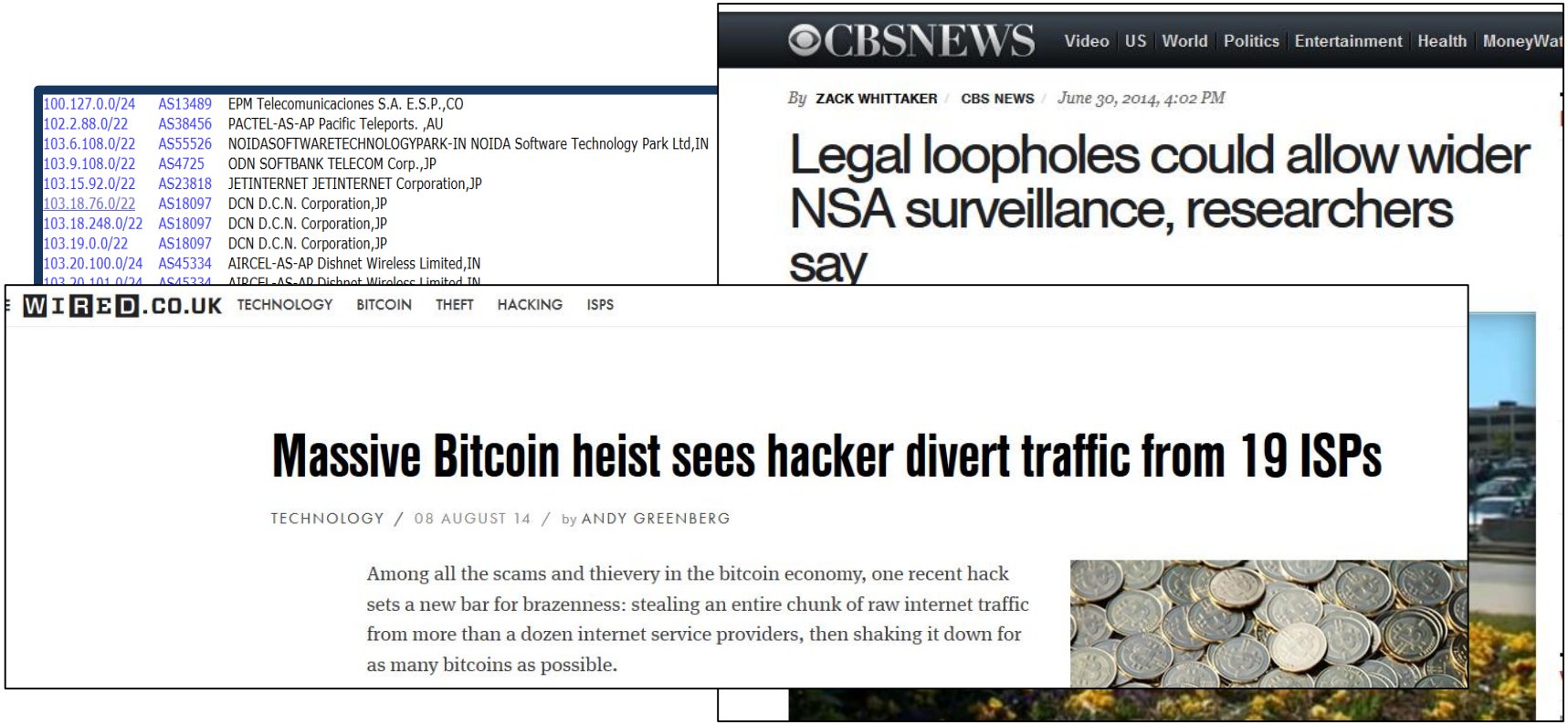
100.127.0.0/24	AS13489	EPM Telecomunicaciones S.A. E.S.P.,CO
102.2.88.0/22	AS38456	PACTEL-AS-AP Pacific Teleports. ,AU
103.6.108.0/22	AS55526	NOIDASOFTWARETECHNOLOGYPARK-IN NOIDA Software Technology Park Ltd,IN
103.9.108.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP
103.15.92.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP
103.18.76.0/22	AS18097	DCN D.C.N. Corporation,JP
103.18.248.0/22	AS18097	DCN D.C.N. Corporation,JP
103.19.0.0/22	AS18097	DCN D.C.N. Corporation,JP
103.20.100.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN
103.20.101.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN
103.21.4.0/22	AS12182	INTERNAP-2BLK - Internap Network Services Corporation,US
103.26.116.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP
103.228.132.0/22	AS4826	VOCUS-BACKBONE-AS Vocus Connect International Backbone,AU
103.248.88.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP
103.248.220.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP
103.249.8.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP
103.250.0.0/22	AS17676	GIGAINFRA Softbank BB Corp.,JP
116.206.72.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US
116.206.85.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US
116.206.103.0/24	AS6461	ABOVENET - Abovenet Communications, Inc,US

Each day there are large numbers of bogus route announcements

- e.g., cidr-report.org

Among these we have seen many serious attacks ...

Routing attacks increasingly common



100.127.0.0/24	AS13489	EPM Telecomunicaciones S.A. E.S.P.,CO
102.2.88.0/22	AS38456	PACTEL-AS-AP Pacific Teleports. ,AU
103.6.108.0/22	AS55526	NOIDASOFTWARETECHNOLOGYPARK-IN NOIDA Software Technology Park Ltd,IN
103.9.108.0/22	AS4725	ODN SOFTBANK TELECOM Corp.,JP
103.15.92.0/22	AS23818	JETINTERNET JETINTERNET Corporation,JP
103.18.76.0/22	AS18097	DCN D.C.N. Corporation,JP
103.18.248.0/22	AS18097	DCN D.C.N. Corporation,JP
103.19.0.0/22	AS18097	DCN D.C.N. Corporation,JP
103.20.100.0/24	AS45334	AIRCEL-AS-AP Dishnet Wireless Limited,IN

CBSNEWS Video US World Politics Entertainment Health MoneyWat

By ZACK WHITTAKER / CBS NEWS / June 30, 2014, 4:02 PM

Legal loopholes could allow wider NSA surveillance, researchers say

WIRED.CO.UK TECHNOLOGY BITCOIN THEFT HACKING ISPS

Massive Bitcoin heist sees hacker divert traffic from 19 ISPs

TECHNOLOGY / 08 AUGUST 14 / by ANDY GREENBERG

Among all the scams and thievery in the bitcoin economy, one recent hack sets a new bar for brazenness: stealing an entire chunk of raw internet traffic from more than a dozen internet service providers, then shaking it down for as many bitcoins as possible.

Each day there are large numbers of bogus route announcements

- e.g., cidr-report.org

Among these we have seen many serious attacks ...

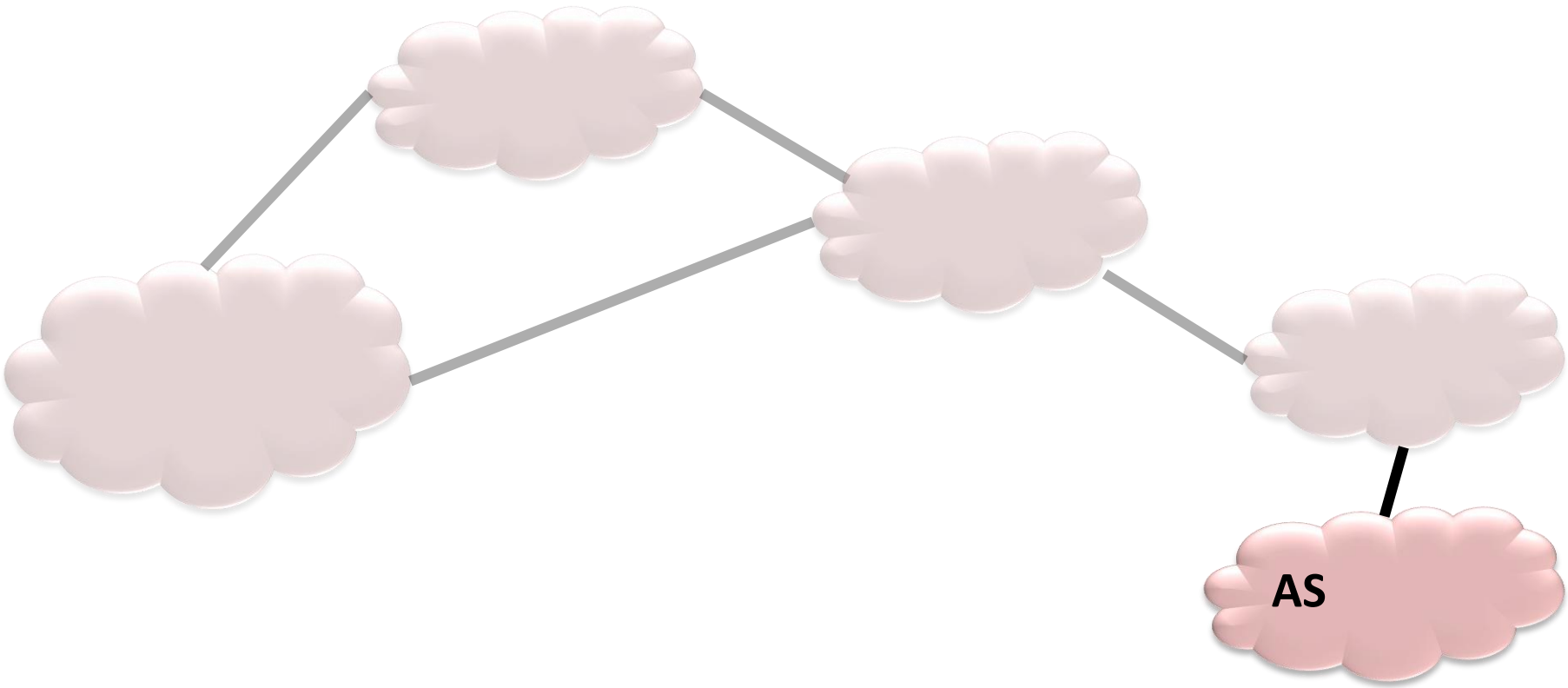
Routing attacks increasingly common

Each day there are large numbers of bogus route announcements

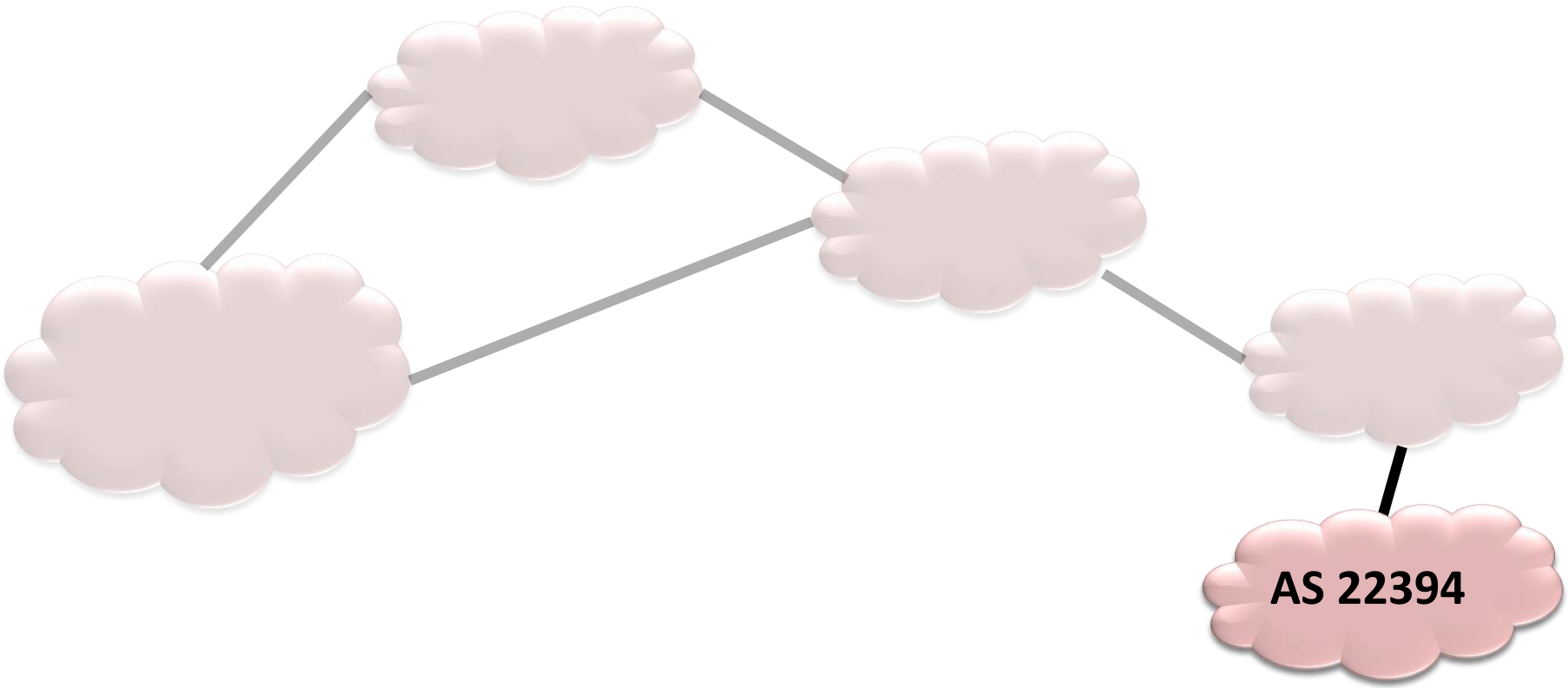
- e.g., cidr-report.org

Among these we have seen many serious attacks ...

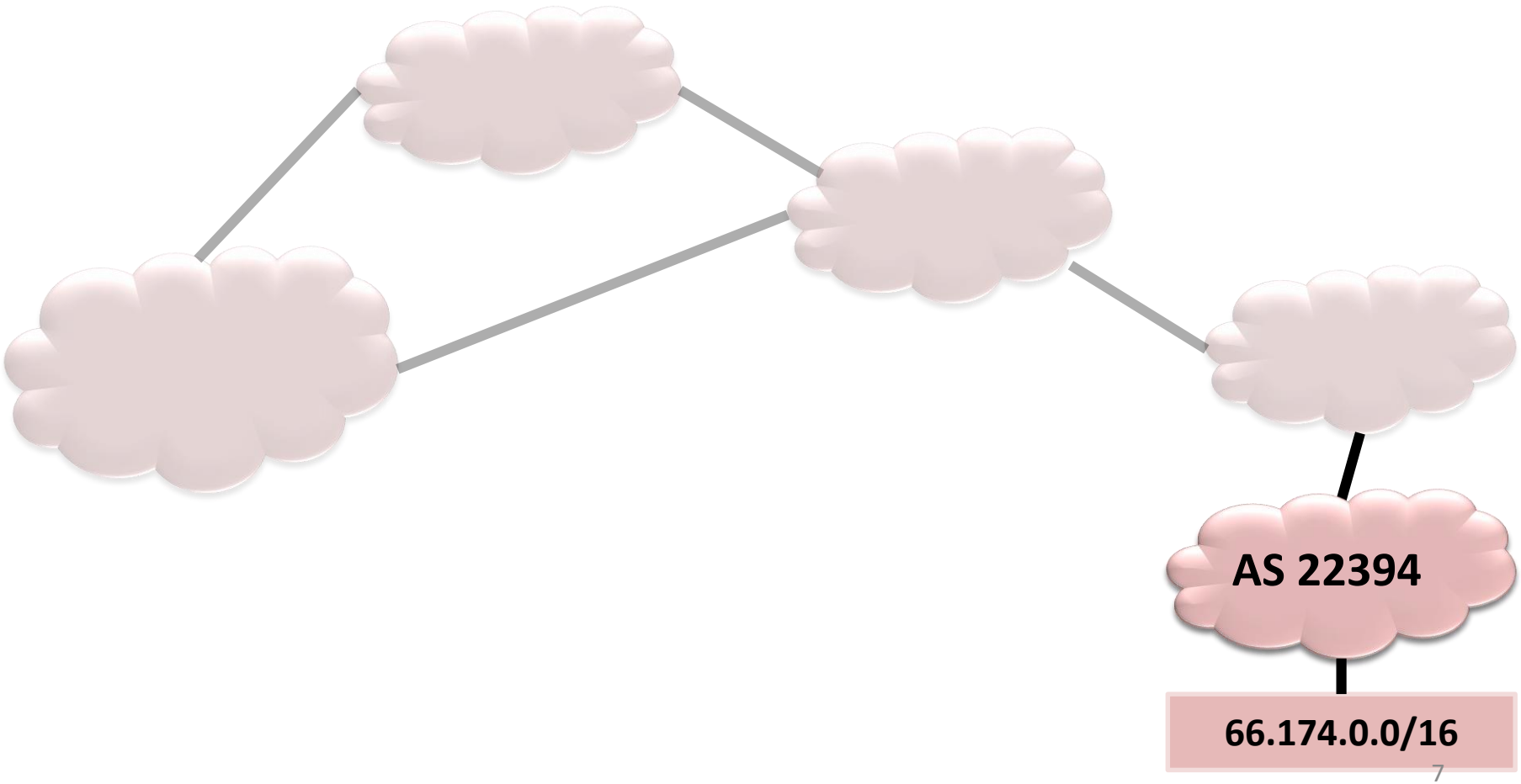
BGP refresher



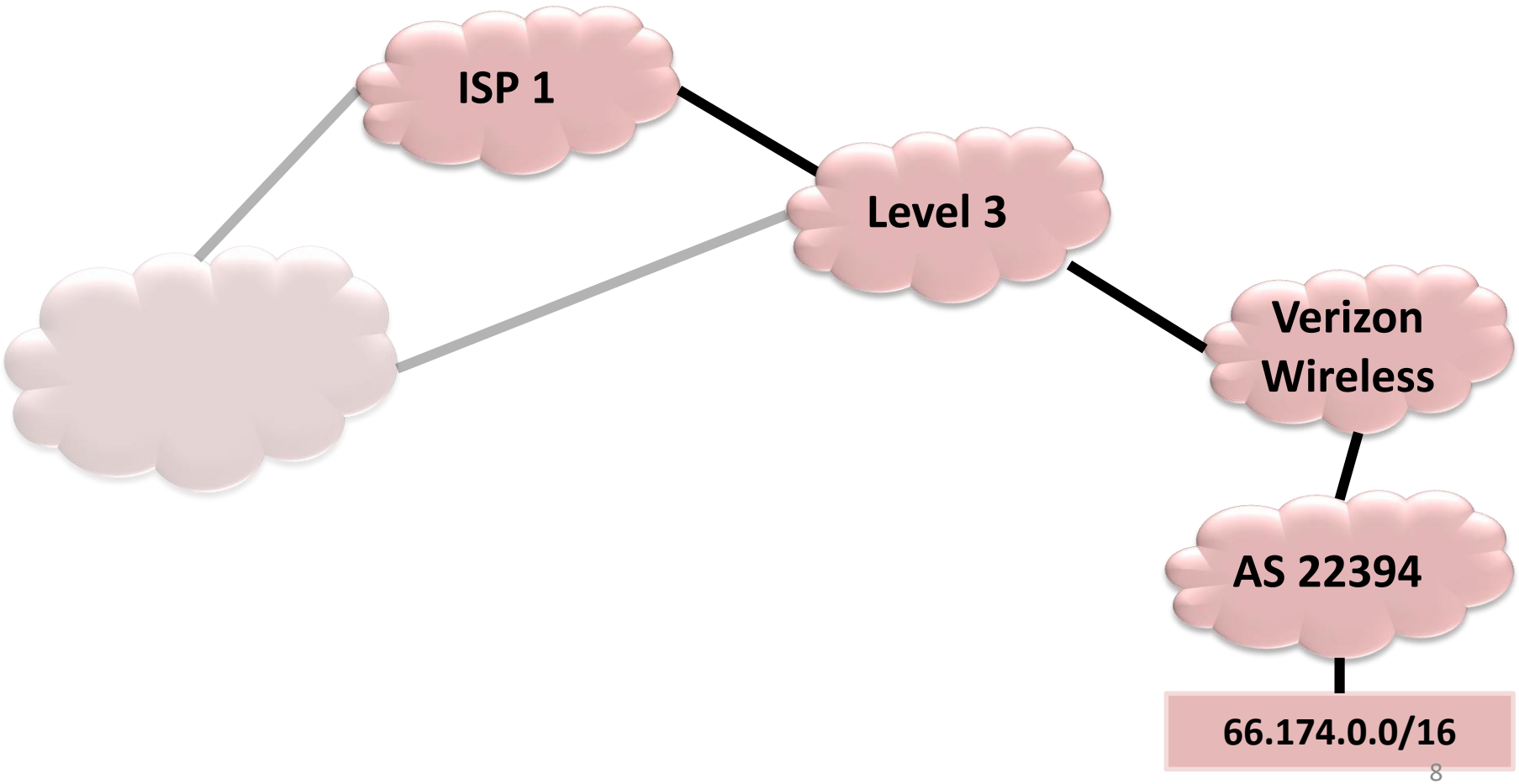
BGP refresher



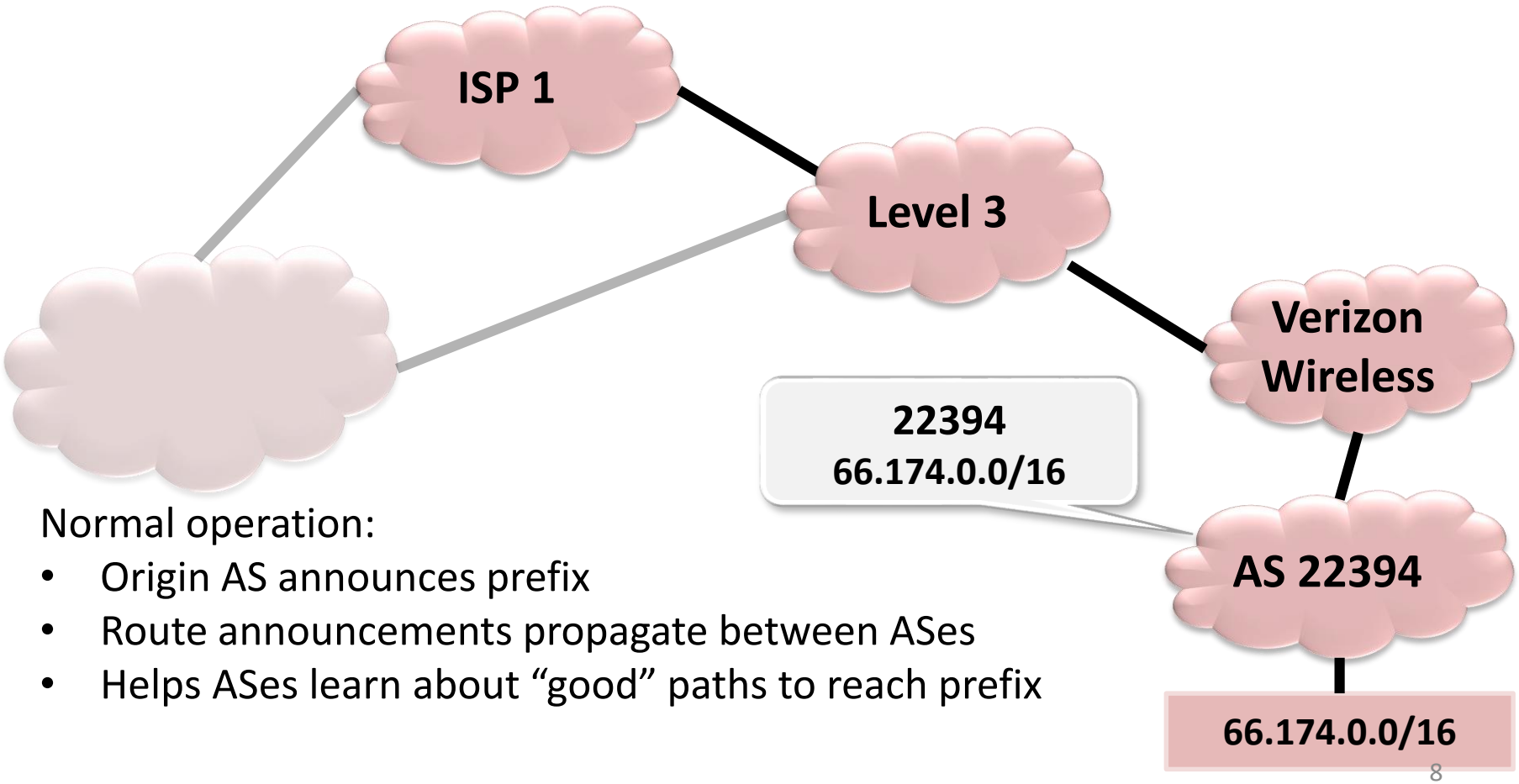
BGP refresher



BGP refresher



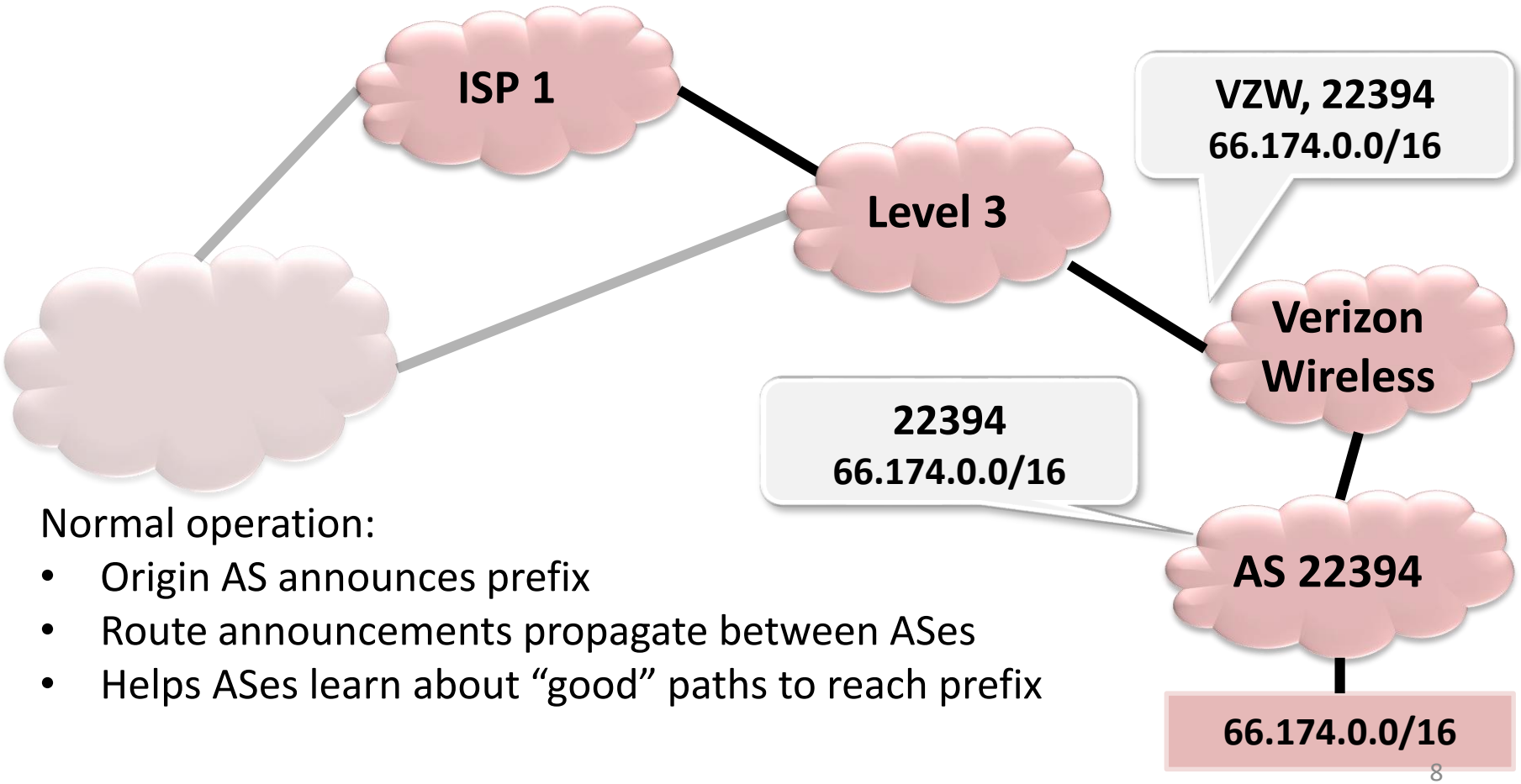
BGP refresher



Normal operation:

- Origin AS announces prefix
- Route announcements propagate between ASes
- Helps ASes learn about “good” paths to reach prefix

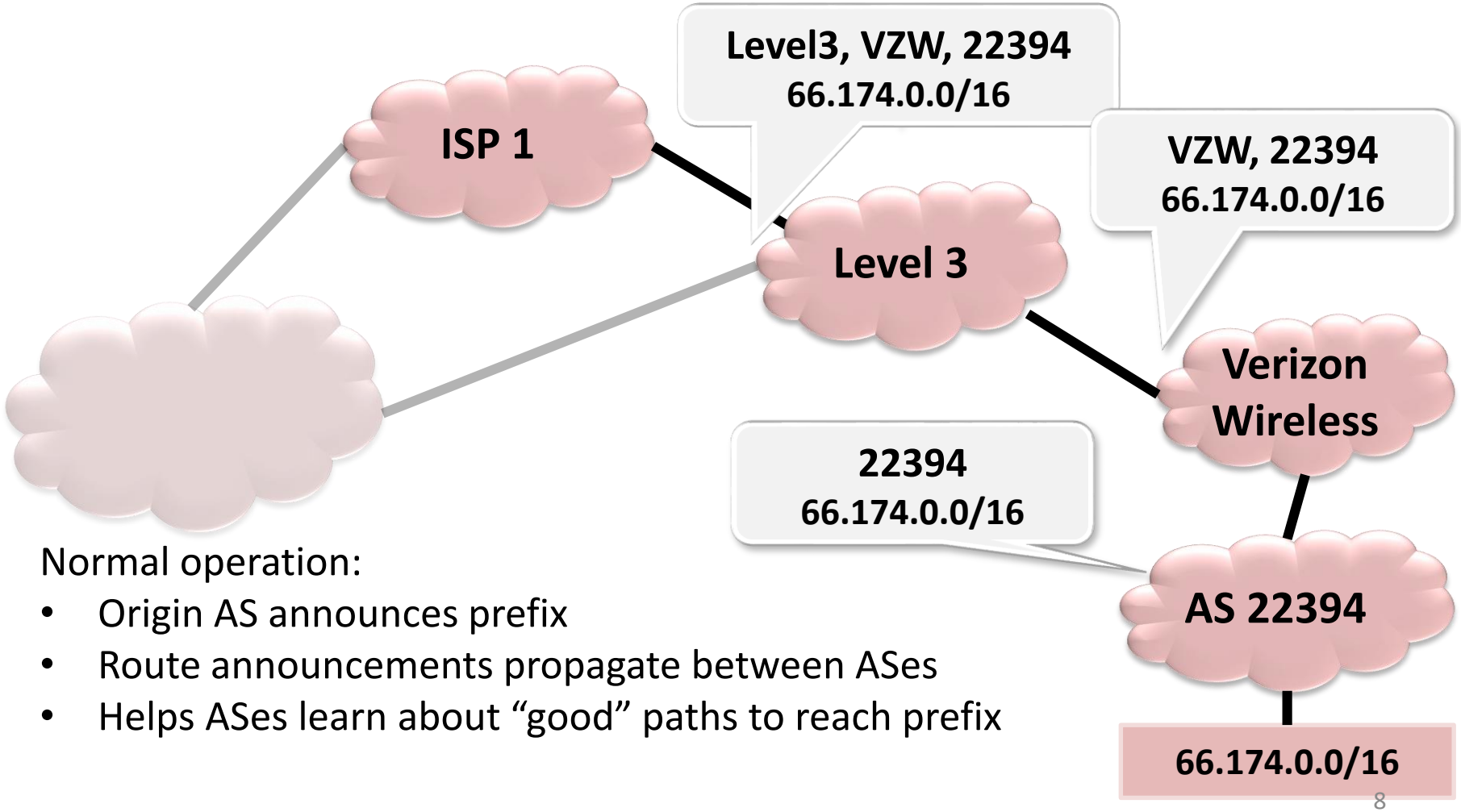
BGP refresher



Normal operation:

- Origin AS announces prefix
- Route announcements propagate between ASes
- Helps ASes learn about “good” paths to reach prefix

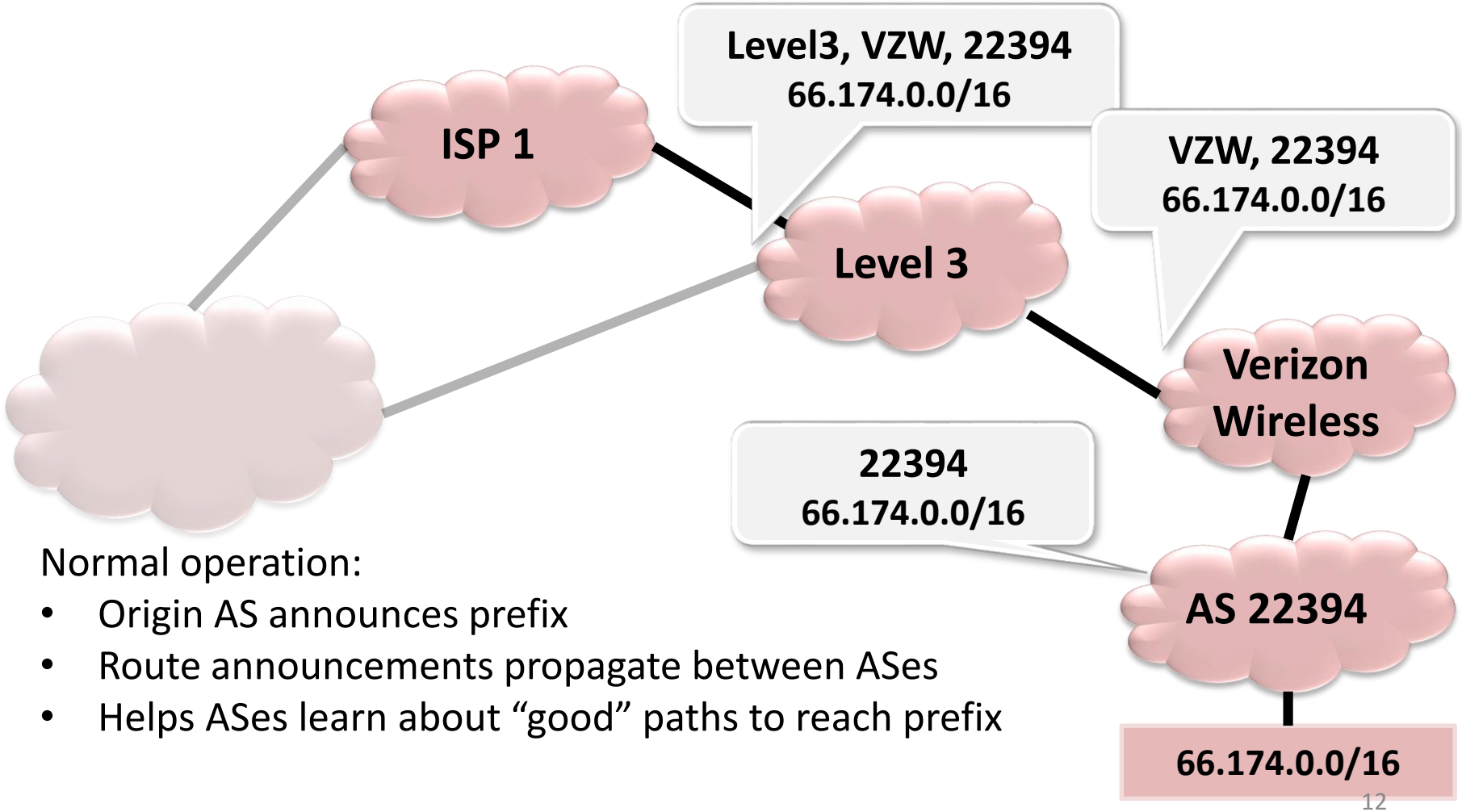
BGP refresher



Normal operation:

- Origin AS announces prefix
- Route announcements propagate between ASes
- Helps ASes learn about “good” paths to reach prefix

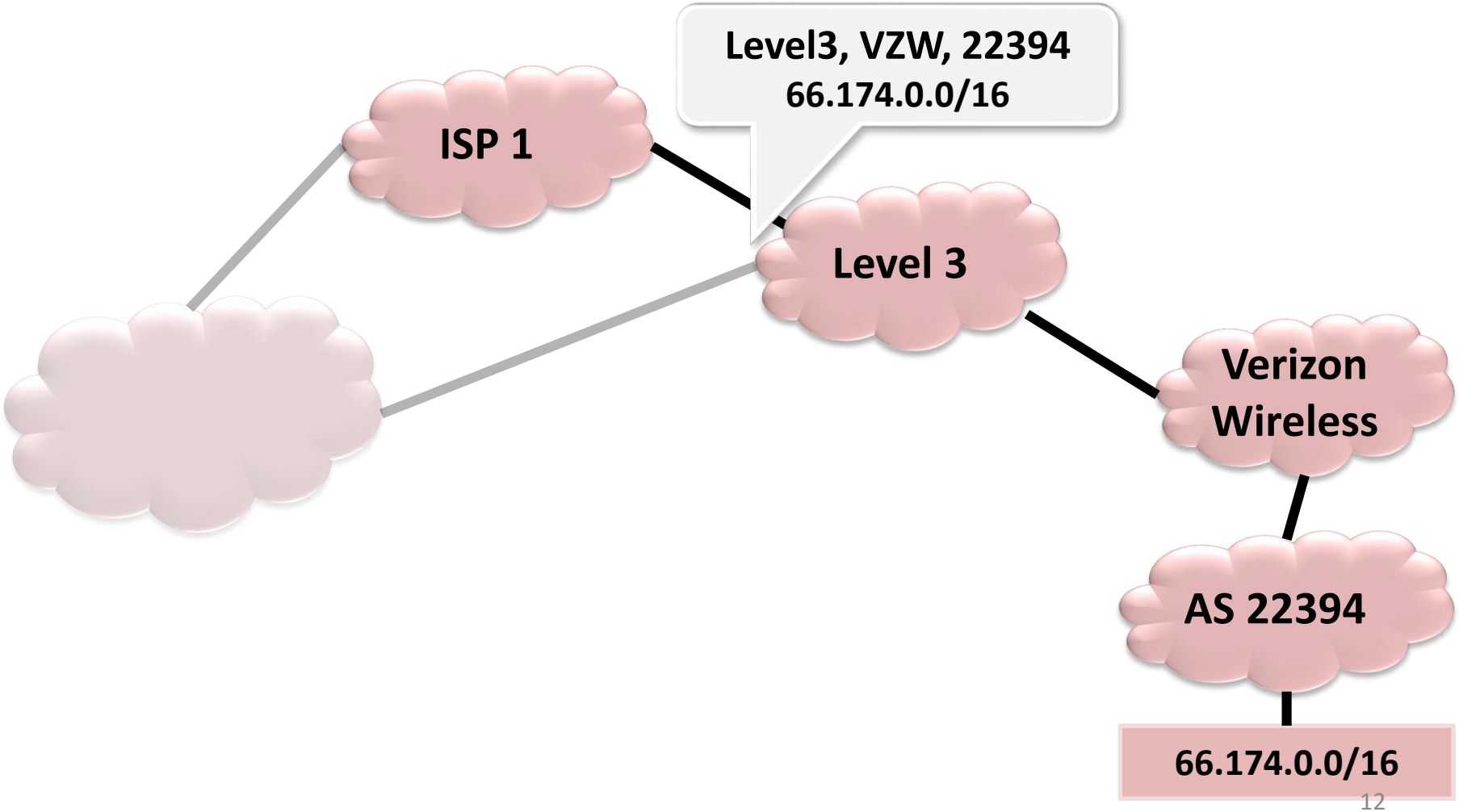
BGP refresher



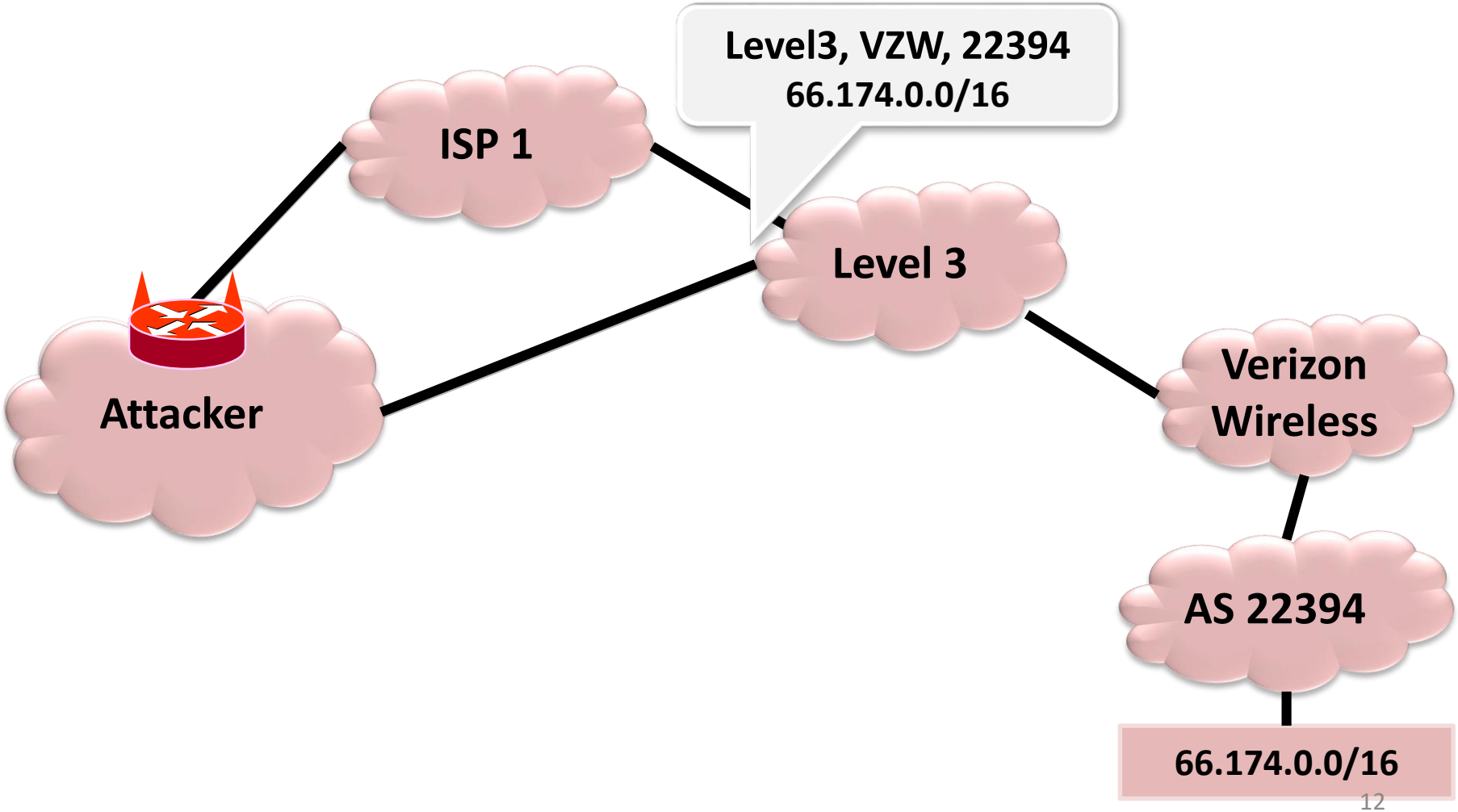
Normal operation:

- Origin AS announces prefix
- Route announcements propagate between ASes
- Helps ASes learn about “good” paths to reach prefix

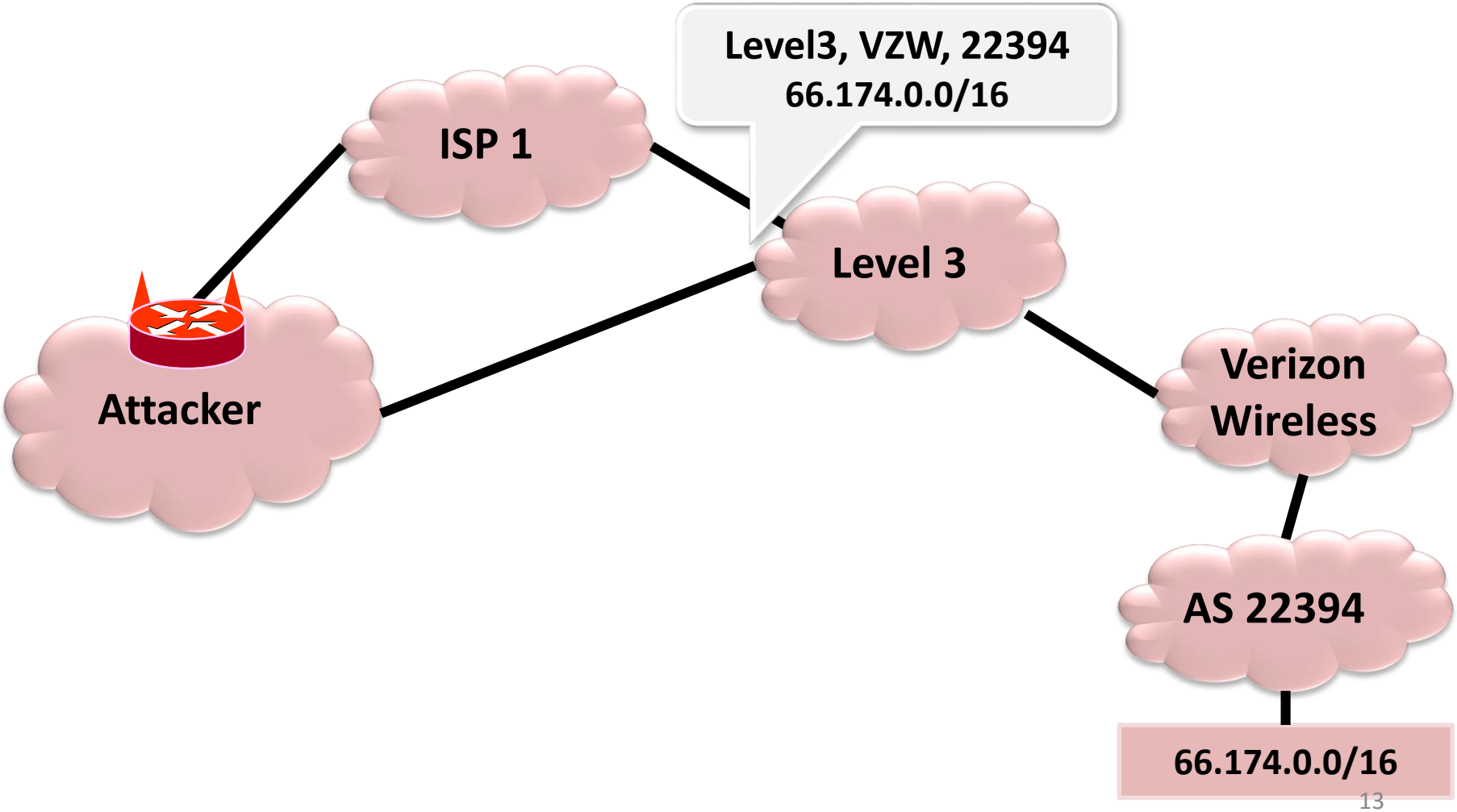
BGP refresher



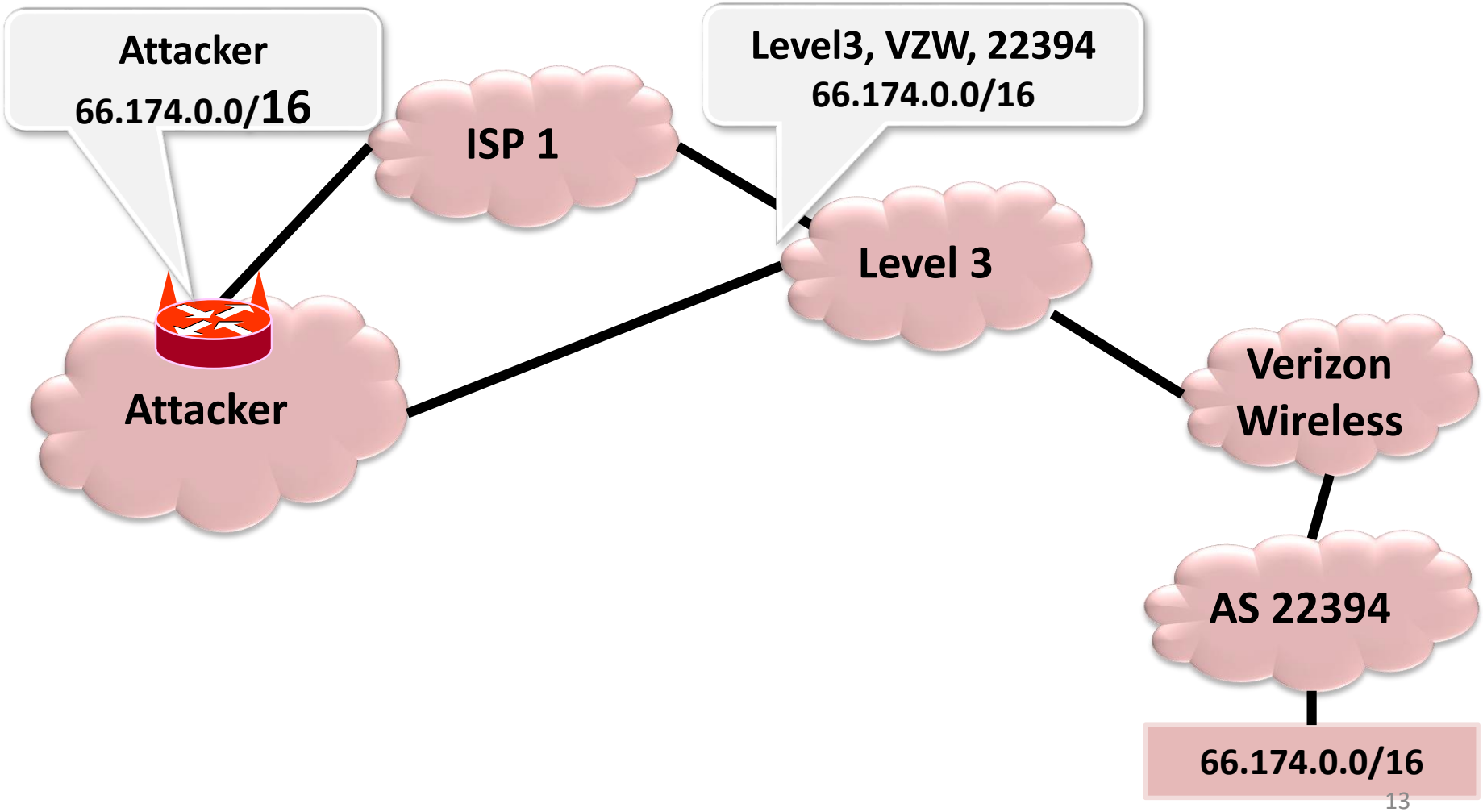
BGP refresher



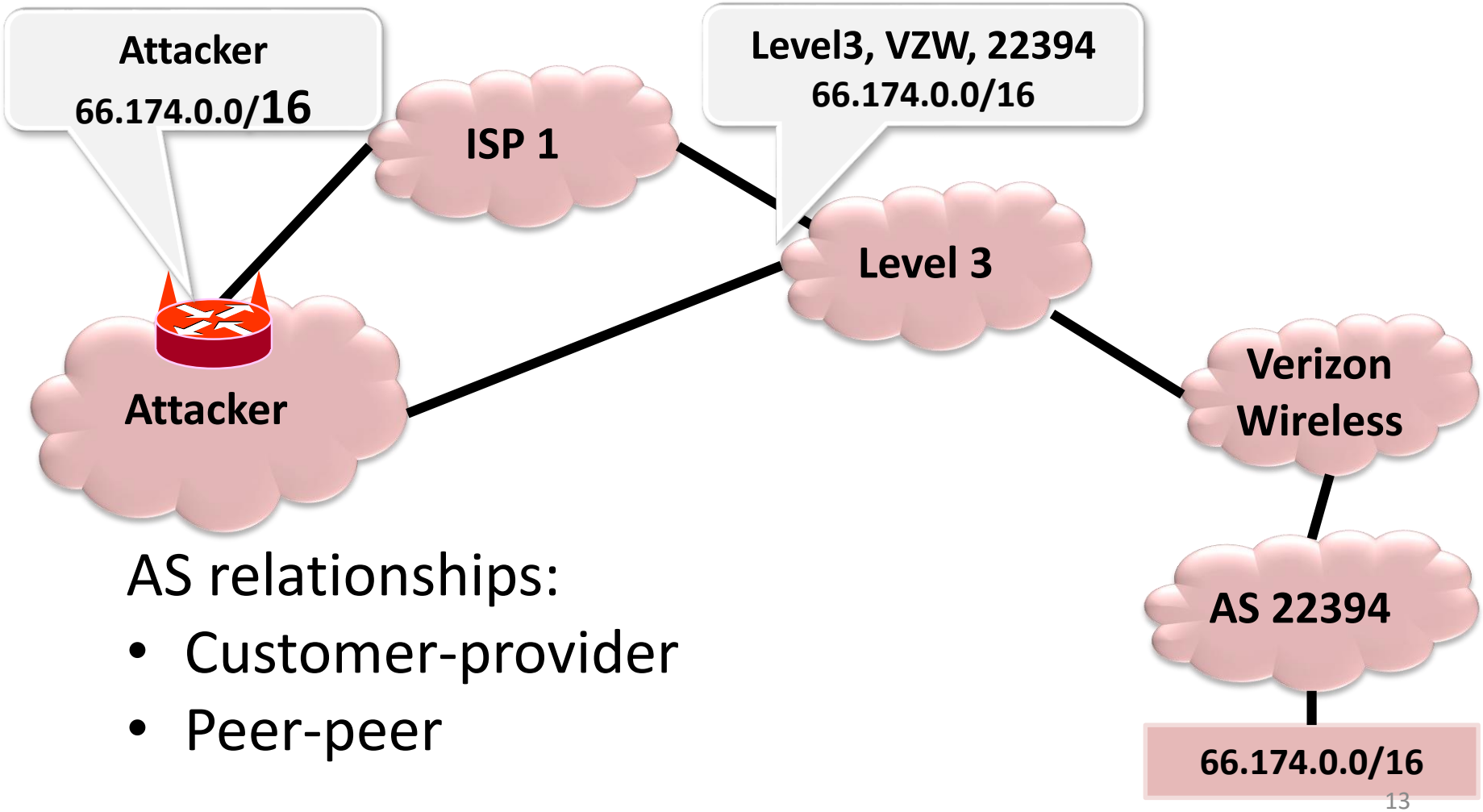
Prefix hijack attack



Prefix hijack attack



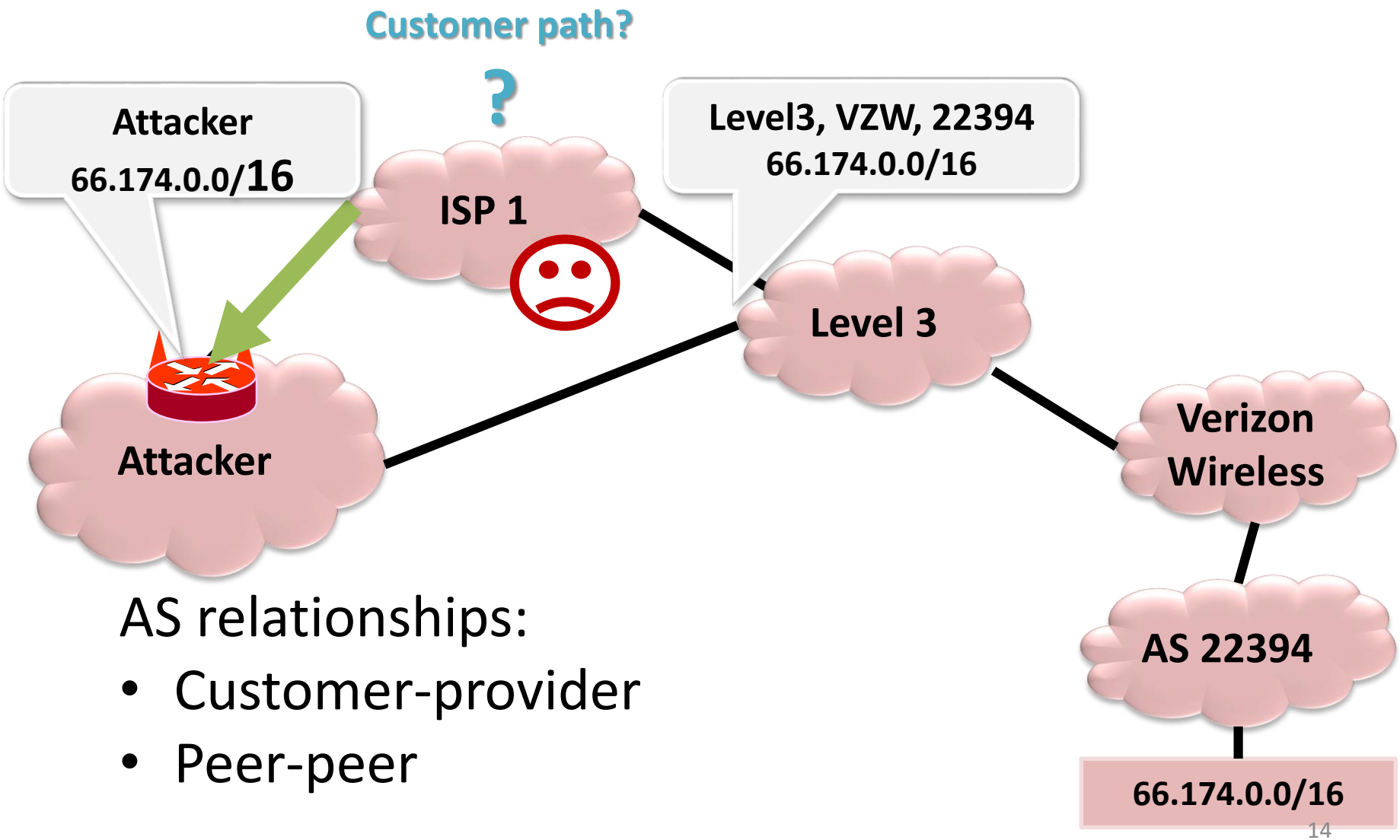
Prefix hijack attack



AS relationships:

- Customer-provider
- Peer-peer

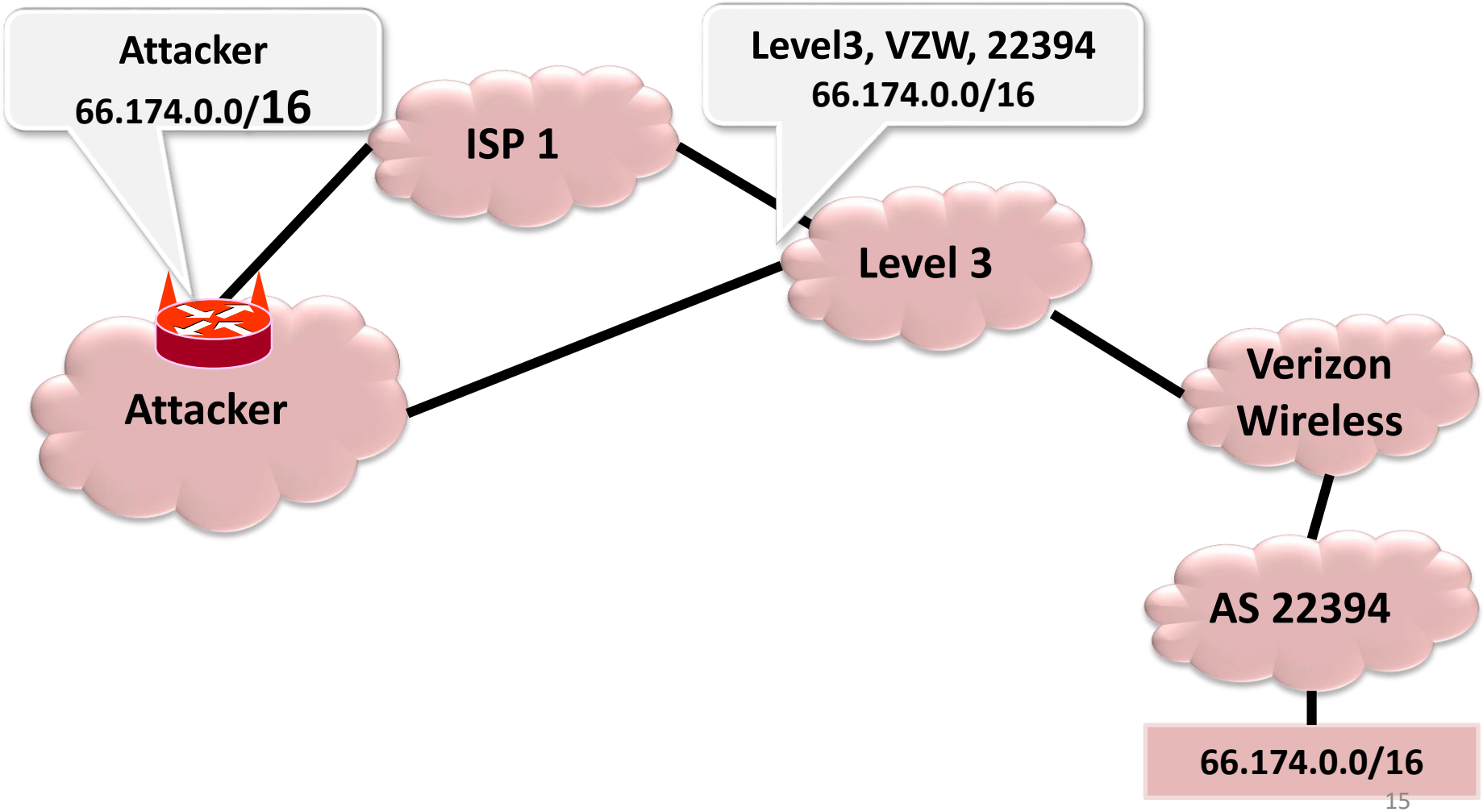
Prefix hijack attack



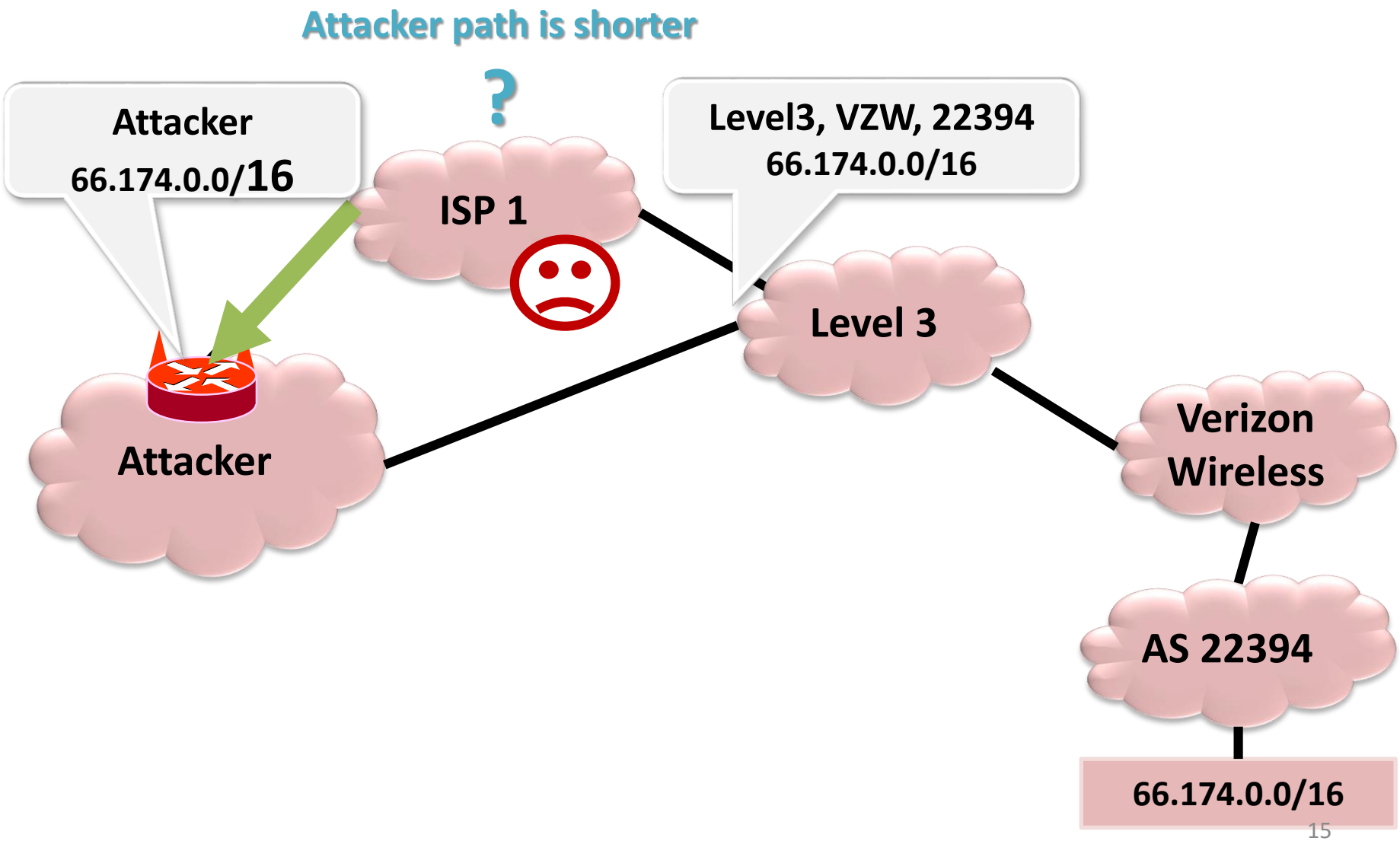
AS relationships:

- Customer-provider
- Peer-peer

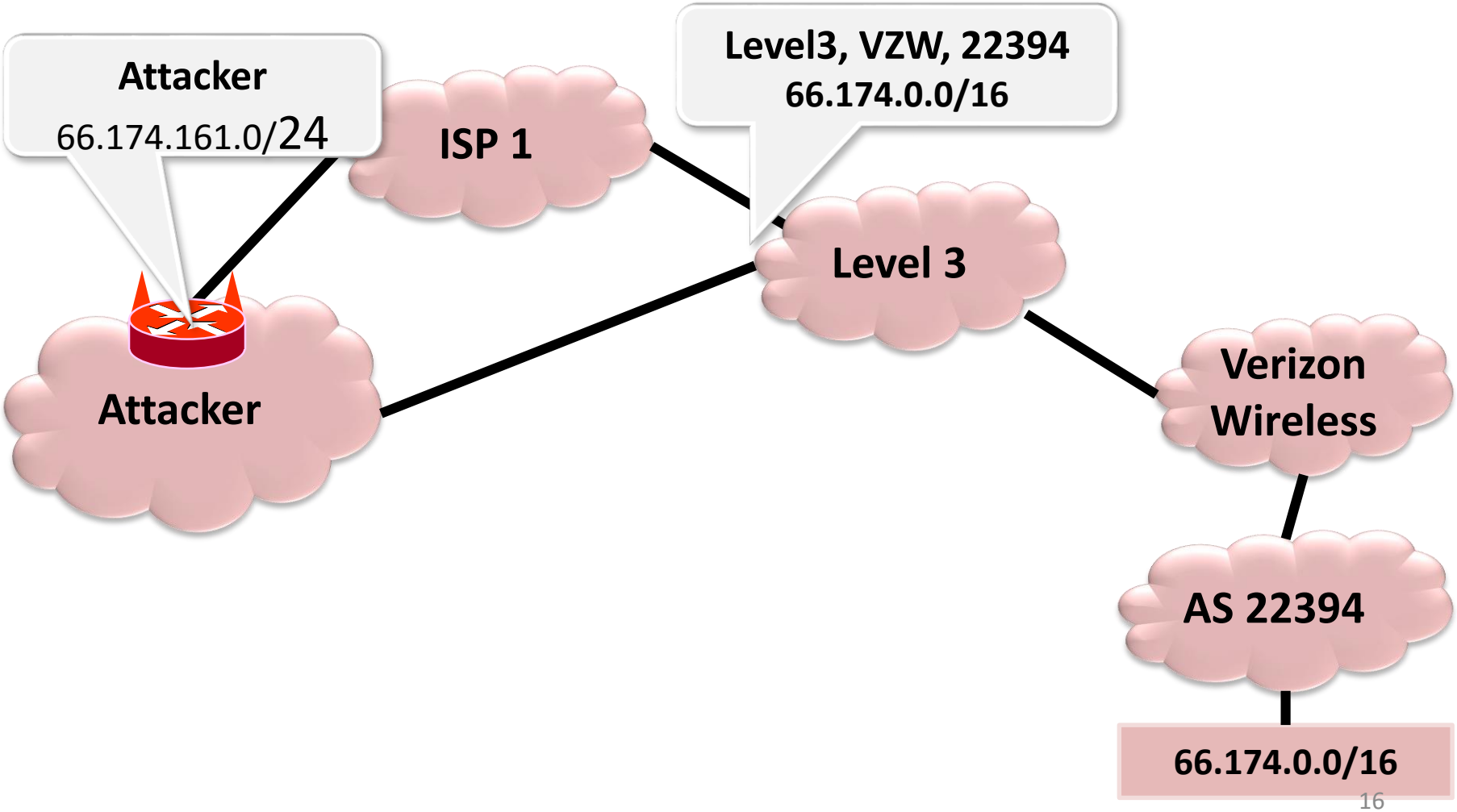
Prefix hijack attack



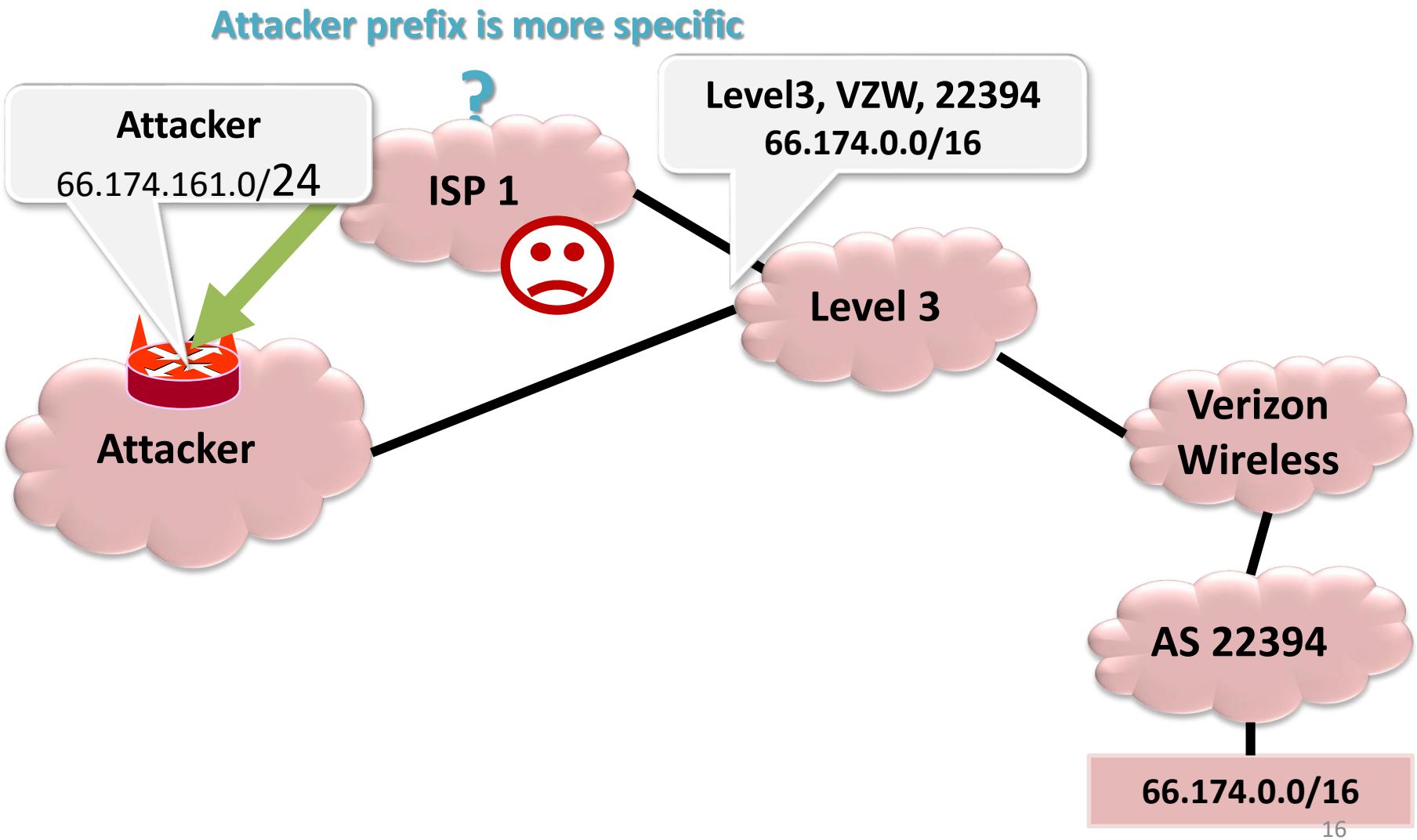
Prefix hijack attack



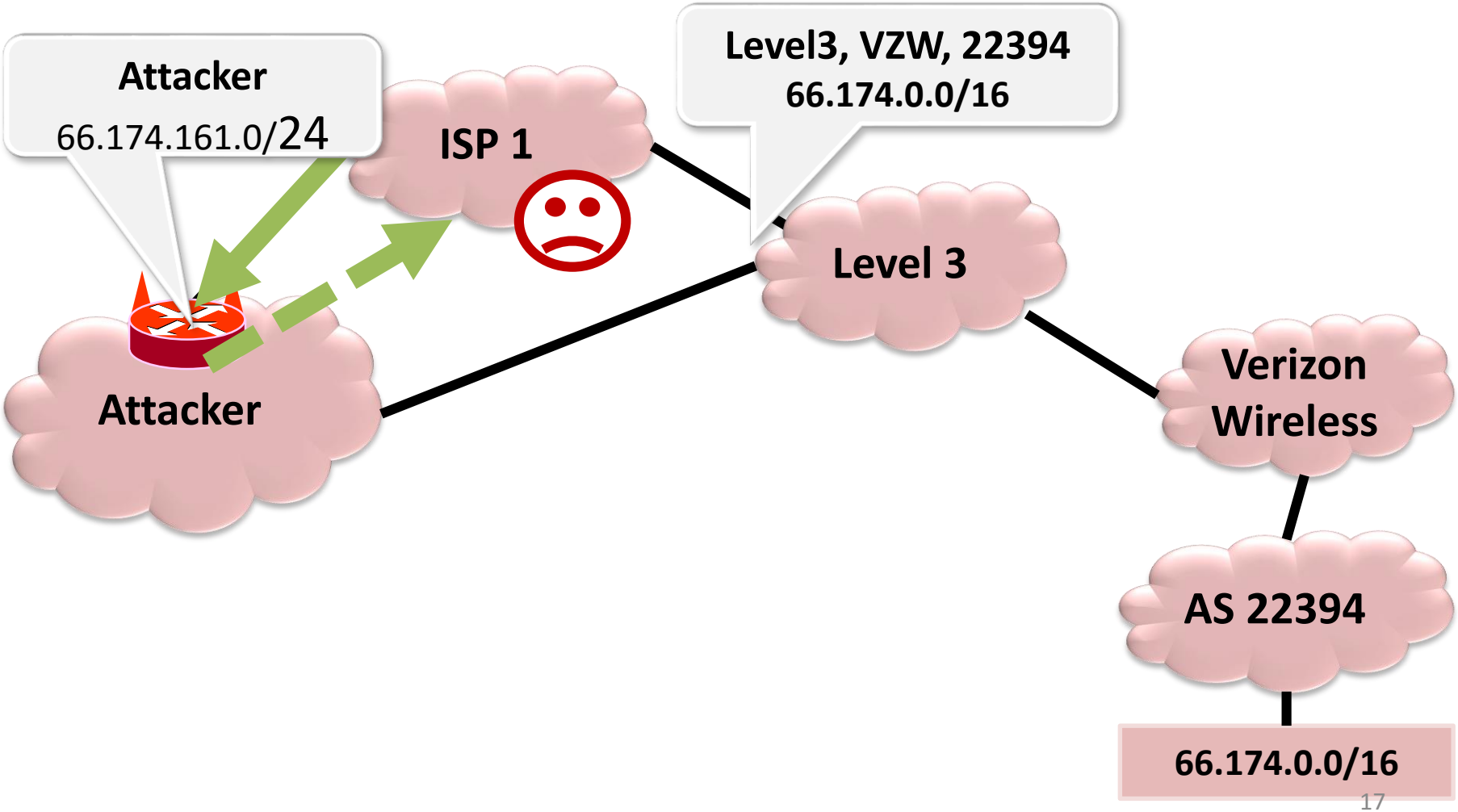
Subprefix hijack attack



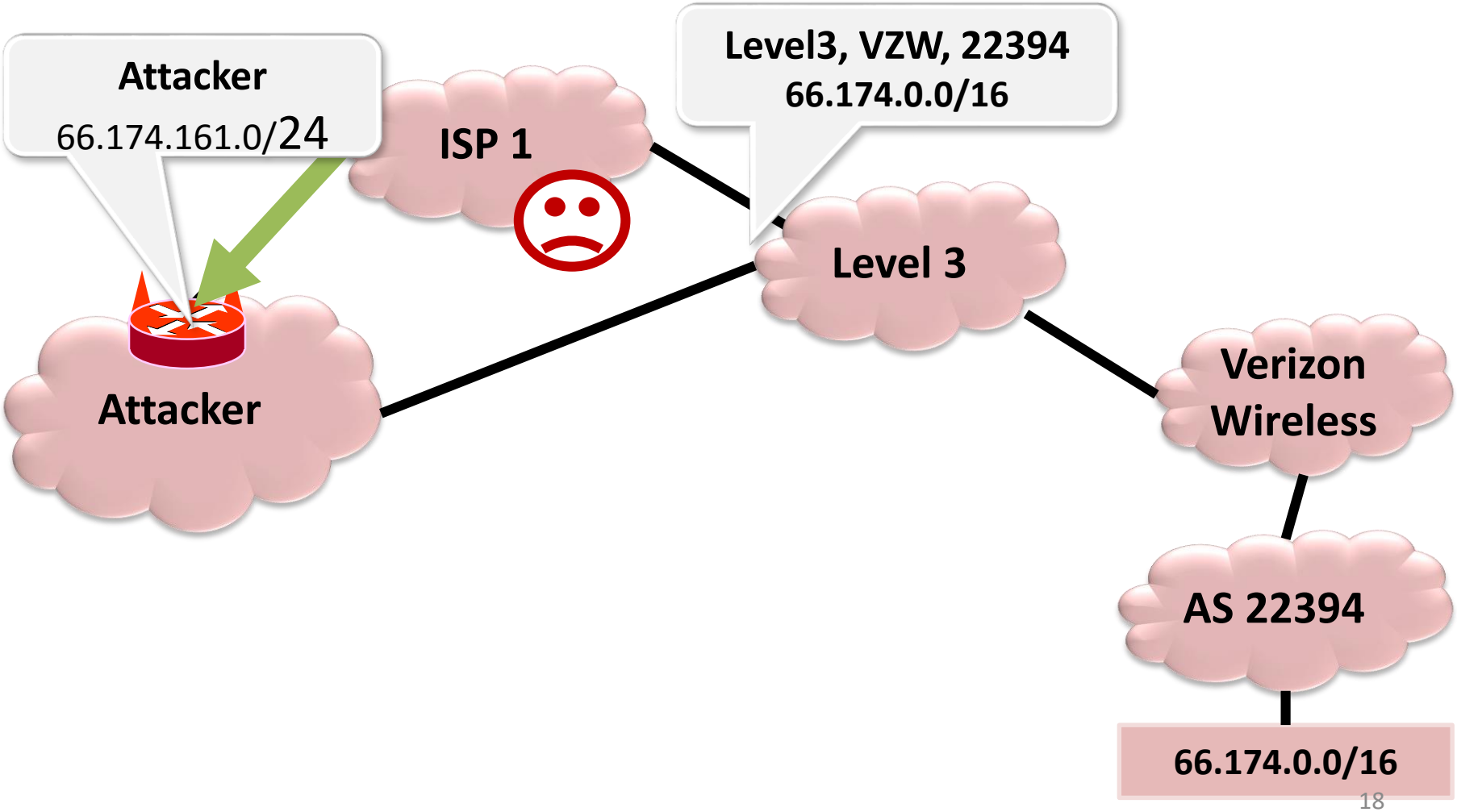
Subprefix hijack attack



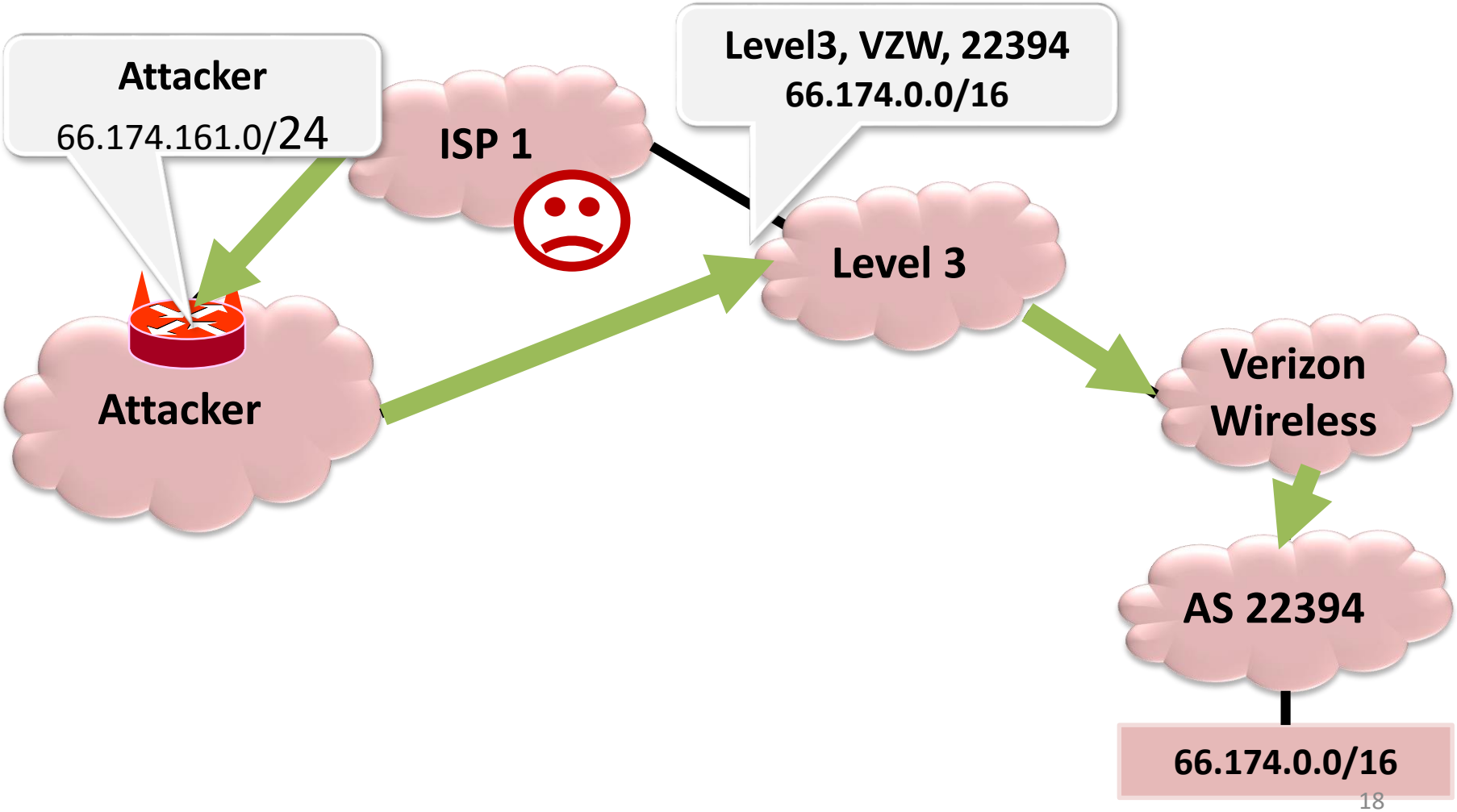
Imposture attack



Interception attack



Interception attack



Examples of systems to secure BGP

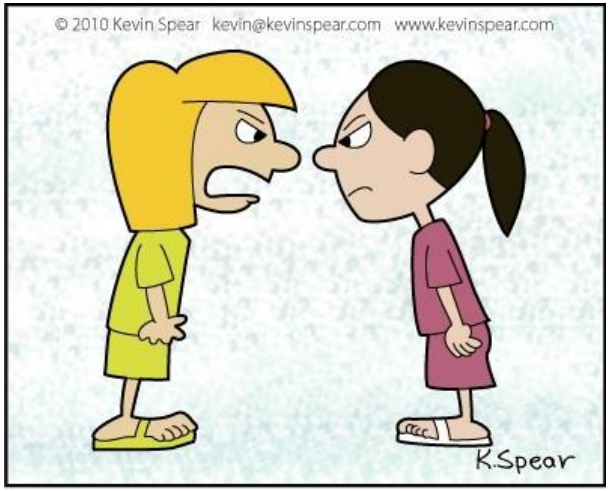
Information shared	Prefix hijack	Subprefix hijack	Interception	Imposture	Example solutions
Prefix origin (Hijack prevention)	✓	✓	✗	✗	Route filtering, RPKI, ROVER
Route path updates (Hijack detection)	✓	✓	✗	✗	PHAS, PrefiSec, PG/BGP
Passive measurements	✗	✗	✓	✓	CrowdSec
Active measurements	✗	✗	✓	✓	Zheng at. al., PrefiSec

Security gain when large ASes collaborate

Security gain when large ASes collaborate

- Several ASes with few large size AS gives good security
- Locality aspects often not considered

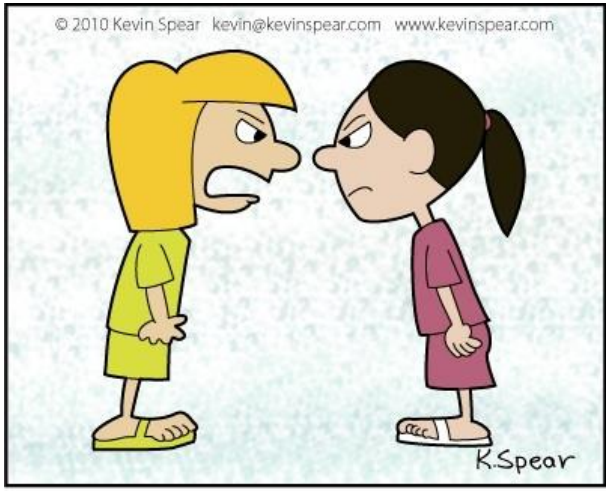
AS Relationship issues



"I am NOT upset. I'm just more animated than usual."

- In October, 2010, Sprint severed its connection with Cogent
- These two ASes had issues with peering relationship that allowed them to exchange traffic at no cost
- ASes do not agree with each other

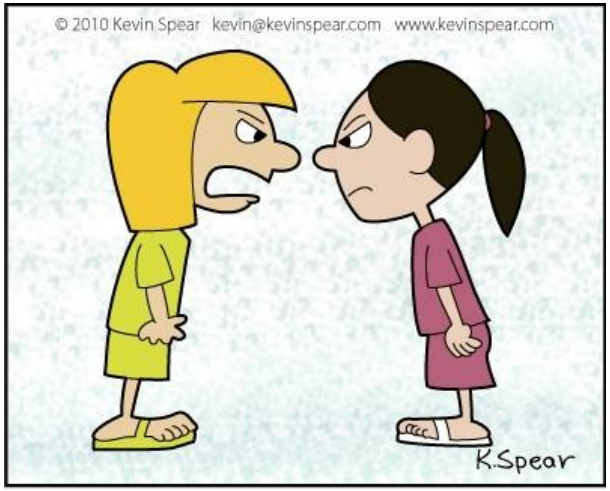
AS Relationship issues



"I am NOT upset. I'm just more animated than usual."

- In October, 2010, Sprint severed its connection with Cogent
- These two ASes had issues with peering relationship that allowed them to exchange traffic at no cost
- ASes do not agree with each other

AS Relationship issues



"I am NOT upset. I'm just more animated than usual."

- In October, 2010, Sprint severed its connection with Cogent
- These two ASes had issues with peering relationship that allowed them to exchange traffic at no cost
- ASes do not agree with each other

- Global collaboration not practical
- Collaboration among networks within same region plausible, for example, through legislation

Research questions

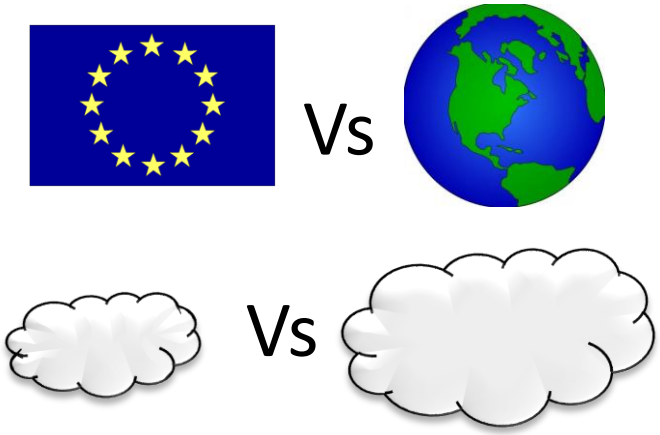
- How are attack prevention/detection rates affected
  - When location of participant ASes is considered?
  - When size of participant ASes is considered?
  - When number of ASes participating in the collaboration is considered?
- In the context of last two questions, we consider the locality aspects

Research questions

Vs

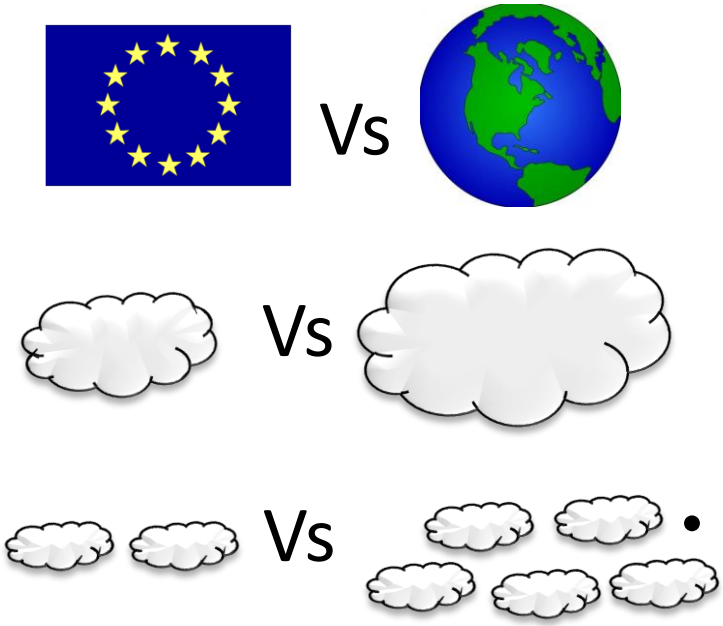
- How are attack prevention/detection rates affected
  - When location of participant ASes is considered?
  - When size of participant ASes is considered?
  - When number of ASes participating in the collaboration is considered?
- In the context of last two questions, we consider the locality aspects

Research questions



- How are attack prevention/detection rates affected
  - When location of participant ASes is considered?
  - When size of participant ASes is considered?
  - When number of ASes participating in the collaboration is considered?
- In the context of last two questions, we consider the locality aspects

Research questions



- How are attack prevention/detection rates affected
  - When location of participant ASes is considered?
  - When size of participant ASes is considered?
  - When number of ASes participating in the collaboration is considered?
- In the context of last two questions, we consider the locality aspects

Contributions

- Systematic data-driven evaluation
- Using real world topologies and routing information we evaluate the impact of:
  - Locality
  - Scale
  - Size
- The research questions are evaluated for three different techniques that are based on sharing
  - Prefix origin
  - Route path updates
  - Passively collected RTT

Examples of systems to secure BGP

Information shared	Prefix hijack	Subprefix hijack	Interception	Imposture	Example solutions
Prefix origin	✓	✓	✗	✗	Route filtering, RPKI, ROVER
Route path updates	✓	✓	✗	✗	PHAS, PrefiSec, PG/BGP
Passive measurements	✗	✗	✓	✓	CrowdSec
Active measurements	✗	✗	✓	✓	Zheng at. al., PrefiSec

Examples of systems to secure BGP

Information shared	Prefix hijack	Subprefix hijack	Interception	Imposture	Example solutions
Prefix origin	✓	✓	✗	✗	Route filtering, RPKI, ROVER
Route path updates	✓	✓	✗	✗	PHAS, PrefiSec, PG/BGP
Passive measurements	✗	✗	✓	✓	CrowdSec
Active measurements	✗	✗	✓	✓	Zheng at. al., PrefiSec

Contributions

- Systematic data-driven evaluation
- Using real world topologies and routing information we evaluate the impact of:
  - Locality
  - Scale
  - Size
- The research questions are evaluated for three different techniques that share:
  - Prefix origin → hijack prevention mechanisms
  - Route path updates → hijack detection mechanisms
  - Passively collected RTT

Hijack prevention technique evaluation

- Simulation based evaluation
- Simulate route propagation using standard routing policy used over the Internet
- Modified and used BSIM tool
- AS-level topology and AS relationship information that has 51,507 ASes and 199,540 relationships

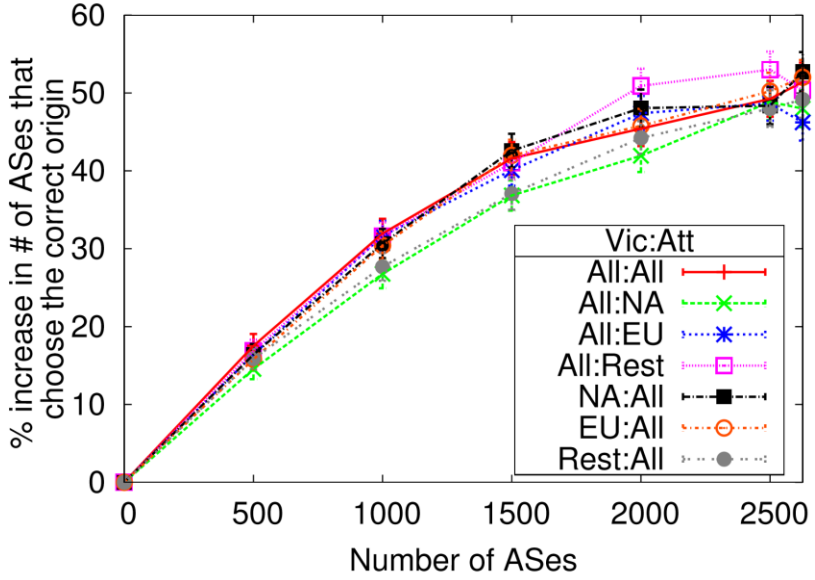
Evaluation methodology

- Simulate route propagation when hijack prevention mechanism is present and absent
- Measure fraction of ASes that choose correct destination AS for the prefix
- Calculate percentage increase in ASes that choose correct origin
- Victim and attacker AS chosen randomly

Evaluation methodology

- Simulate route propagation when hijack prevention mechanism is present and absent
- Measure fraction of ASes that choose correct destination AS for the prefix
- Calculate percentage increase in ASes that choose correct origin
- Victim and attacker AS chosen randomly

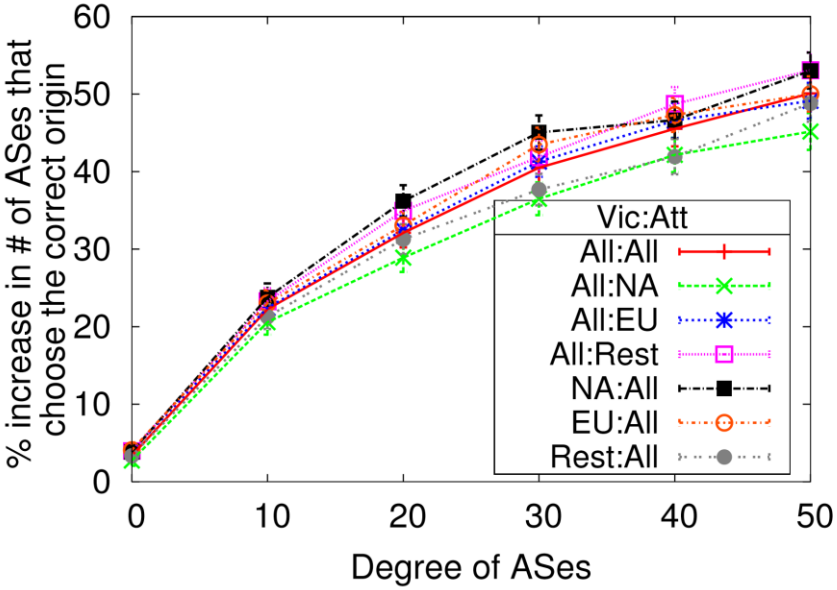
Global baseline: scale



Global

- As number of ASes that collaborate increases, the protection to ASes increases
- With 500 ASes an average gain of 15% across attacker-victim pairs
- Gain rises to 45% when all ASes with node degree >= 20 deploy the prevention mechanism

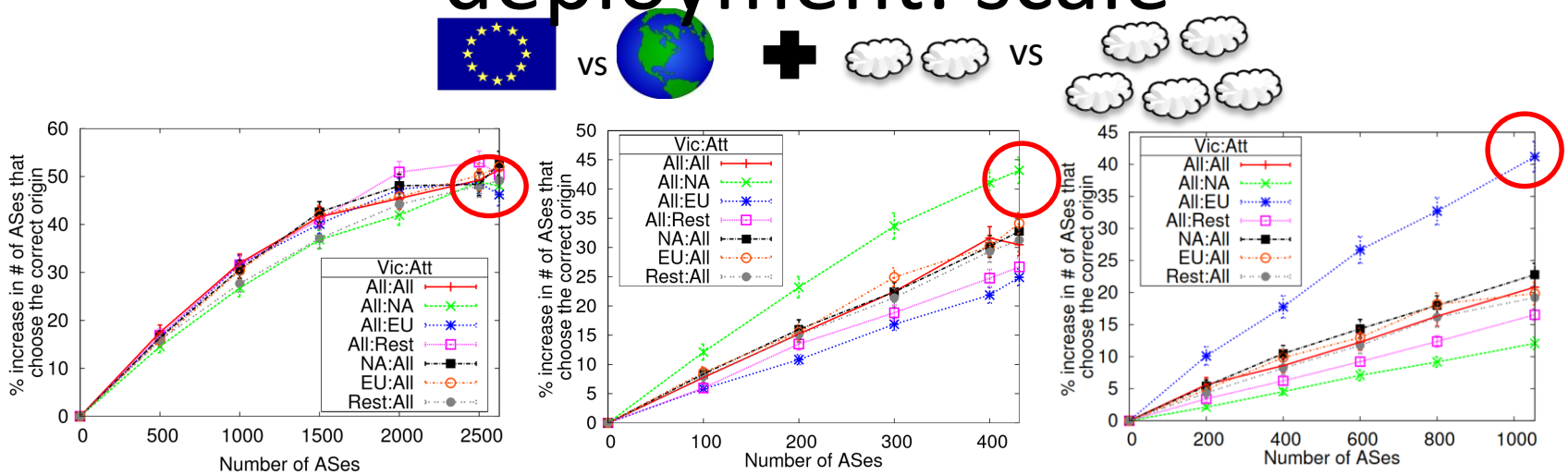
Global baseline: size



Global

- Size of an AS is based on the number of neighbors of that AS and is termed as degree of AS
- As size of ASes that collaborate increases, the protection to ASes increases

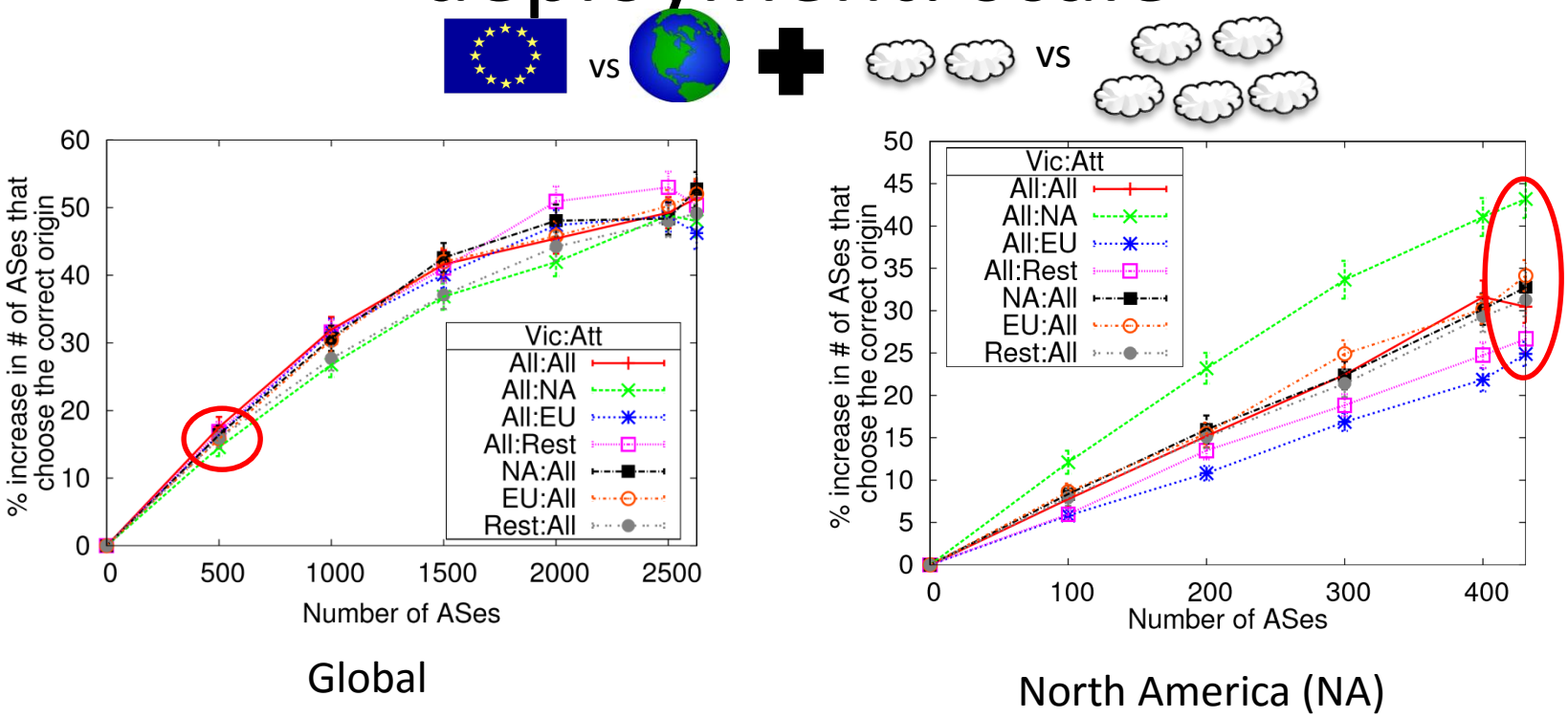
Compare global and regional deployment: scale



Global North America (NA) European Union (EU)

- Regional deployment provide improvements similar to global deployment when attacker is local
- Deployment to prevent attacks from own region
- Mechanisms for greater good

Compare global and regional deployment: scale



- 500 randomly selected global ASes vs 431 ASes in NA region

Contributions

- Systematic data-driven evaluation
- Using real world topologies and routing information we evaluate the impact of:
  - Locality
  - Scale
  - Size
- The research questions are evaluated for three different techniques that share:
  - Prefix origin → hijack prevention mechanisms
  - Route path updates → hijack detection mechanisms
  - Passively collected RTT

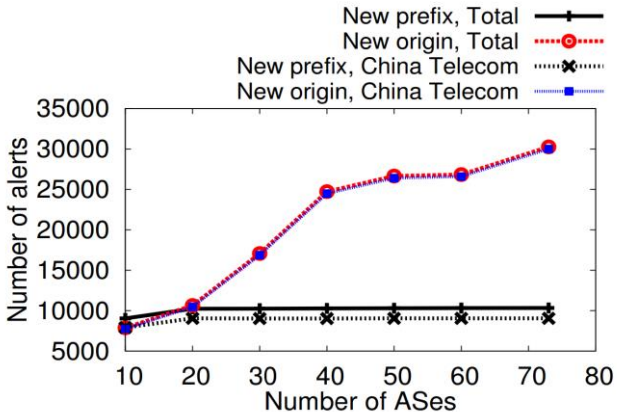
Contributions

- Systematic data-driven evaluation
- Using real world topologies and routing information we evaluate the impact of:
  - Locality
  - Scale
  - Size
- The research questions are evaluated for three different techniques that share:
  - Prefix origin → hijack prevention mechanisms
  - Route path updates → hijack detection mechanisms
  - Passively collected RTT

Hijack detection system evaluation

- Extended earlier proposed system that uses route path announcements to aid in raising alerts for routing attacks
- Routepath updates from RouteViews project around large scale routing anomaly
- On April 8, 2010, China Telecom announced ≈50,000 prefixes allocated to other networks

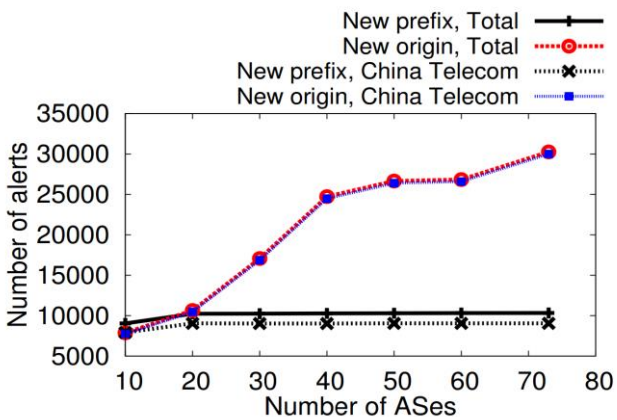
Global vs regional baseline: scale



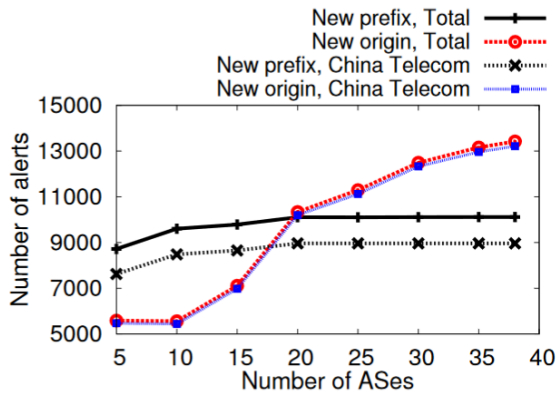
Global

- Number of alerts for prefix hijack increases number of ASes
- Few ASes needed to detect subprefix hijack alerts
- High detection rate in *rest of the world* region despite fewer ASes
- Confirms result with the hijack prevention mechanisms

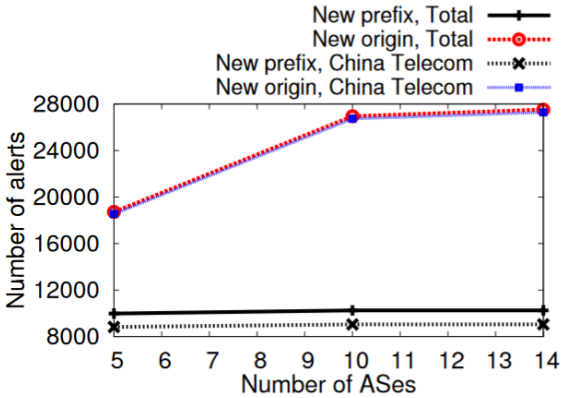
Global vs regional baseline: scale



Global



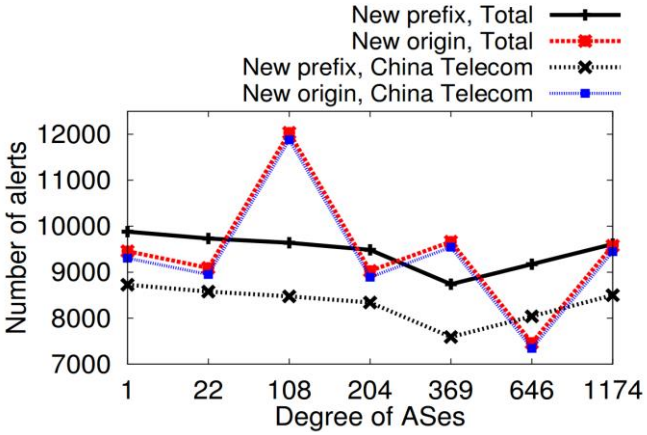
NA



Rest of the world

- Number of alerts for prefix hijack increases number of ASes
- Few ASes needed to detect subprefix hijack alerts
- High detection rate in *rest of the world* region despite fewer ASes
- Confirms result with the hijack prevention mechanisms

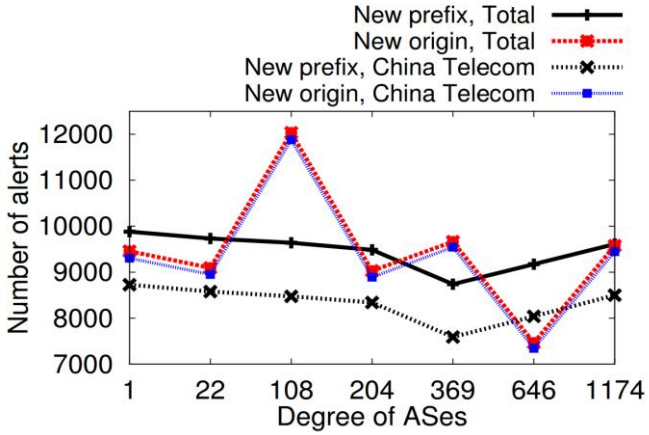
Global baseline: size



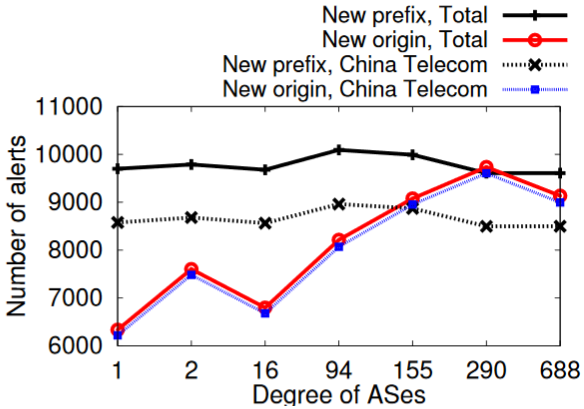
Global

- With increasing degree threshold the alerts rate does not increase
- Regional deployment with complementing ASes from other regions
- Routes learnt by mid/tier ASes may not reach their providers

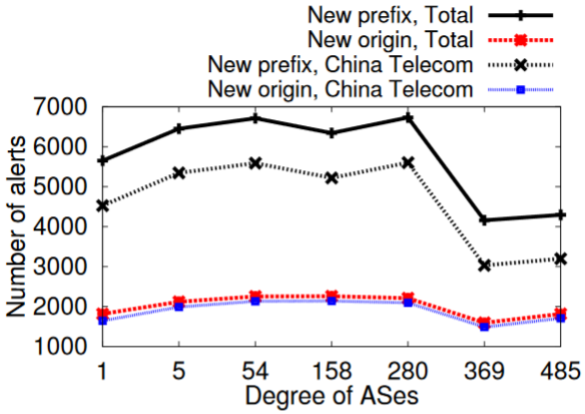
Global baseline: size



Global



North America (NA)



European Union (EU)

- With increasing degree threshold the alerts rate does not increase
- Regional deployment with complementing ASes from other regions
- Routes learnt by mid/tier ASes may not reach their providers

Contributions

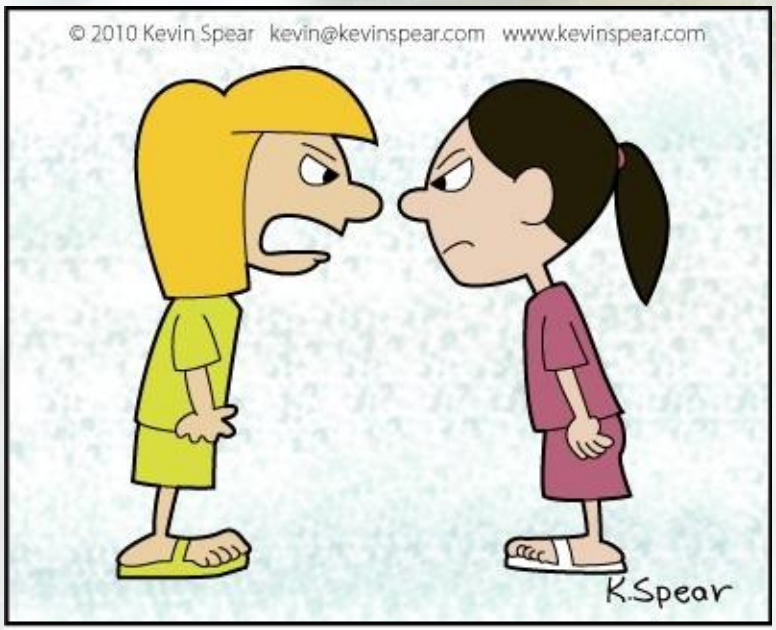
- Systematic data-driven evaluation
- Using real world topologies and routing information we evaluate the impact of:
  - Locality
  - Scale
  - Size
- The research questions are evaluated for three different techniques that share:
  - Prefix origin
  - Route path updates
  - Passively collected RTT

Conclusion

- Systematic evaluation of three broad classes of routing attack prevention/detection techniques
- Locality, size, and scale aspects considered
- For all three classes of techniques we see cases where regional deployment provides substantial benefits
- Regional deployment with carefully selected participants can outperform global deployment that is not planned

Linköping University

expanding reality



"I am NOT upset. I'm just more animated than usual."

Does Scale, Size, and Locality Matter?

Rahul Hiran

rahul.hiran@liu.se