

PrefiSec: A Distributed Alliance Framework for Collaborative BGP Monitoring and Prefix-based Security

Rahul Hiran, Niklas Carlsson, Nahid Shahmehri

Linköping University, Sweden

Nov. 3, 2014

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	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	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	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	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	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	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 Pa
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

Internet Society | **Deploy360 Programme**

Home | **START HERE!** | IPv6 | DNSSEC | Other Topics | ION Confer

Turkish Hijacking of DNS Providers Shows Clear Need For Deploying BGP And DNS Security

« New RFC 7157 Out About IPv6 Multihoming Without NAT | Vint Cerf: I want all of you to a the

Over the weekend there were extremely disturbing reports out of Turkey of escalations in the attempts by the Turkish government to block social media sites such as Twitter and YouTube. The steps now

```
show router bgp routes 8.8.8.8
-----
BGP Router ID: 232.156.136.127 AS: 9121 Local AS: 9121
-----
Legend :
Status codes : u - used, s - suppressed, h - history, d - decayed,
Origin codes : i - IGP, e - EGP, ? - Incomplete, > - best, b - best
-----
BGP IPv4 Routes
-----
Flag Network LocalPref MED
NextHop Path-Id VpnLabel
As-Path
```

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 ...

Routing attacks increasingly common

Internet (Icon) | Deploy360

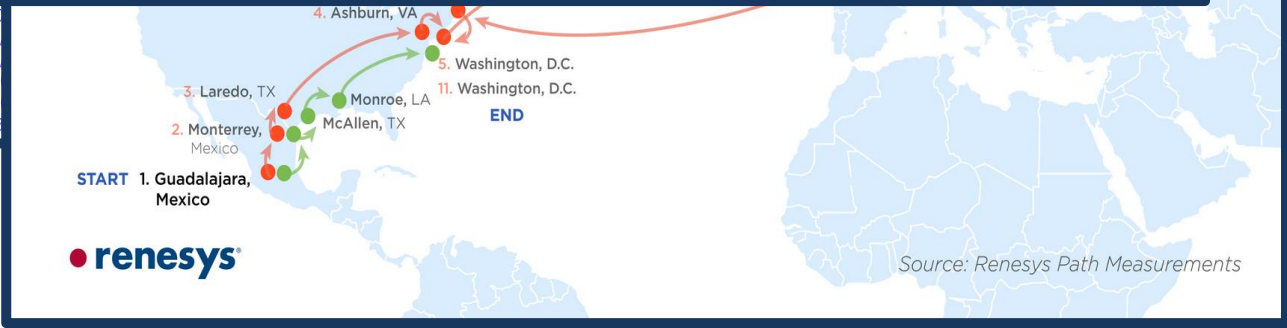
Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*

Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins

BY ANDY GREENBERG 08.07.14 | 1:00 PM | PERMALINK

100.127.0.0
102.2.88.0/

103.248.220
103.249.8.0
103.250.0.0
116.206.72.
116.206.85.
116.206.103



Other Topics | ION Confer

Vint Cerf: I want all of you to a the

DNS Providers Shows BGP And DNS Security

```
router bgp routes 8.8.8.8
router ID: 232.156.136.127 AS: 9121 Local AS: 9121
...
codes: u - used, s - suppressed, h - history, d - decayed,
...
codes: i - IGP, e - EGP, ? - Incomplete, > - best, b - best
...
Pv4 Routes
Network LocalPref MED
osp Path-Id VPLLabel
4h
```

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

The screenshot displays a network monitoring interface. At the top, a header reads "Internet (🌐) | Deploy360". Below it, a yellow box contains the text "Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*". To the right of this box are links for "Other Topics" and "ION Confer".

On the left side, there are two overlapping panels. The top panel has the headline "Hacker Redir Providers to S" and the byline "BY ANDY GREENBERG 08.07". The bottom panel shows a map of Mexico with a red dot indicating a location. The text "START 1. Guadalajara Mexico" is visible, along with the "renesys" logo.

The main content area features a large article title: "Internet Traffic from U.S. Government Websites Was Redirected Via Chinese Networks". Below the title is the byline "By Joshua Rhett Miller / Published November 16, 2010 / FoxNews.com". The article's image shows a server rack with a Chinese flag in the foreground.

IP address lists are visible on the left side of the interface:

- 100.127.0.0
- 102.2.88.0/
- 103.248.220
- 103.249.8.0
- 103.250.0.0
- 116.206.72.
- 116.206.85.
- 116.206.103

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

The screenshot displays a network monitoring interface. At the top, a header reads "Internet (🌐) | Deploy360". Below it, a yellow box contains the text "Traceroute Path 1: from Guadalajara, Mexico to Washington, D.C. via *Belarus*". To the right of this box are links for "Other Topics" and "ION Confer".

On the left side, there is a news article snippet titled "Hacker Redir Providers to S" by Andy Greenberg, dated 08.07. Below the title is a map of Mexico with a red dot indicating a location. The map is labeled "START 1. Guadalajara Mexico" and includes the "renesys" logo.

The main content area features a large headline: "Internet Traffic from U.S. Government Websites Was Redirected Via Chinese Networks". Below the headline, it says "By Joshua Rhett Miller / Published November 16, 2010 / FoxNews.com". The article's image shows a server rack and a Chinese flag.

IP address lists are visible on the left side of the interface:

- 100.127.0.0
- 102.2.88.0/
- 103.248.220
- 103.249.8.0
- 103.250.0.0
- 116.206.72.
- 116.206.85.
- 116.206.103

Each day there are large numbers of bogus route announcements

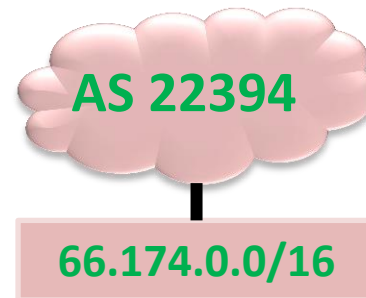
- e.g., cidr-report.org

Among these we have seen many serious attacks ...

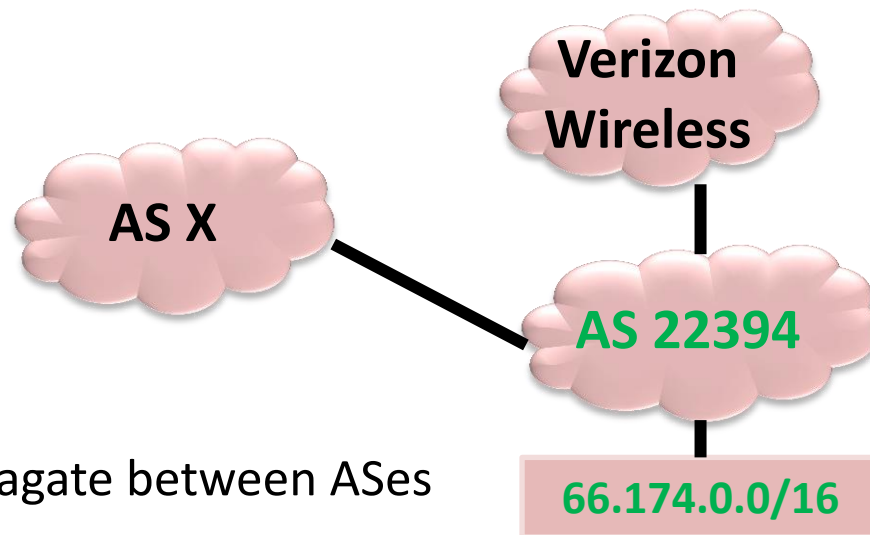
BGP-related Hijacks

Normal operation

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



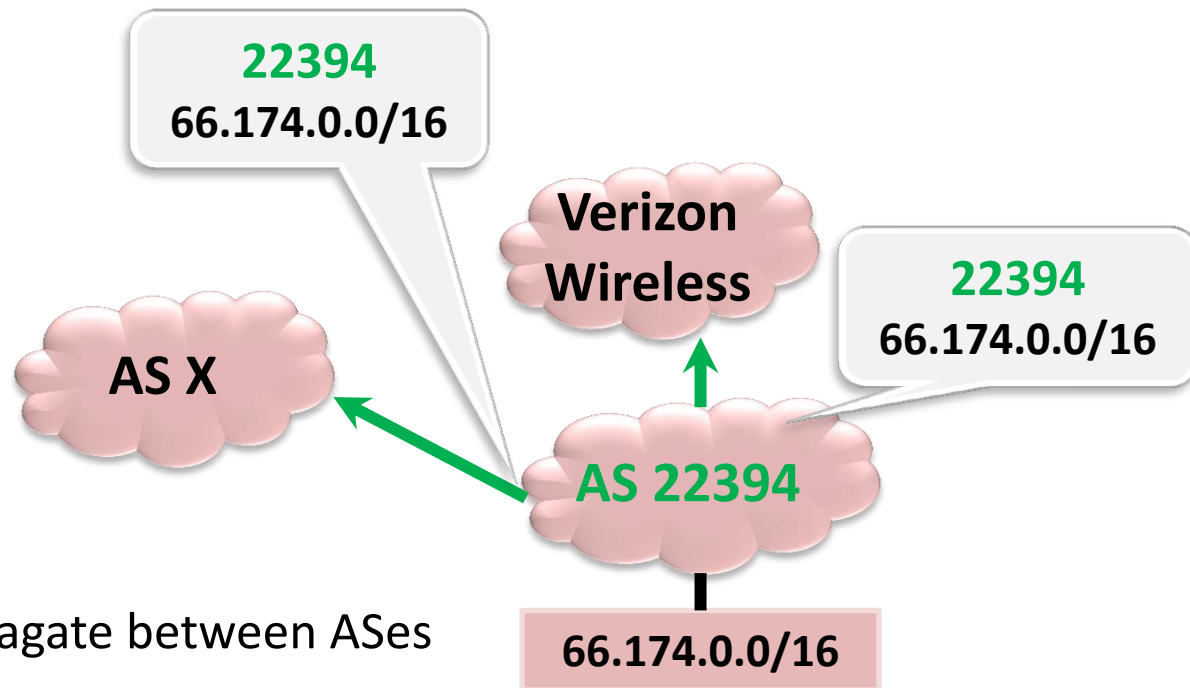
BGP-related Hijacks



Normal operation

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

BGP-related Hijacks



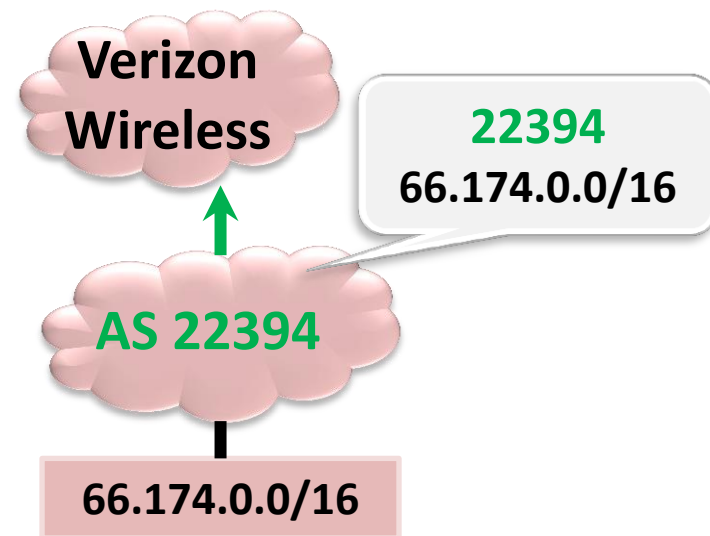
Normal operation

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

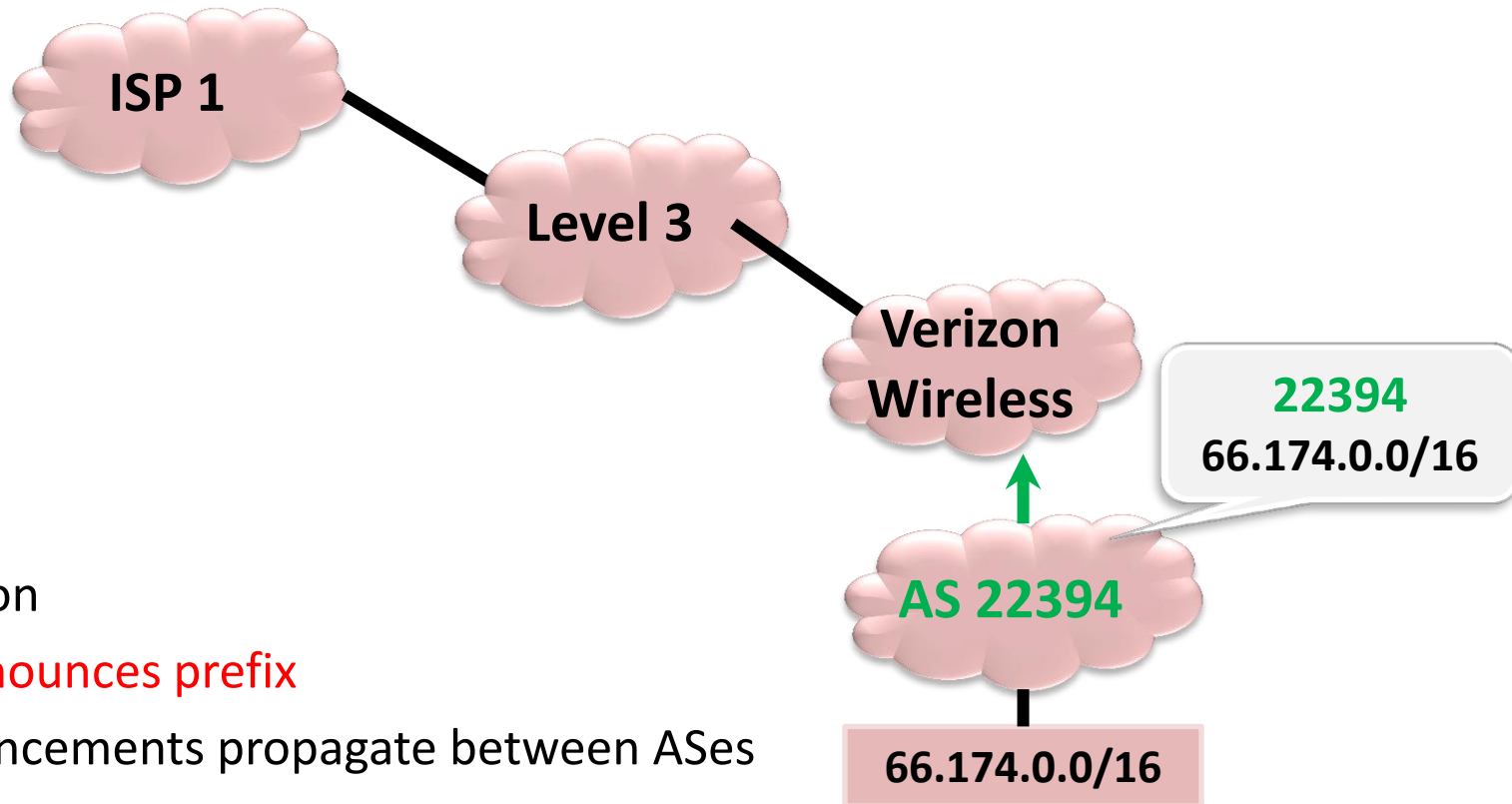
BGP-related Hijacks

Normal operation

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



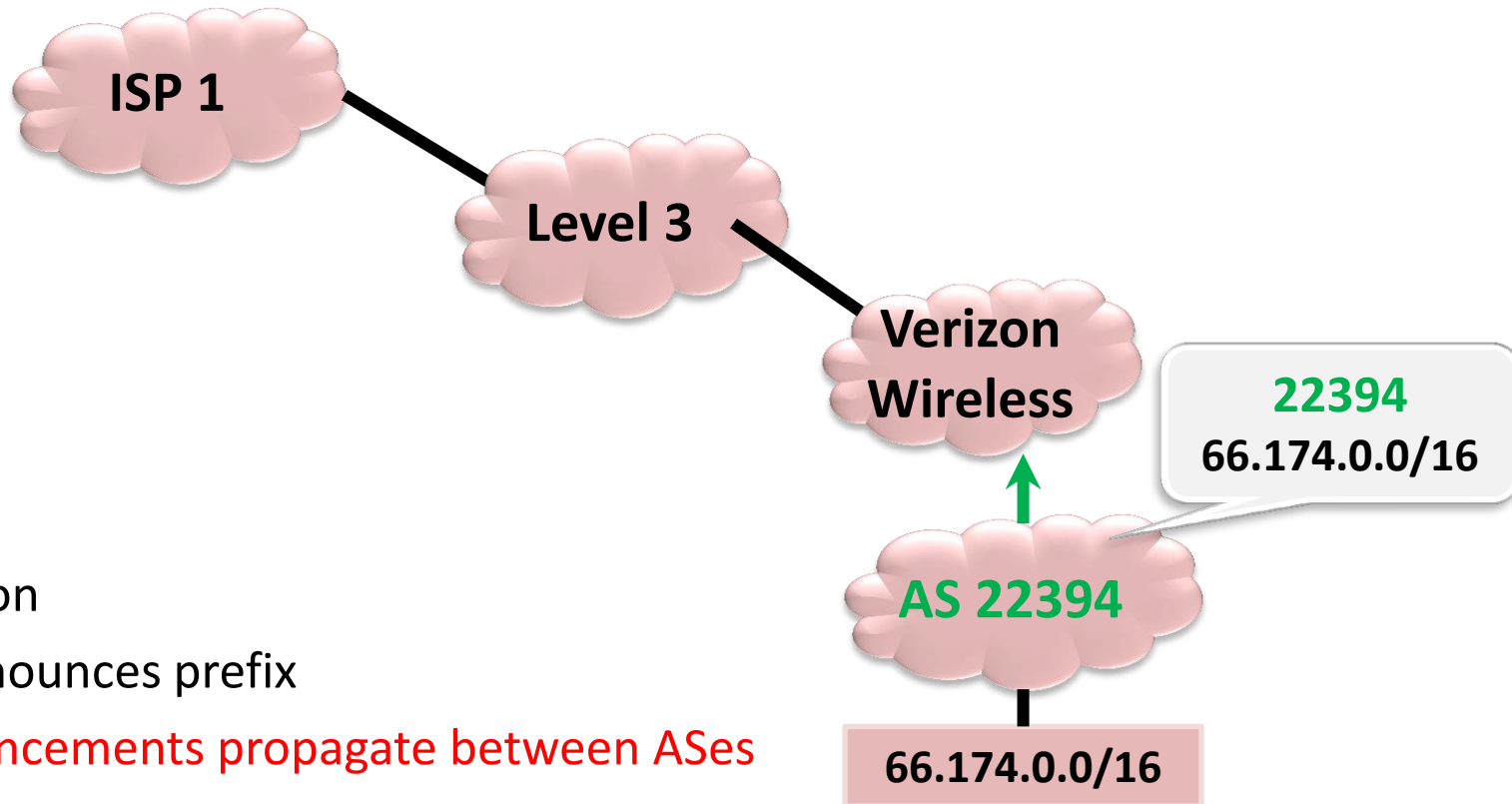
BGP-related Hijacks



Normal operation

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

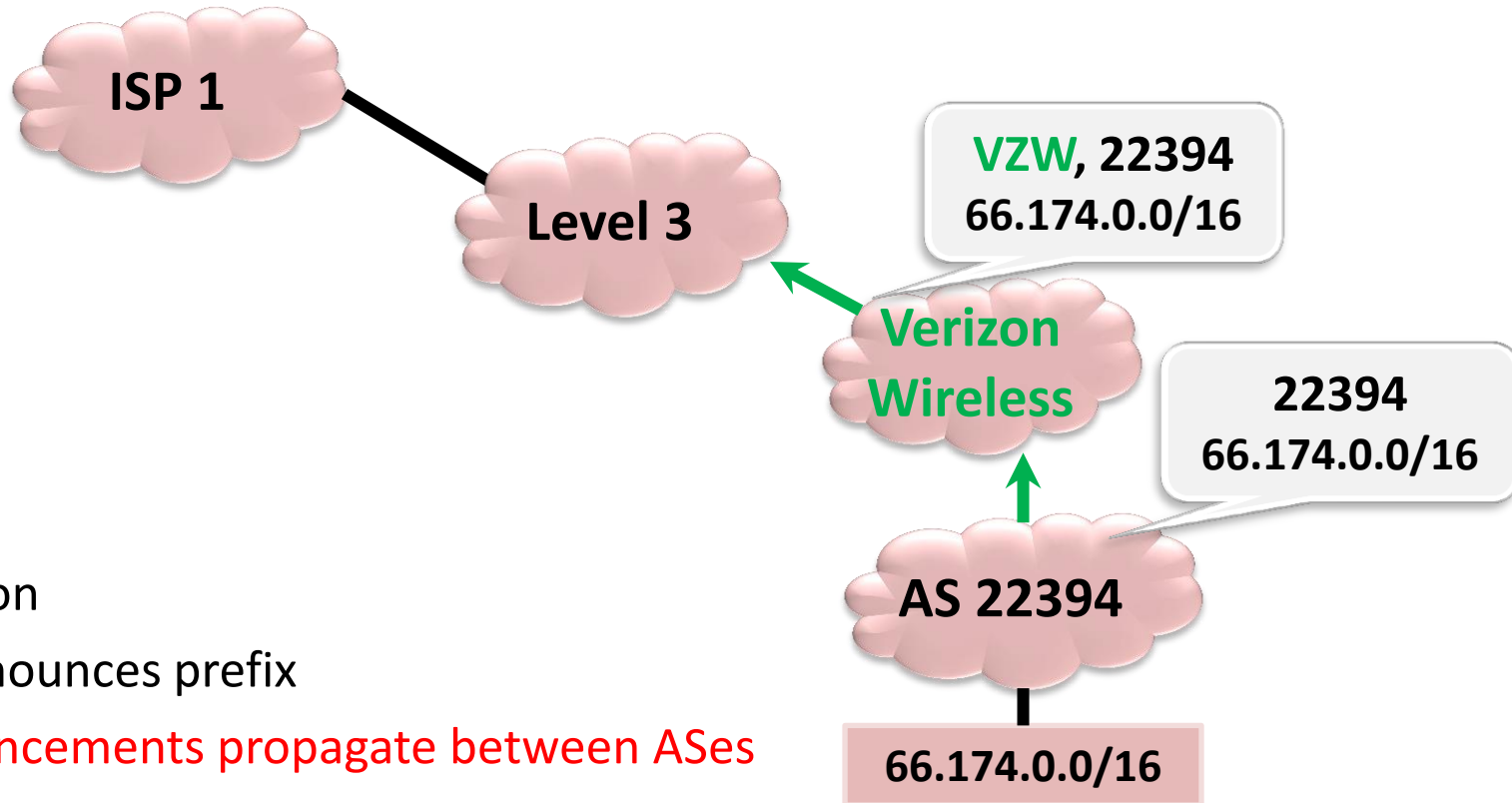
BGP-related Hijacks



Normal operation

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

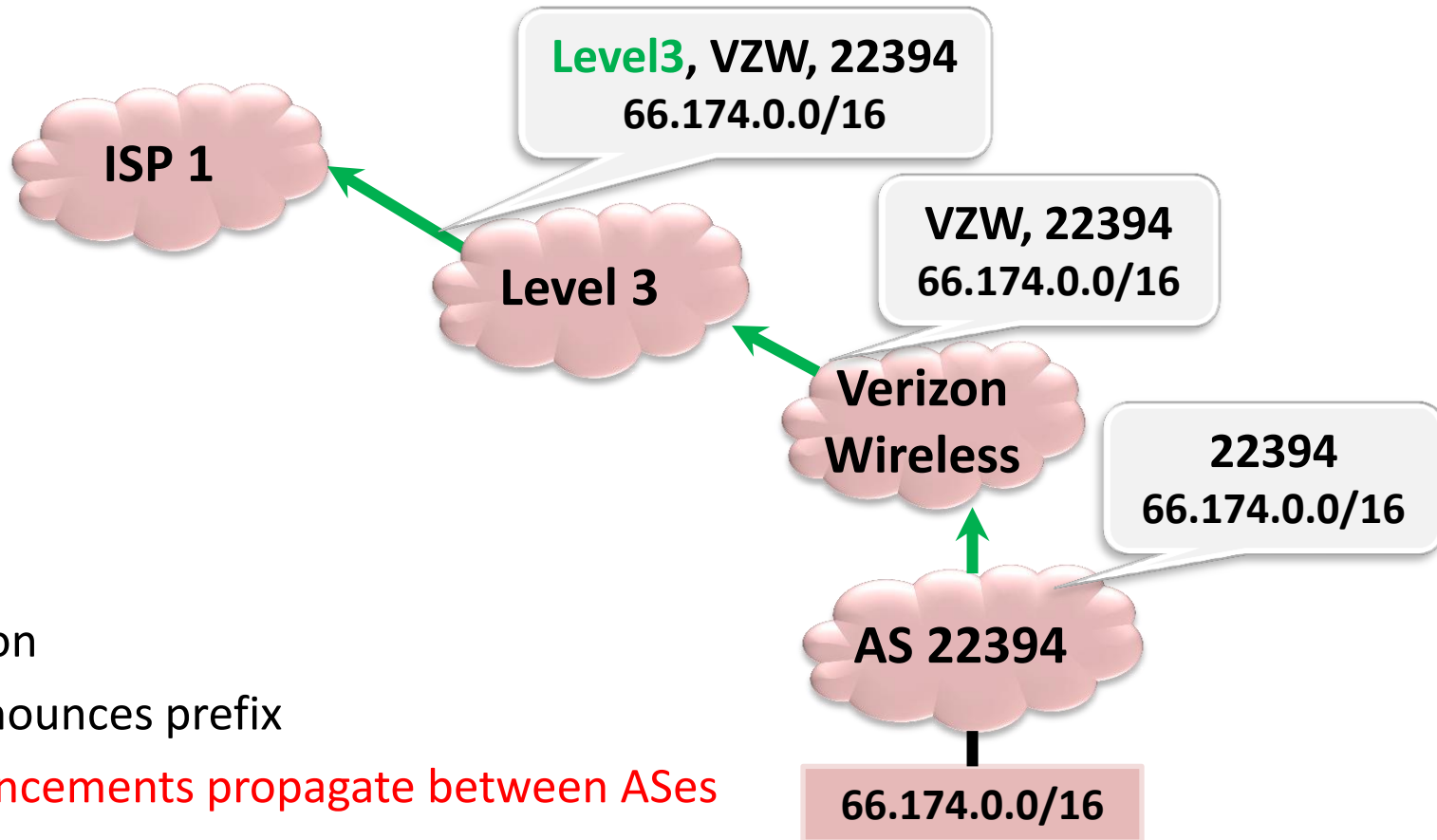
BGP-related Hijacks



Normal operation

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

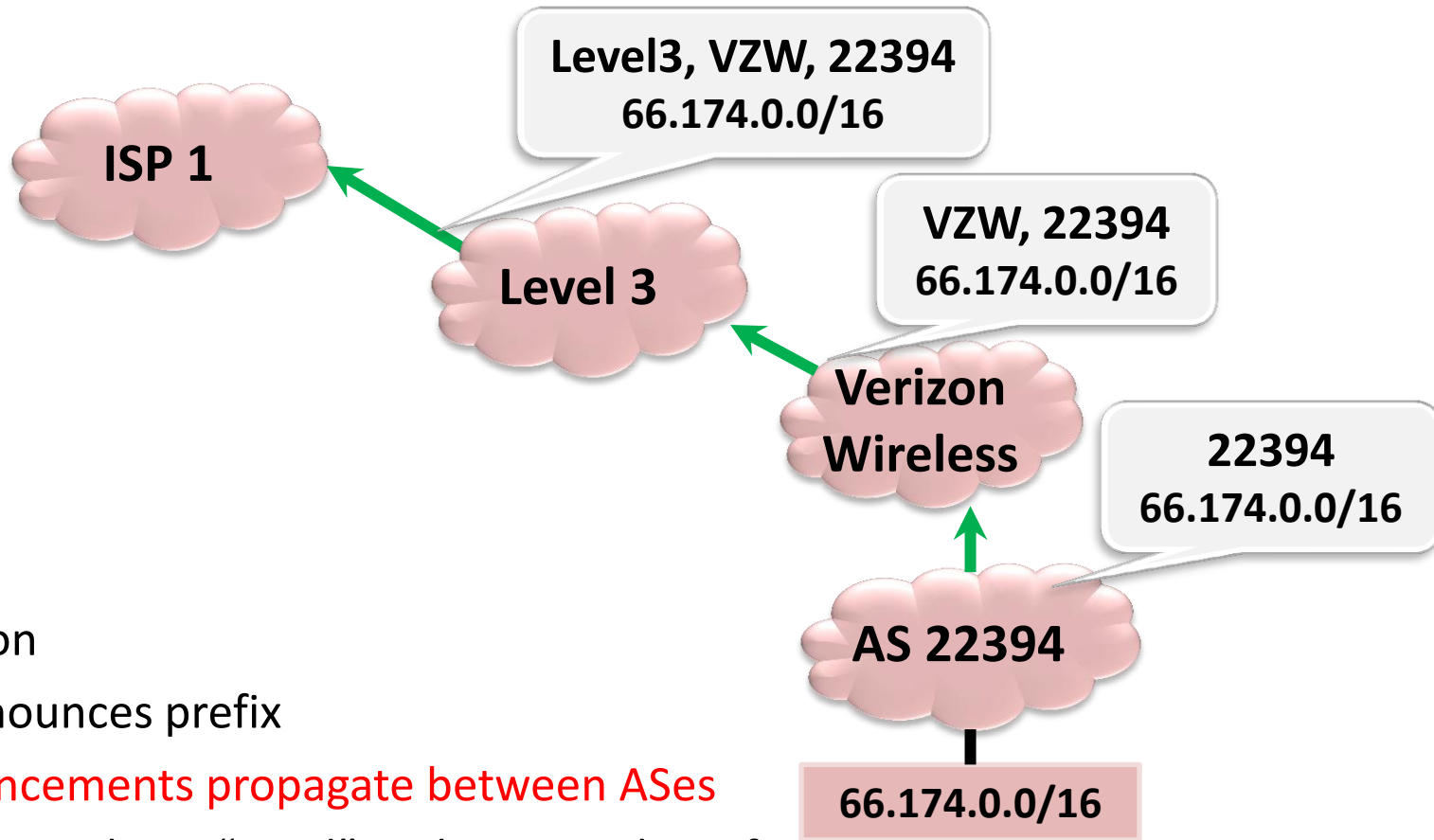
BGP-related Hijacks



Normal operation

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

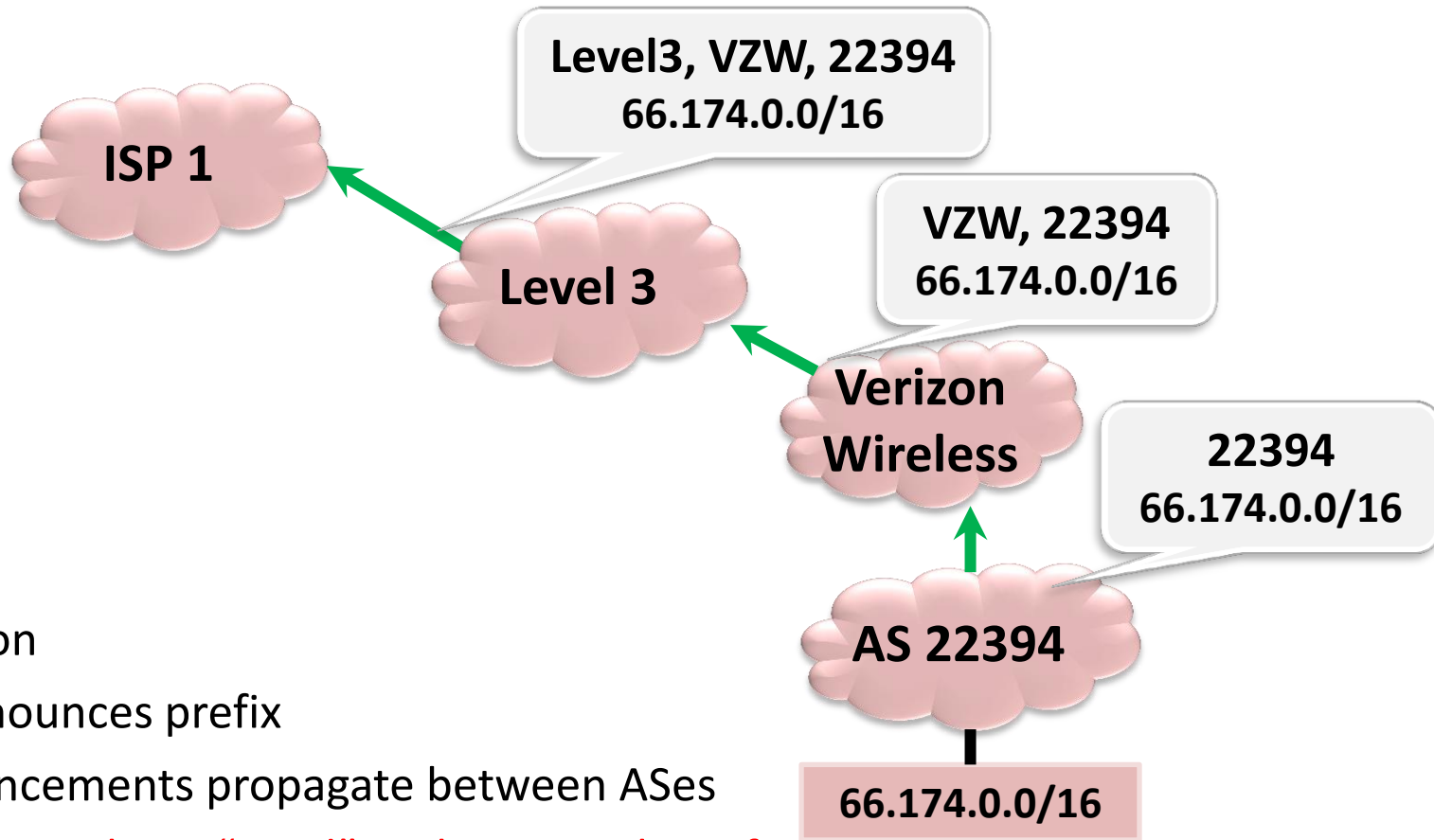
BGP-related Hijacks



Normal operation

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

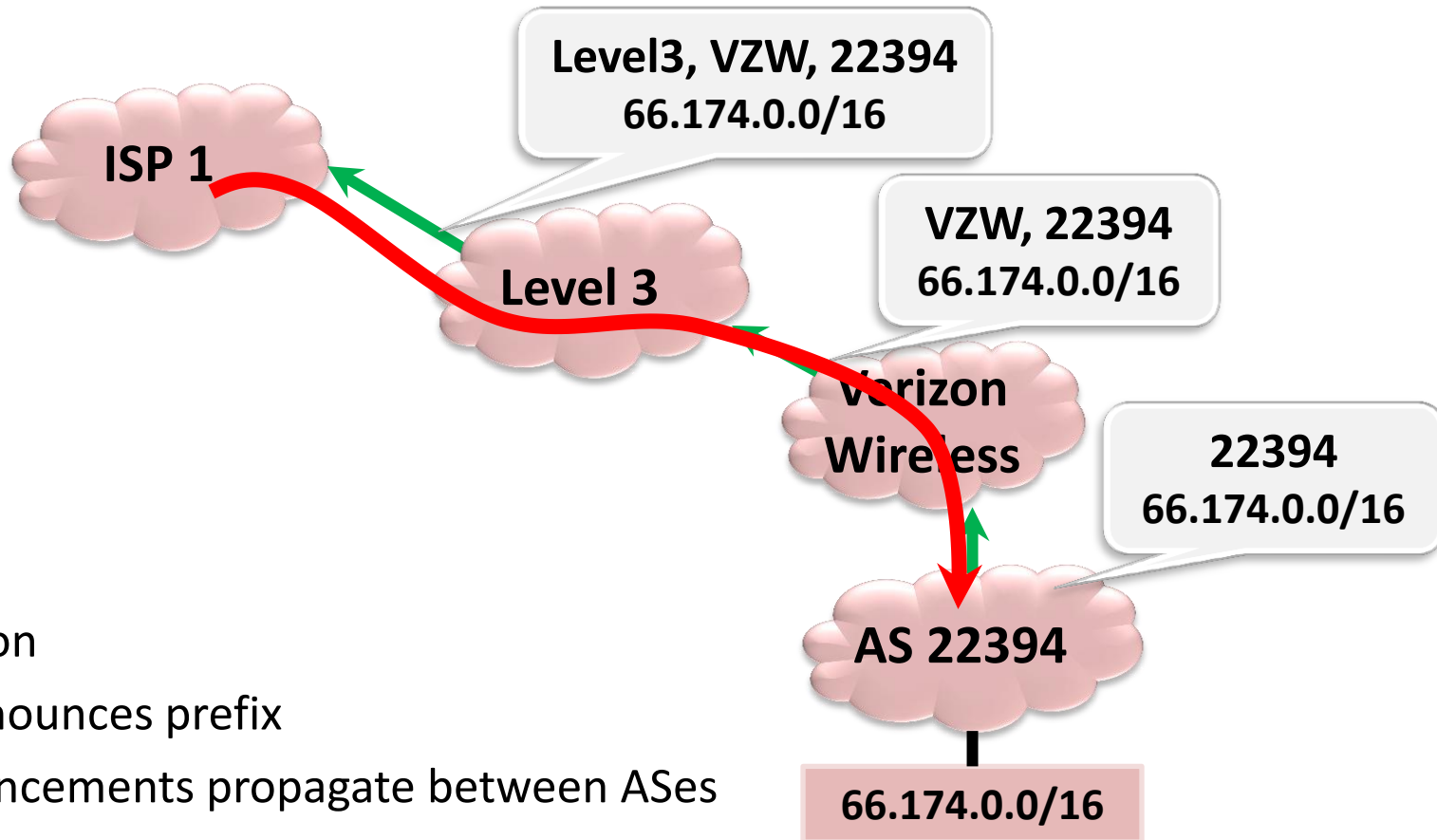
BGP-related Hijacks



Normal operation

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

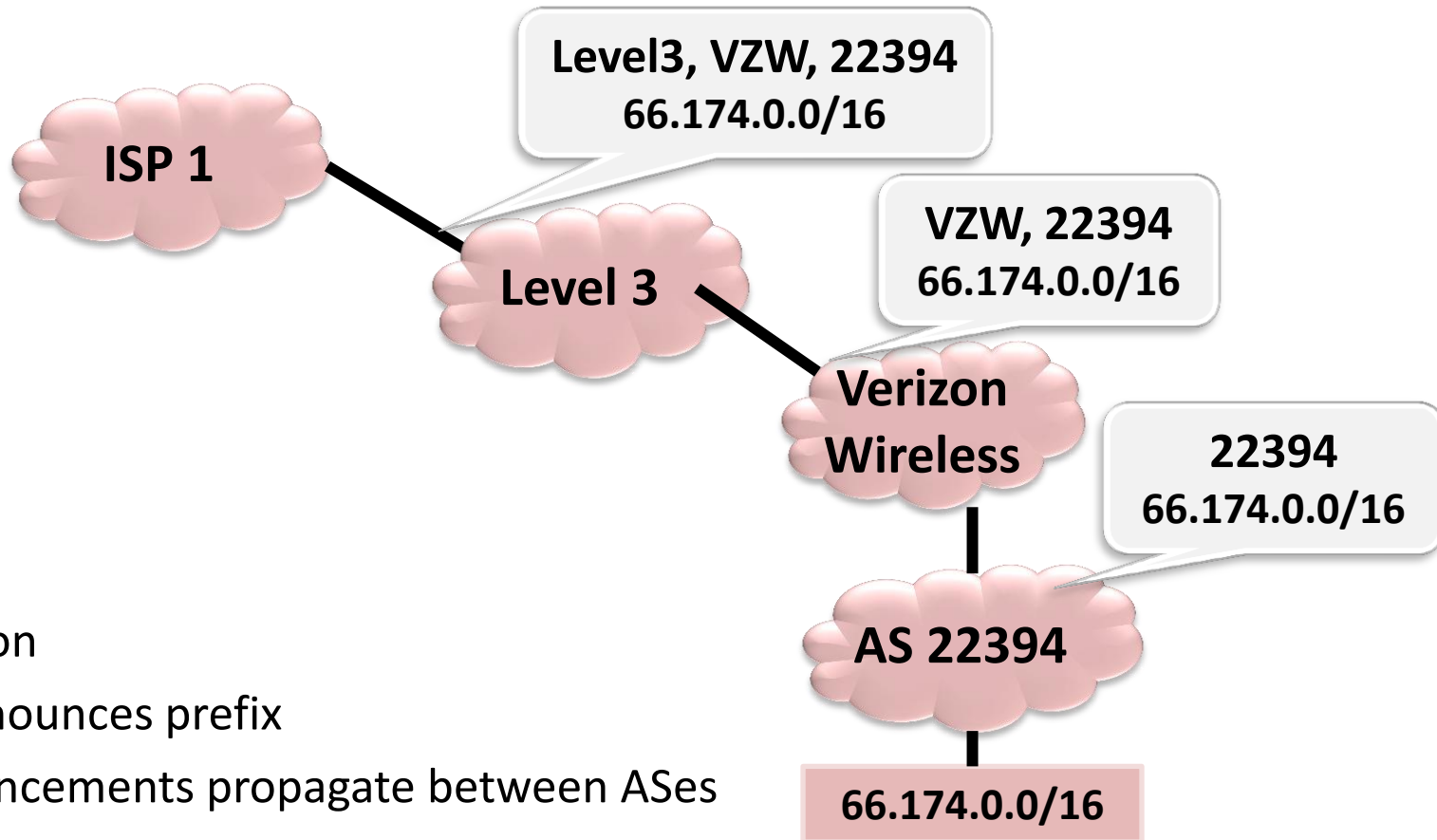
BGP-related Hijacks



Normal operation

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

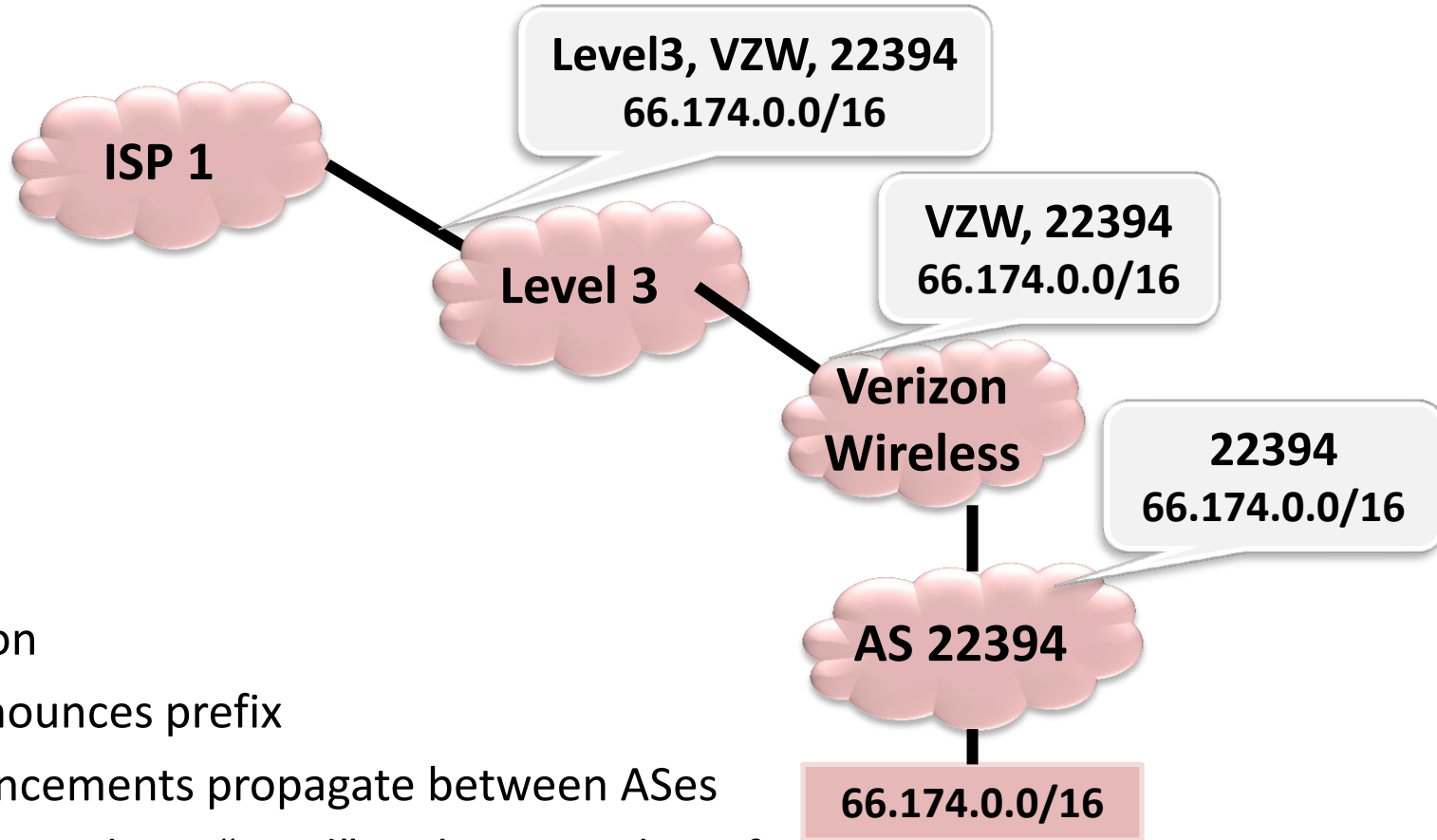
BGP-related Hijacks



Normal operation

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

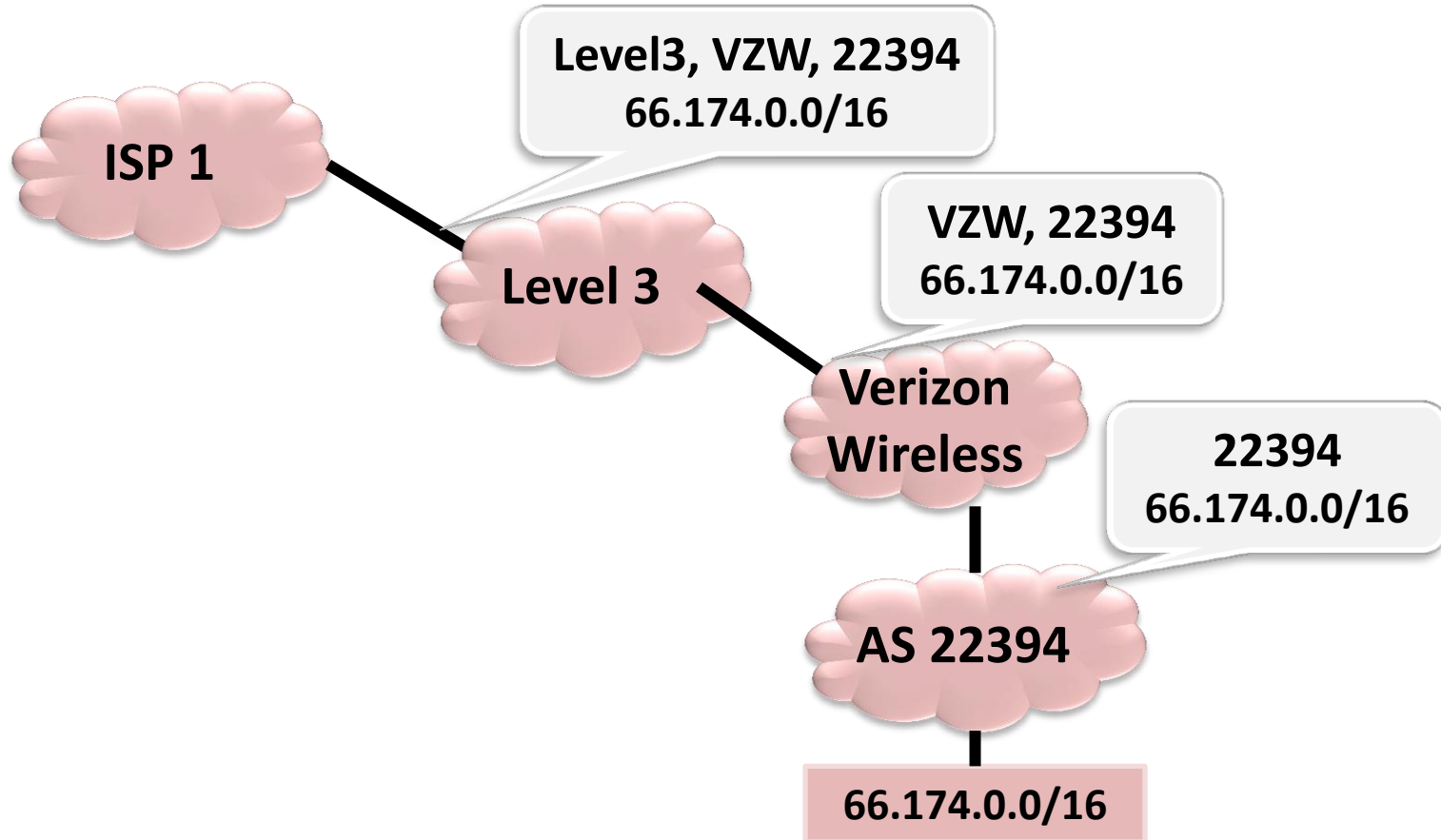
BGP-related Hijacks



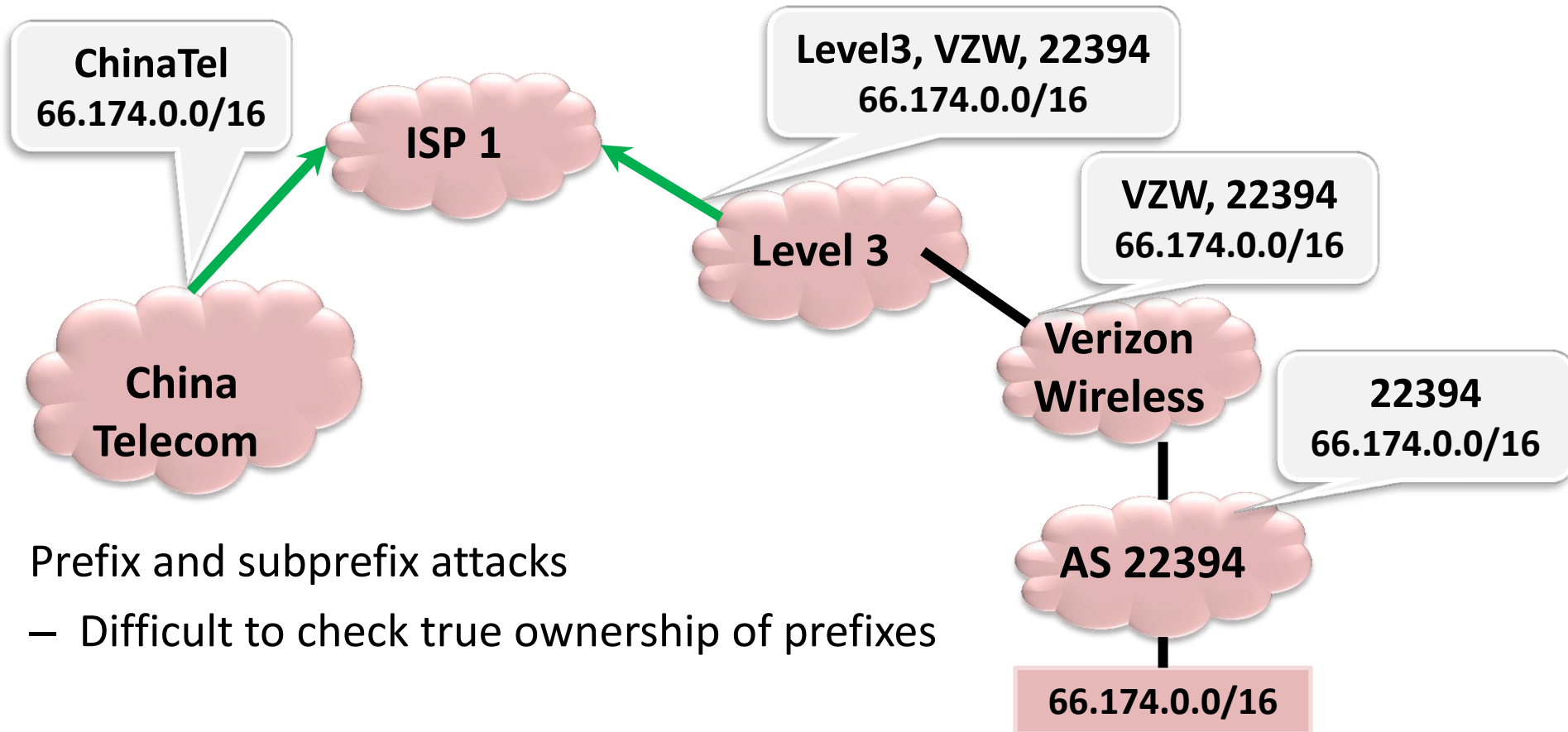
Normal operation

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

BGP-related Hijacks



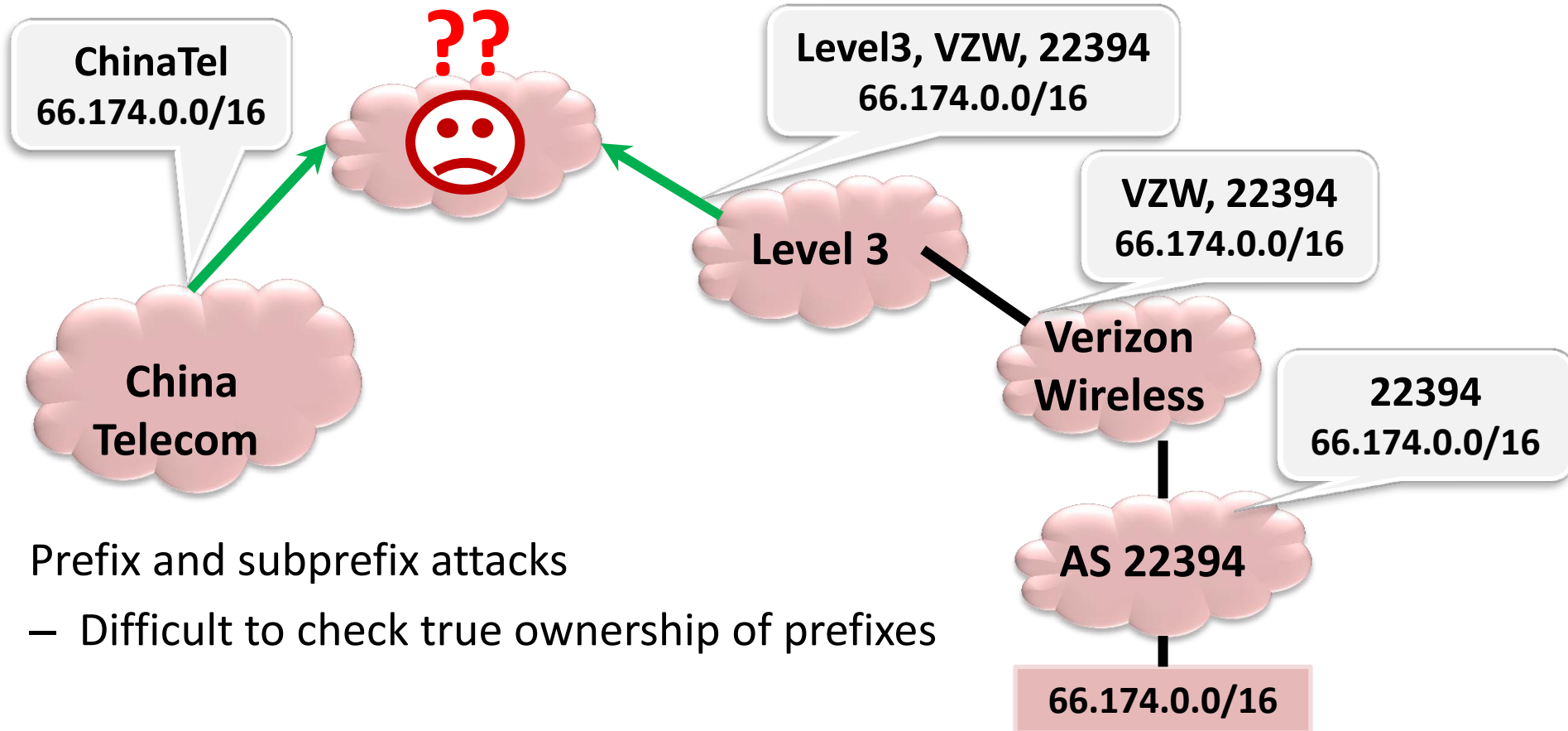
BGP-related Hijacks



Prefix and subprefix attacks

– Difficult to check true ownership of prefixes

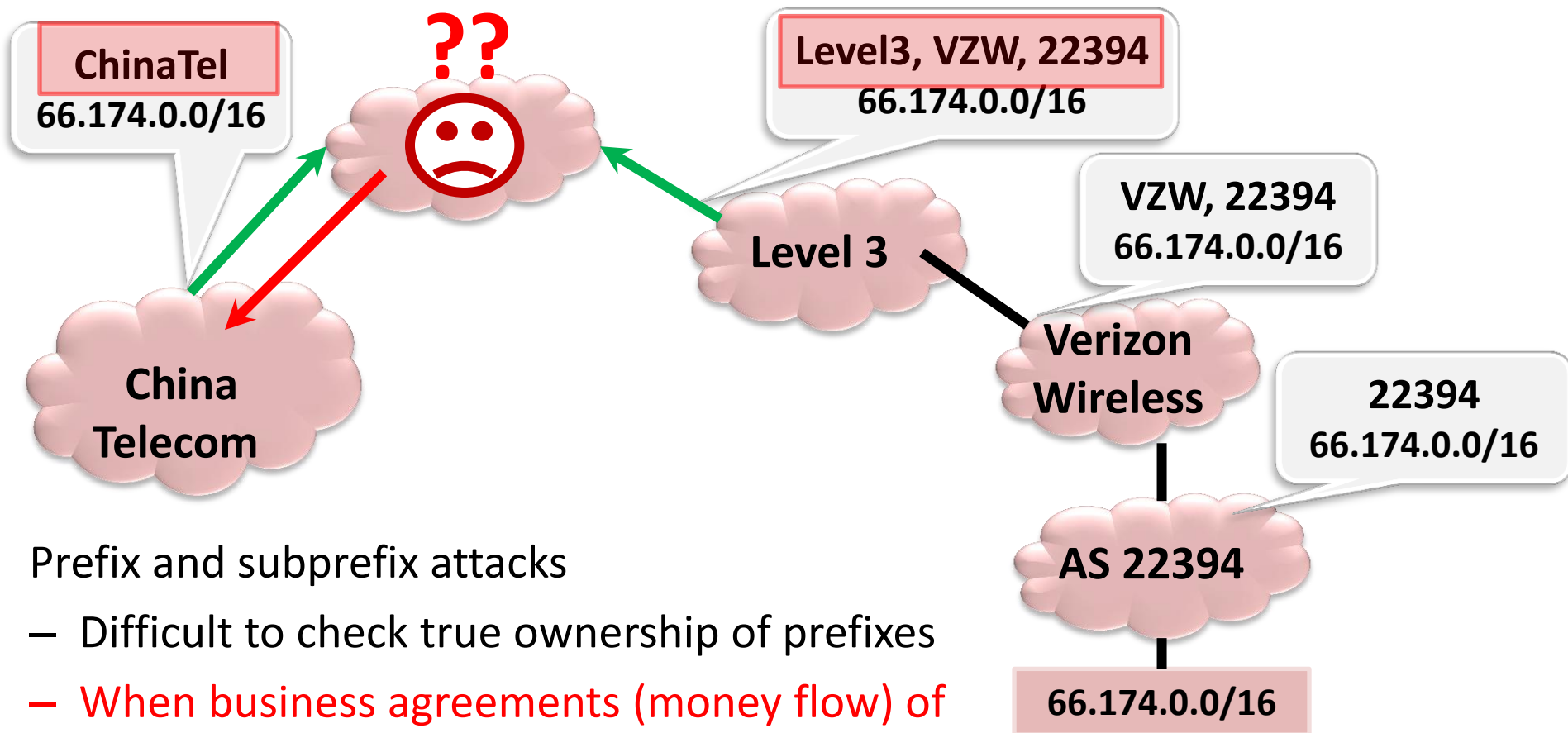
BGP-related Hijacks



Prefix and subprefix attacks

– Difficult to check true ownership of prefixes

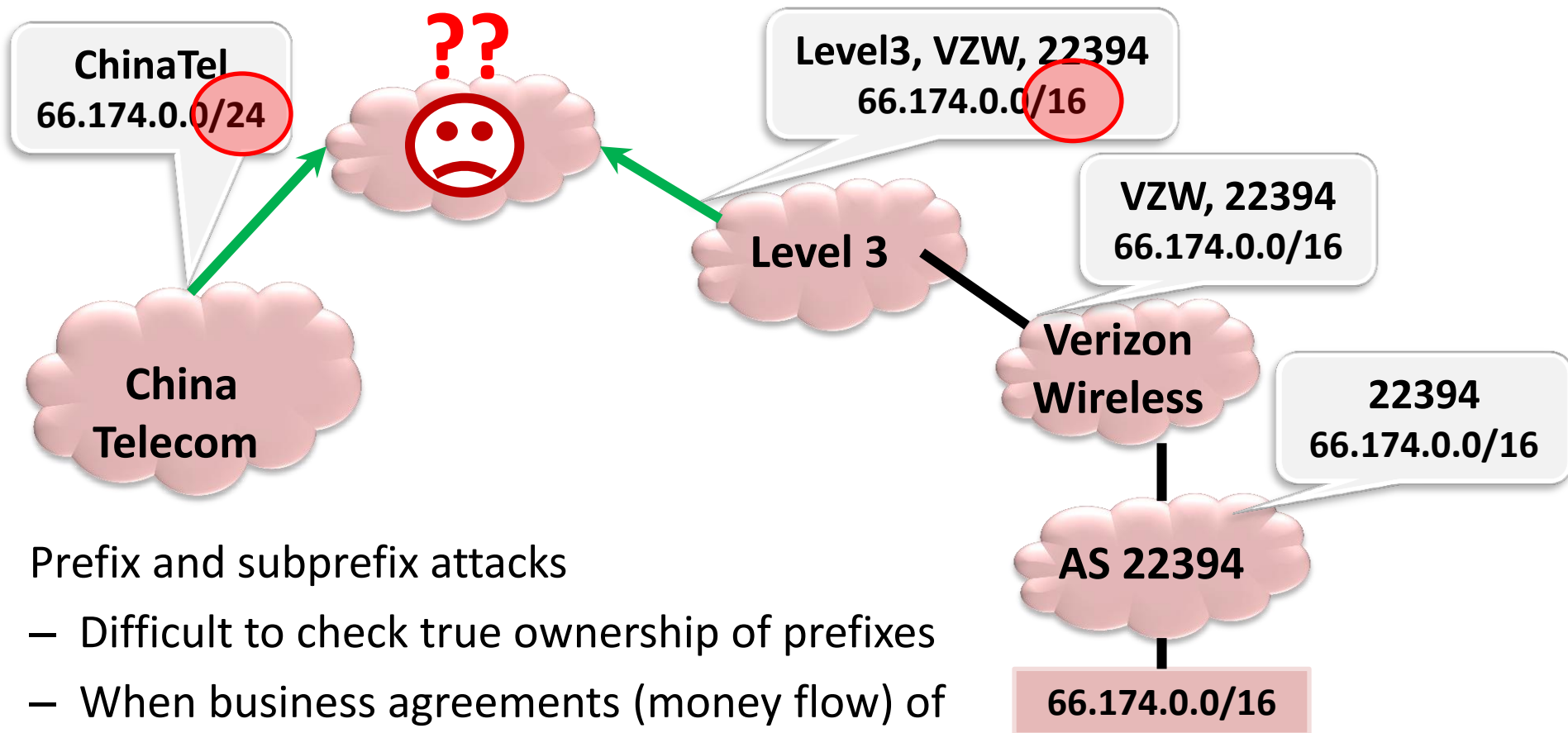
BGP-related Hijacks



Prefix and subprefix attacks

- Difficult to check true ownership of prefixes
- When business agreements (money flow) of same type, typically pick “shorter” path

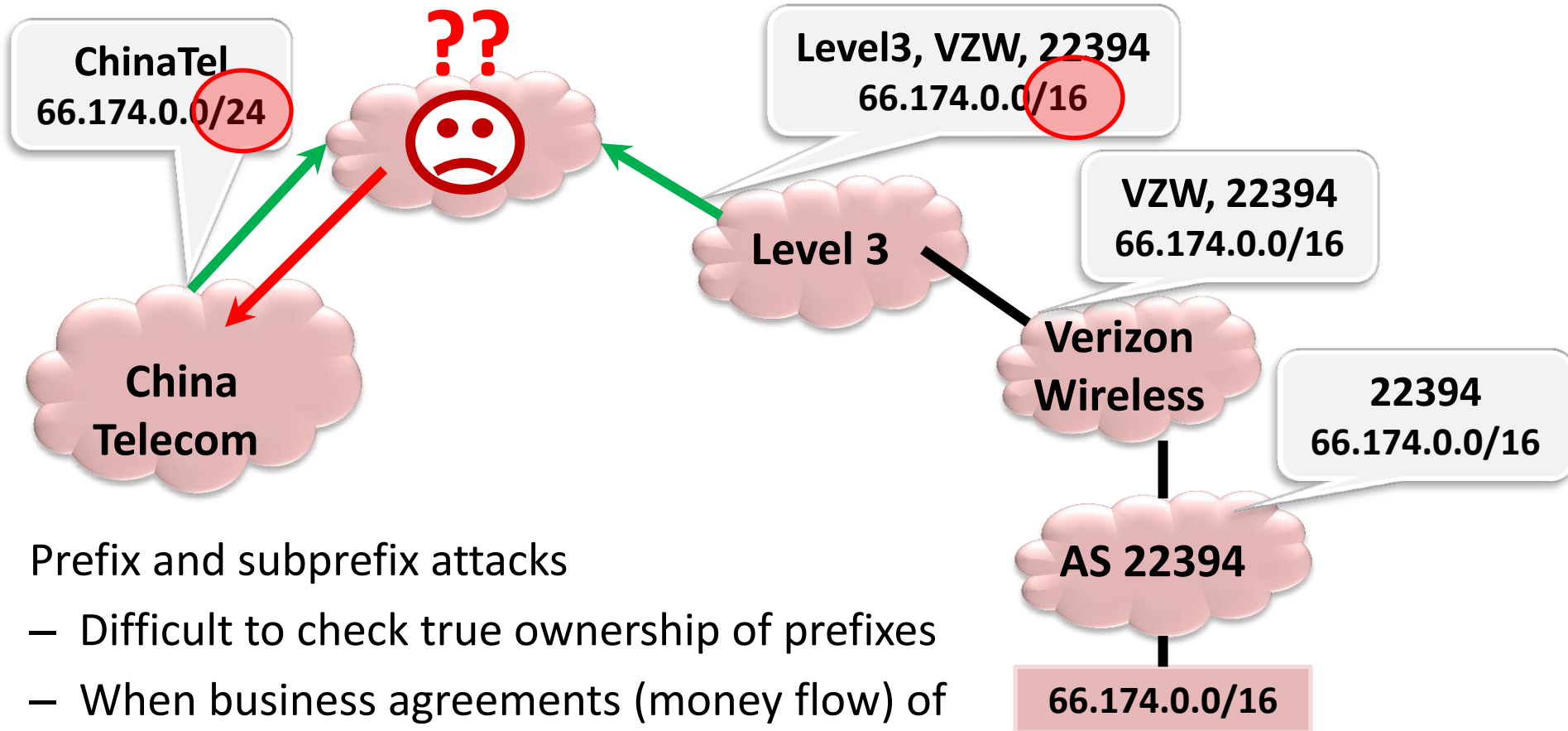
BGP-related Hijacks



Prefix and subprefix attacks

- Difficult to check true ownership of prefixes
- When business agreements (money flow) of same type, typically pick “shorter” path
- Or more specific prefix (subprefix attack)

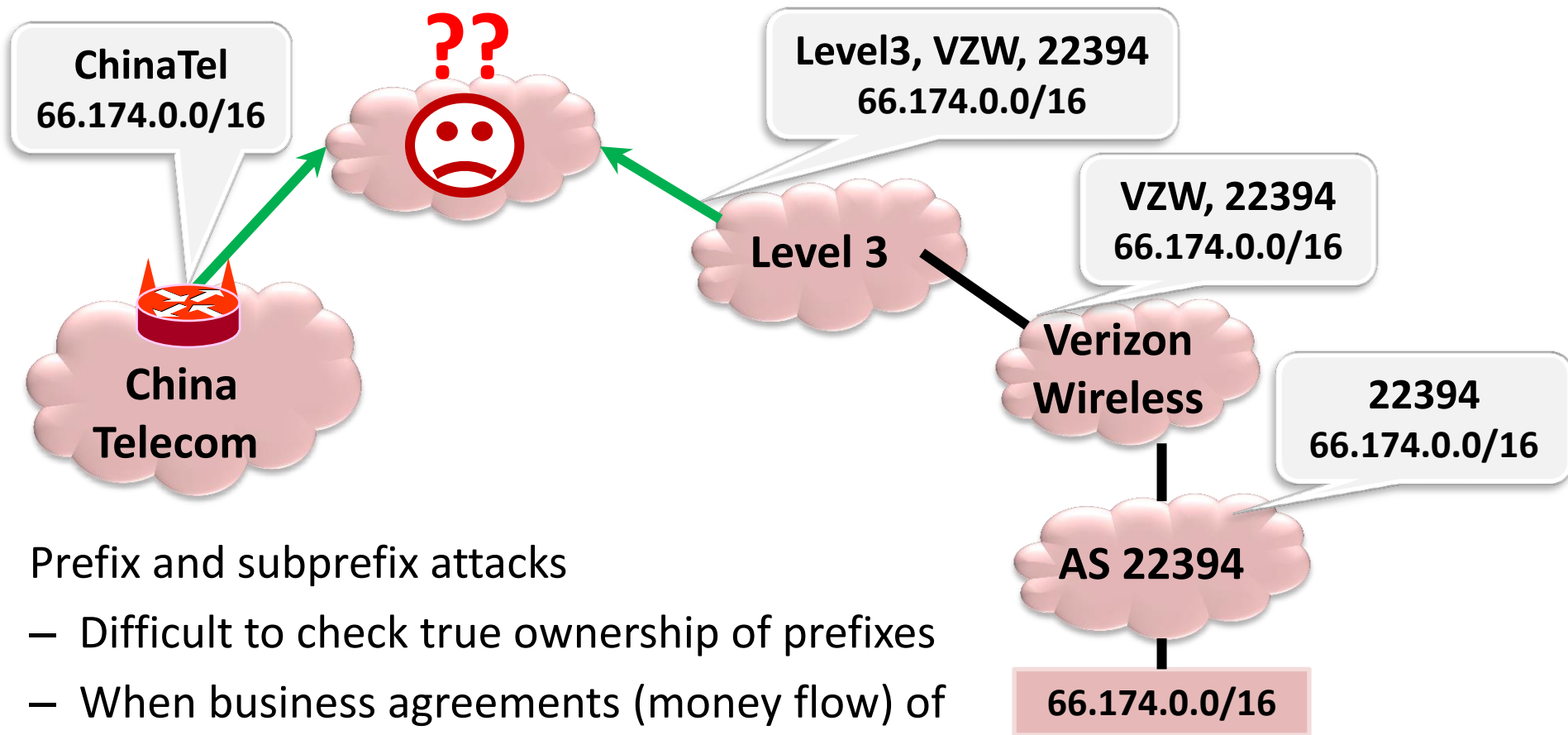
BGP-related Hijacks



Prefix and subprefix attacks

- Difficult to check true ownership of prefixes
- When business agreements (money flow) of same type, typically pick “shorter” path
- Or more specific prefix (subprefix attack)

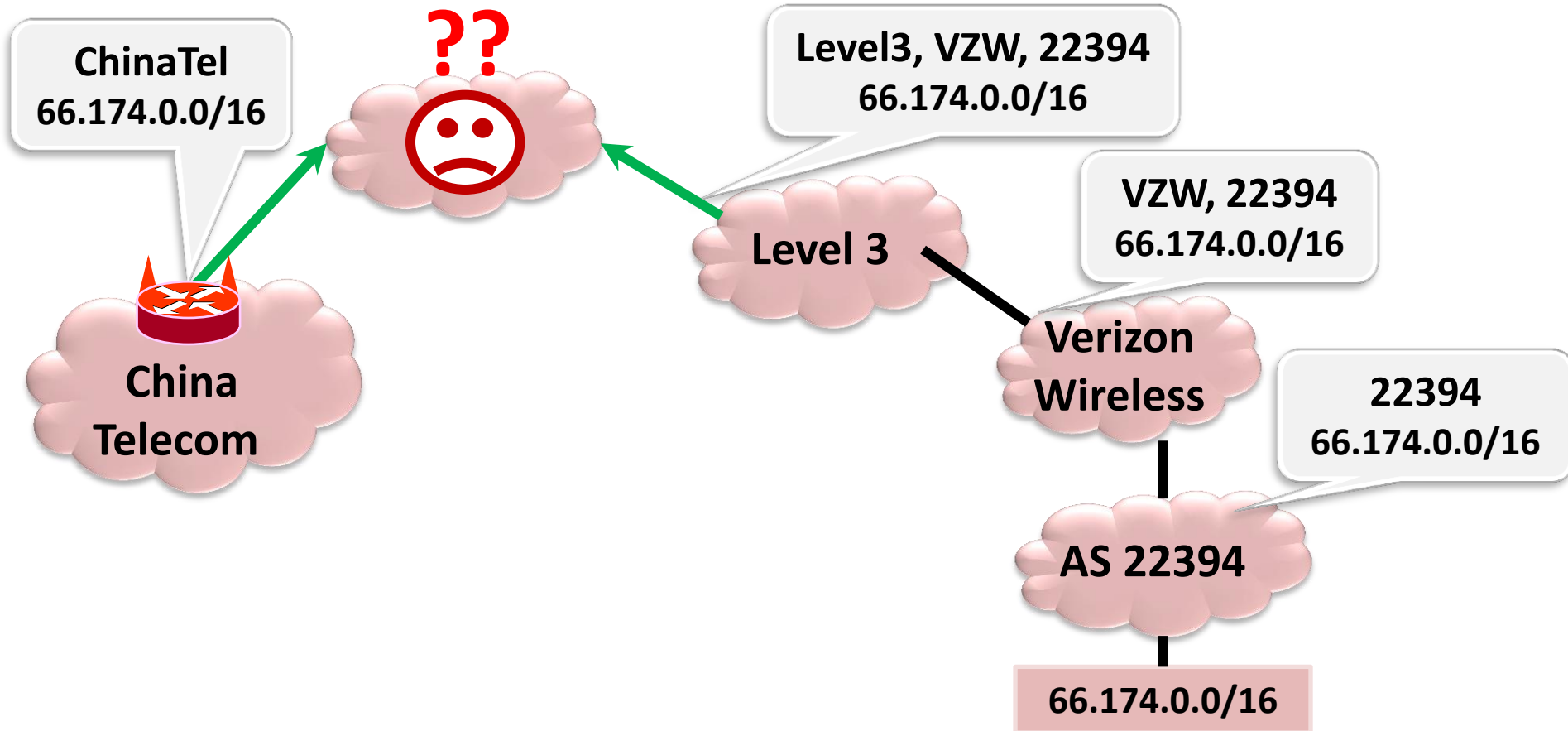
BGP-related Hijacks



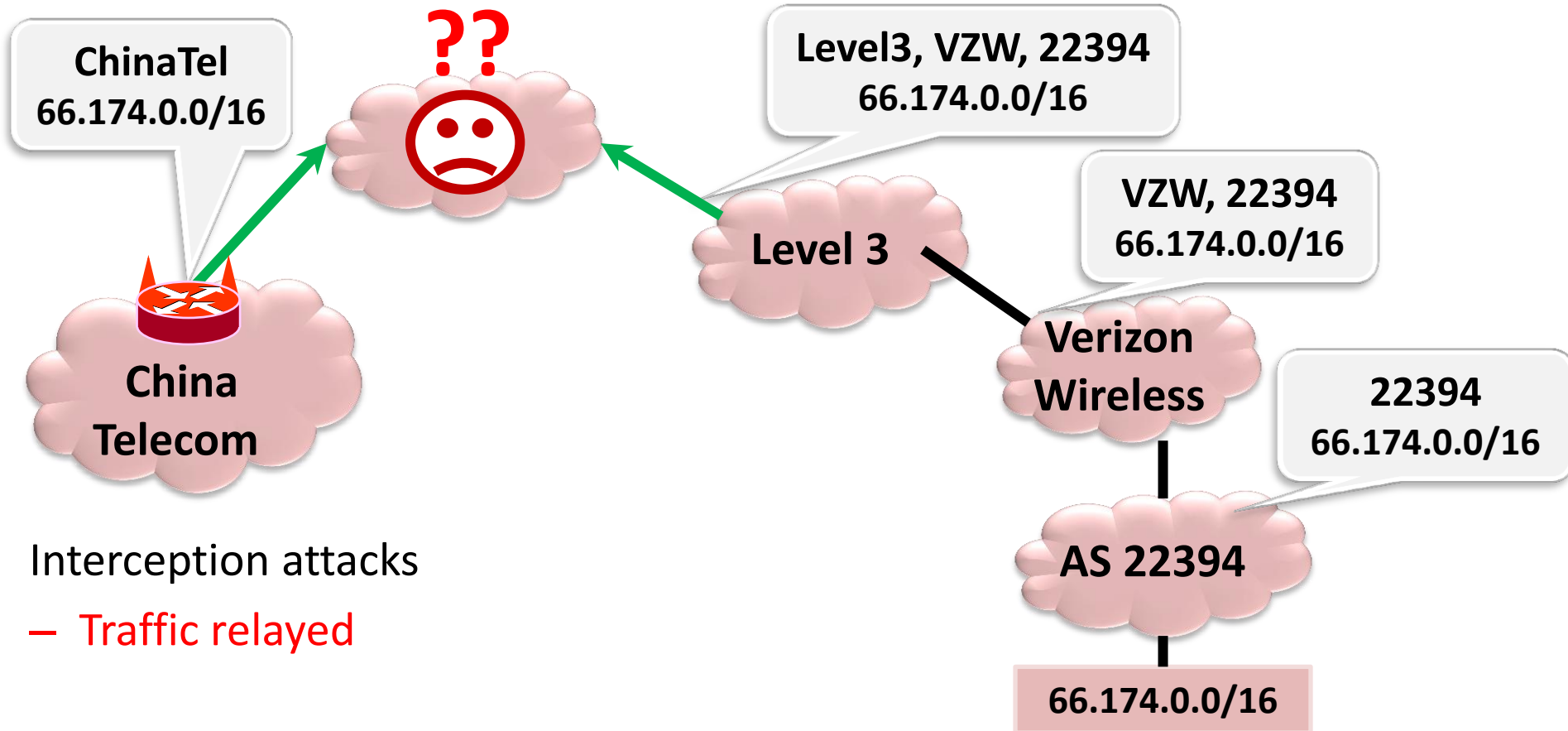
Prefix and subprefix attacks

- Difficult to check true ownership of prefixes
- When business agreements (money flow) of same type, typically pick “shorter” path
- Or more specific prefix (subprefix attack)
- **Apr. 2010: ChinaTel announces 50K prefixes**

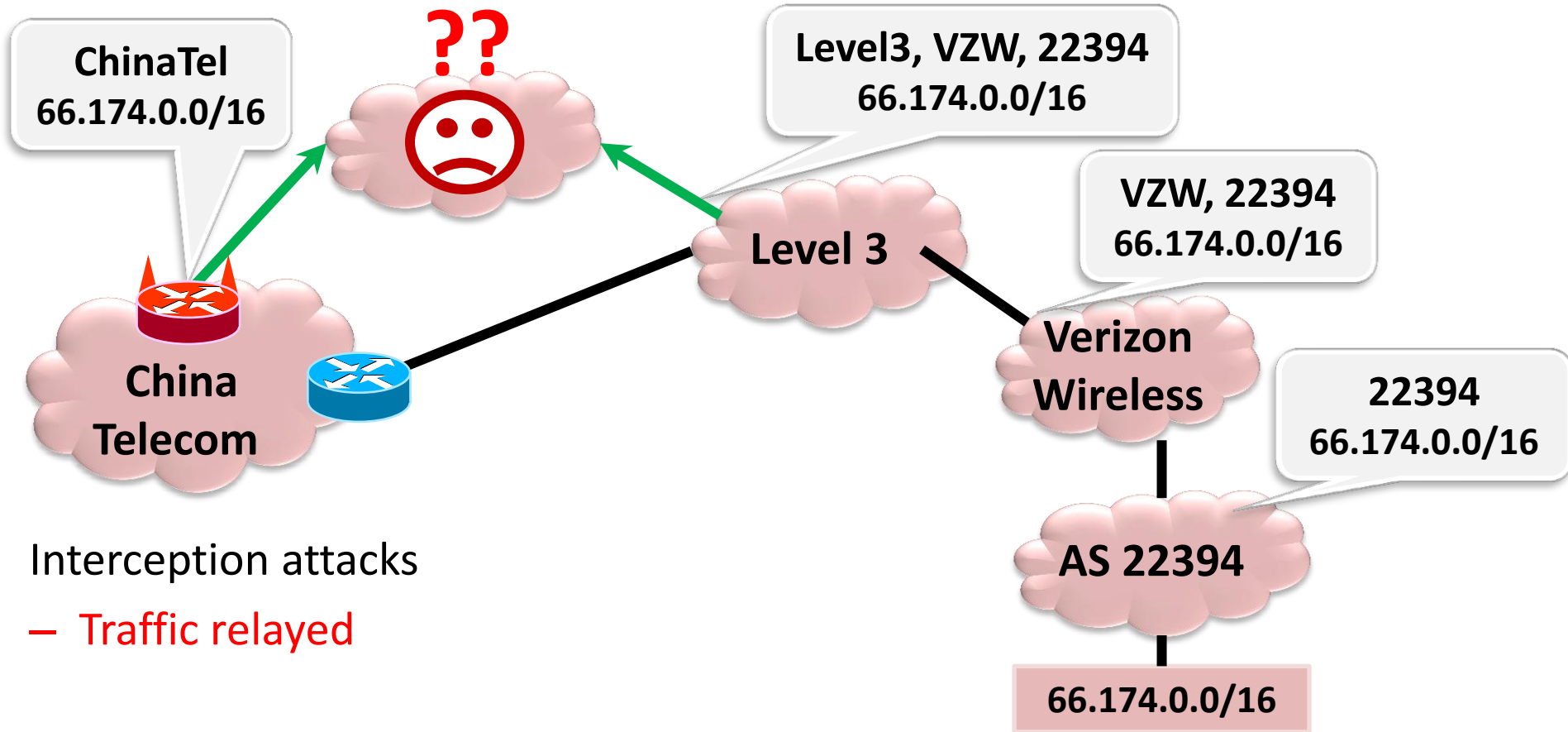
BGP-related Hijacks



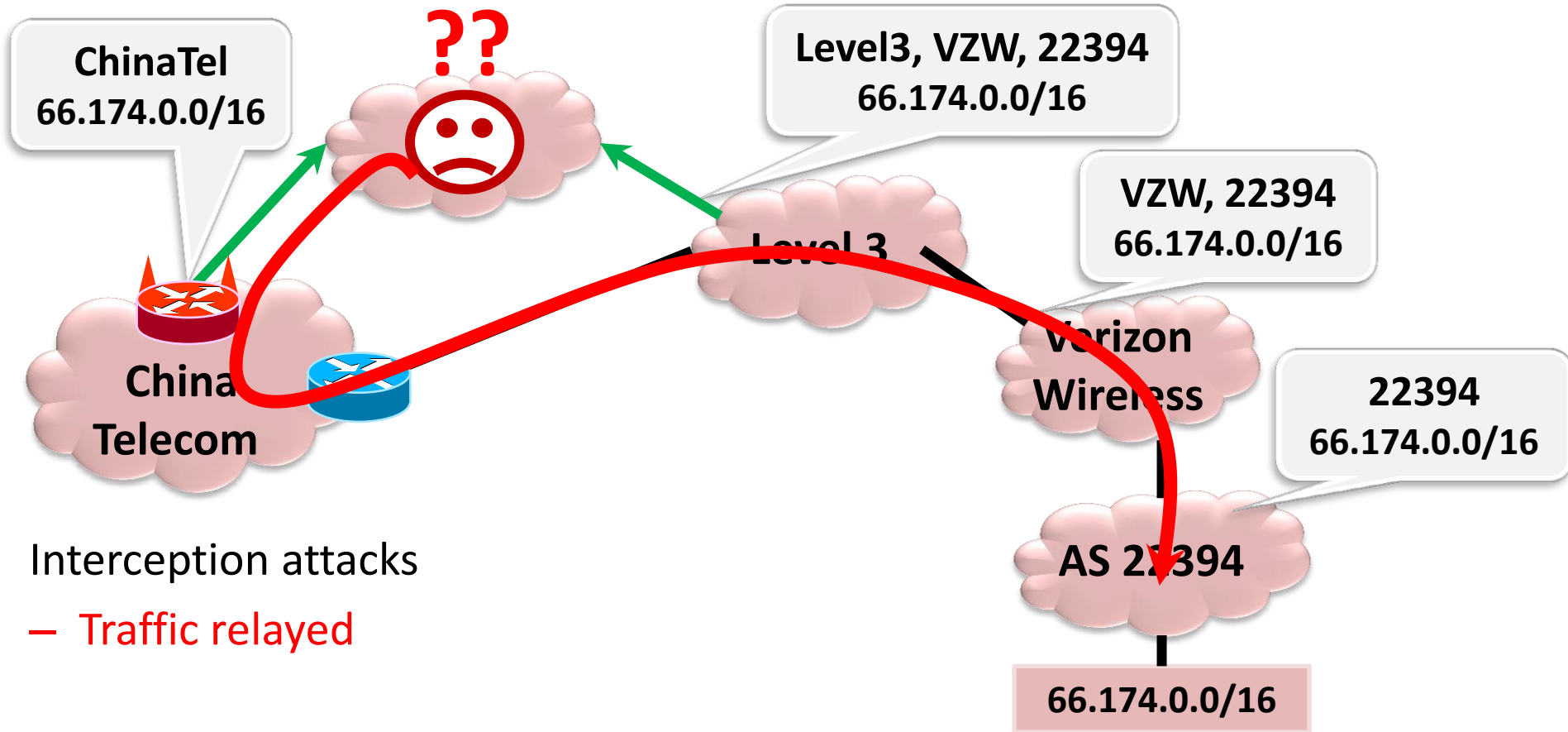
BGP-related Hijacks



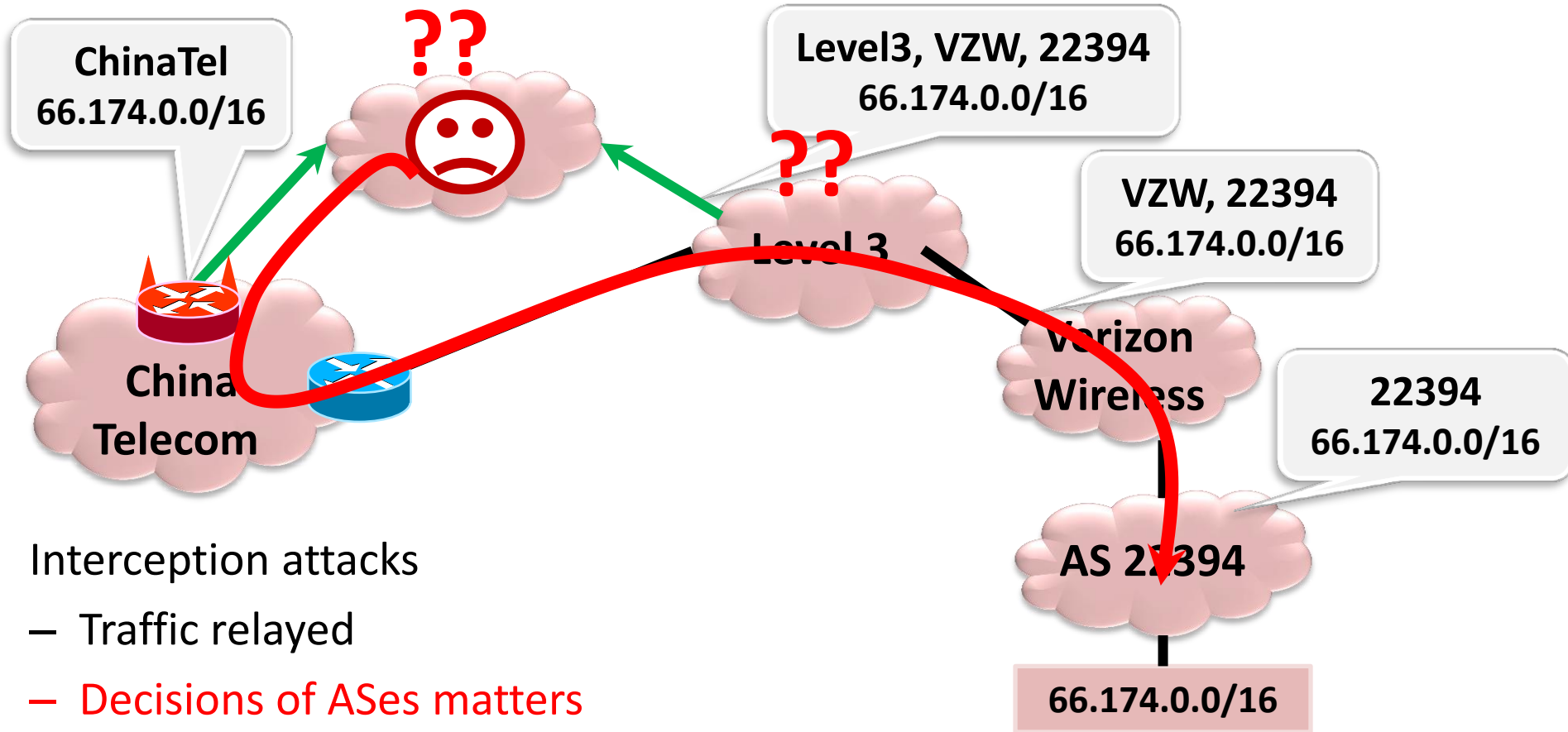
BGP-related Hijacks



BGP-related Hijacks



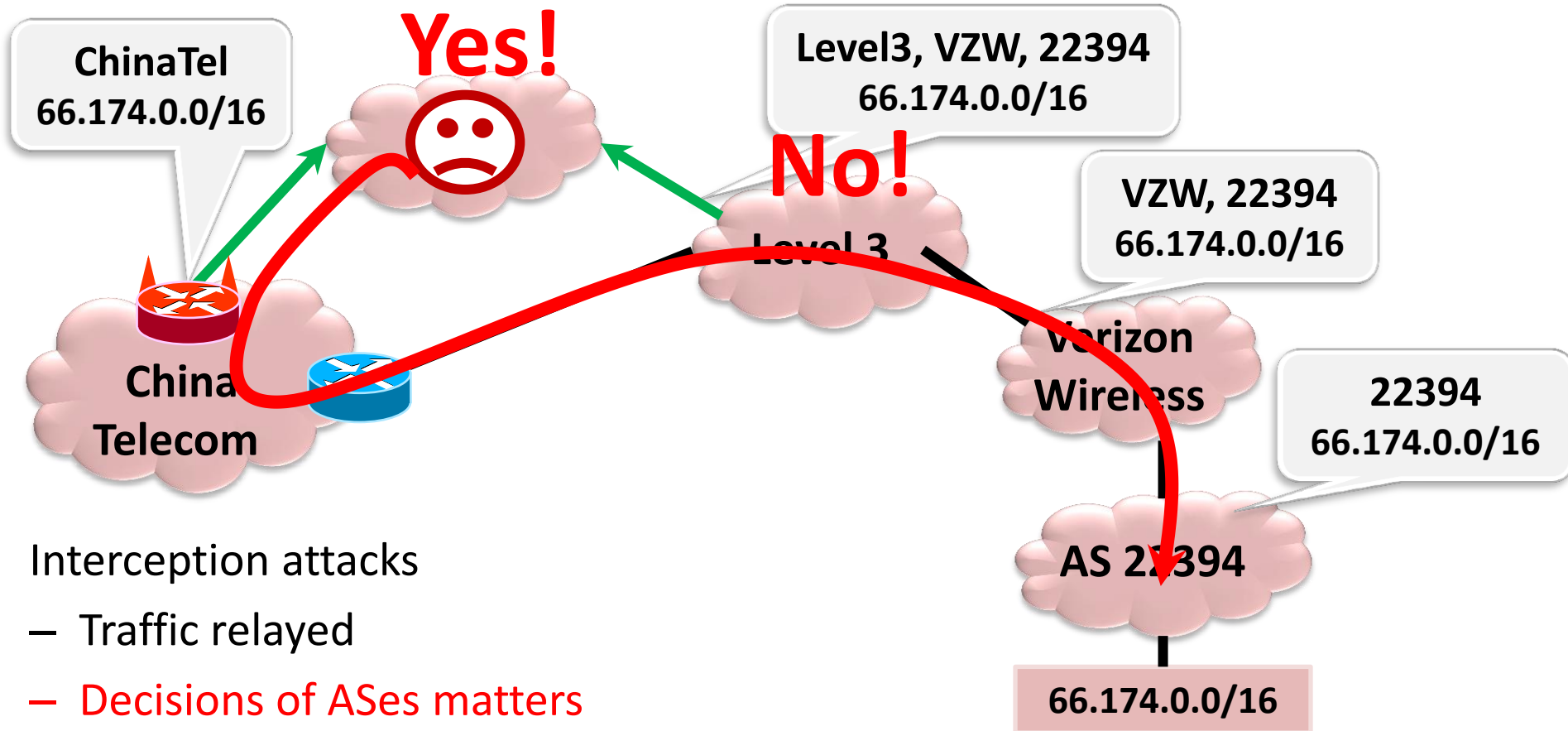
BGP-related Hijacks



Interception attacks

- Traffic relayed
- **Decisions of ASes matters**
 - E.g., selection of ChinaTel path
- Collaboration important

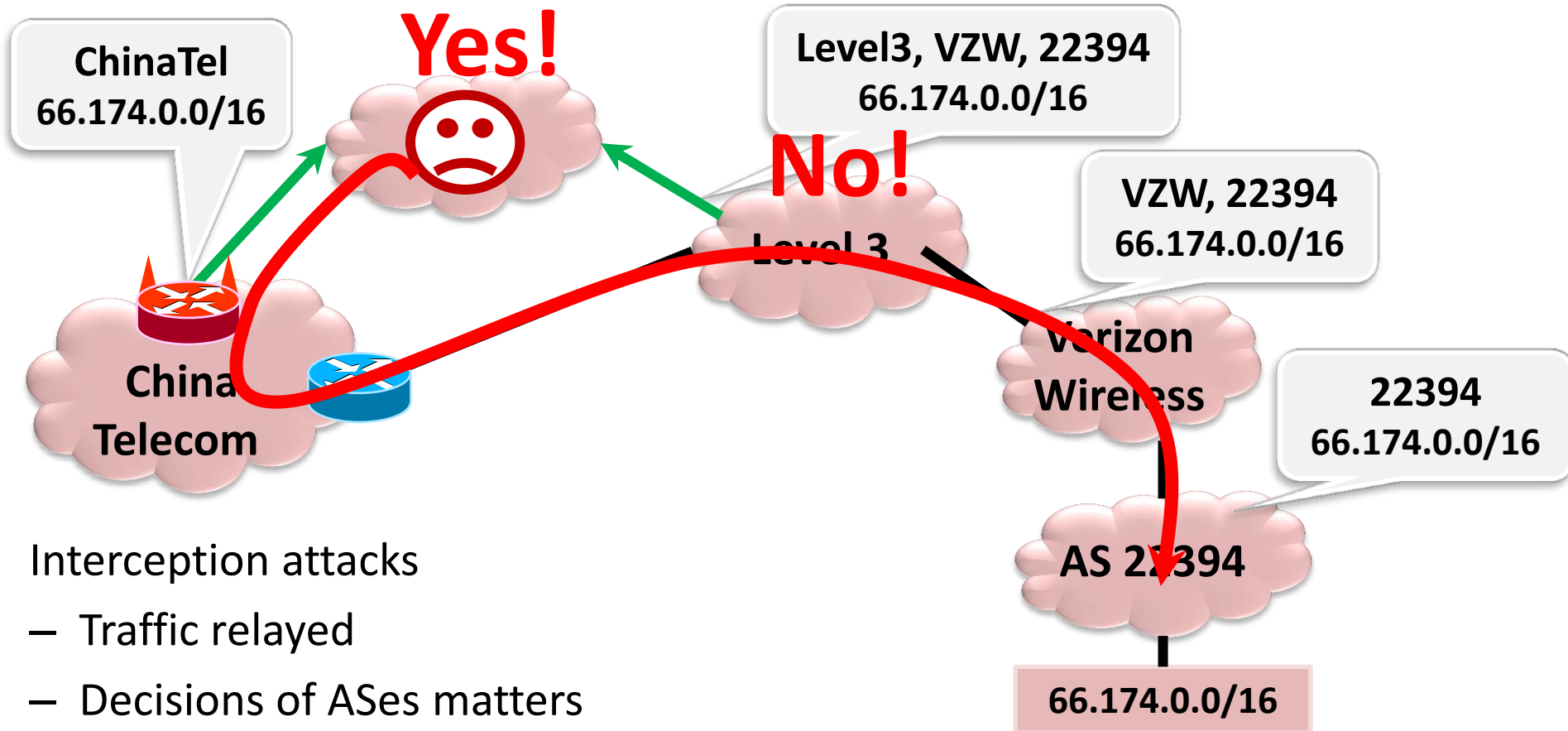
BGP-related Hijacks



Interception attacks

- Traffic relayed
- **Decisions of ASes matters**
 - E.g., selection of ChinaTel path
- Collaboration important

BGP-related Hijacks



Interception attacks

- Traffic relayed
- Decisions of ASes matters
 - E.g., selection of ChinaTel path
- **Collaboration important**

Edge-network-based attacks

- Edge networks and their machines often
 - scanned, probed, or spammed
- Mental agony and personal financial loss
- Threatens nations security and public life in general

Edge-network-based attacks

- Edge networks and their machines often
 - scanned, probed, or spammed
- Mental agony and personal financial loss
- Threatens nations security and public life in general

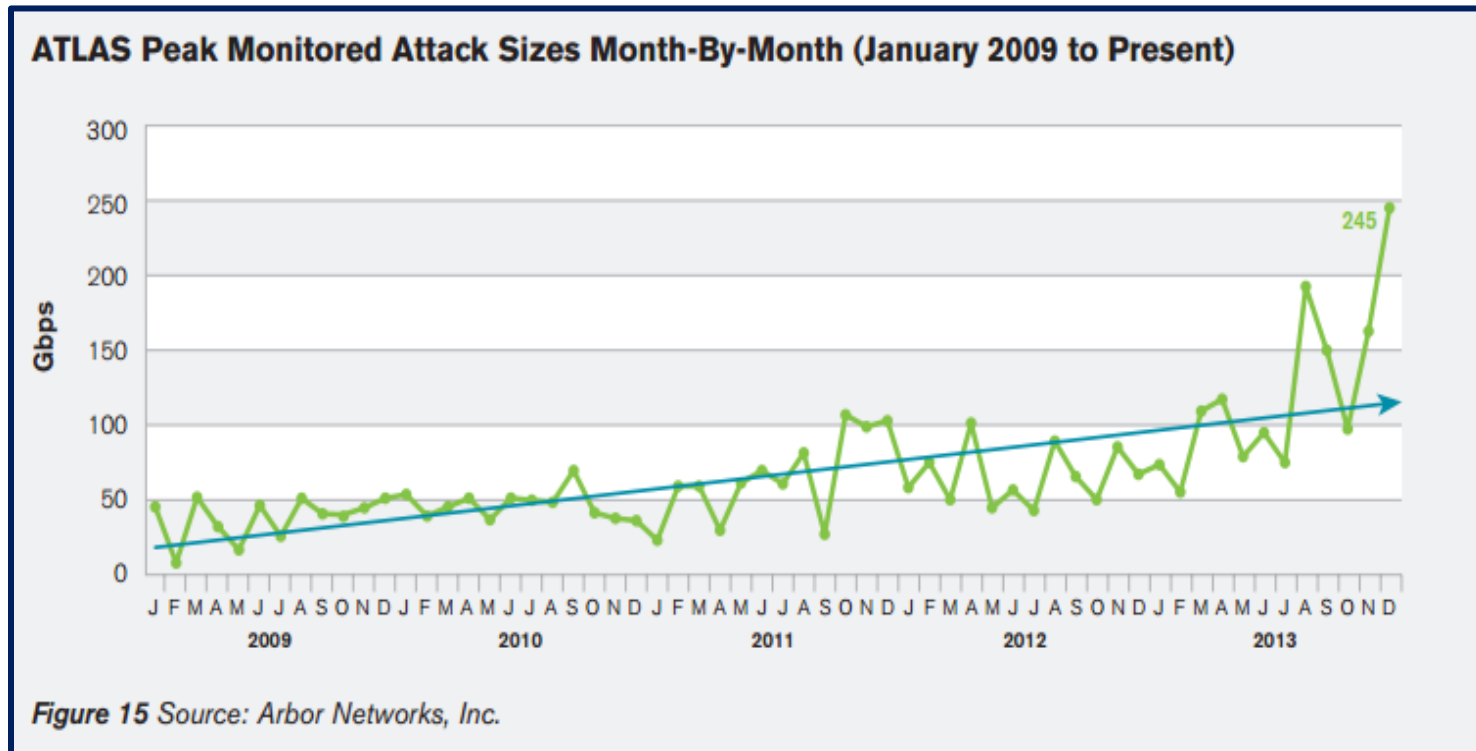
Edge-network-based attacks

- Edge networks and their machines often
 - scanned, probed, or spammed
- **Mental agony and personal financial loss**
- Threatens nations security and public life in general

Edge-network-based attacks

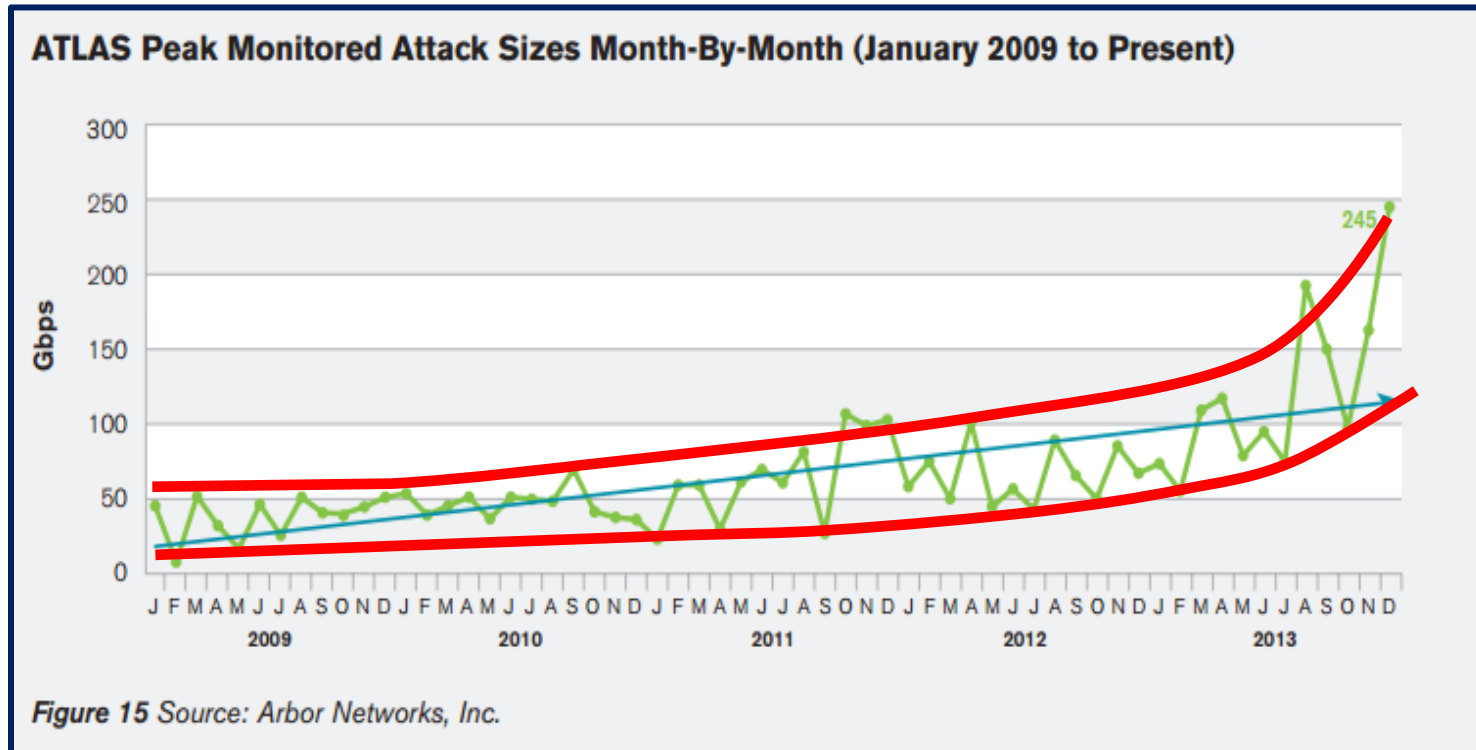
- Edge networks and their machines often
 - scanned, probed, or spammed
- Mental agony and personal financial loss
- Threatens nations security and public life in general

Edge-network-based attacks



- Edge networks and their machines often
 - scanned, probed, or spammed
- Mental agony and personal financial loss
- Threatens nations security and public life in general
- **These attacks are becoming both more frequent and bigger ...**

Edge-network-based attacks



- Edge networks and their machines often
 - scanned, probed, or spammed
- Mental agony and personal financial loss
- Threatens nations security and public life in general
- **These attacks are becoming both more frequent and bigger ...**

Motivation

- Miscreants mounting increasingly sophisticated attacks
- Attacks often cover multiple domains and behaviors
- Collaboration among network entities can provides richer information

Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- **BGP-related attack detection**
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- **Edge-network based information**
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

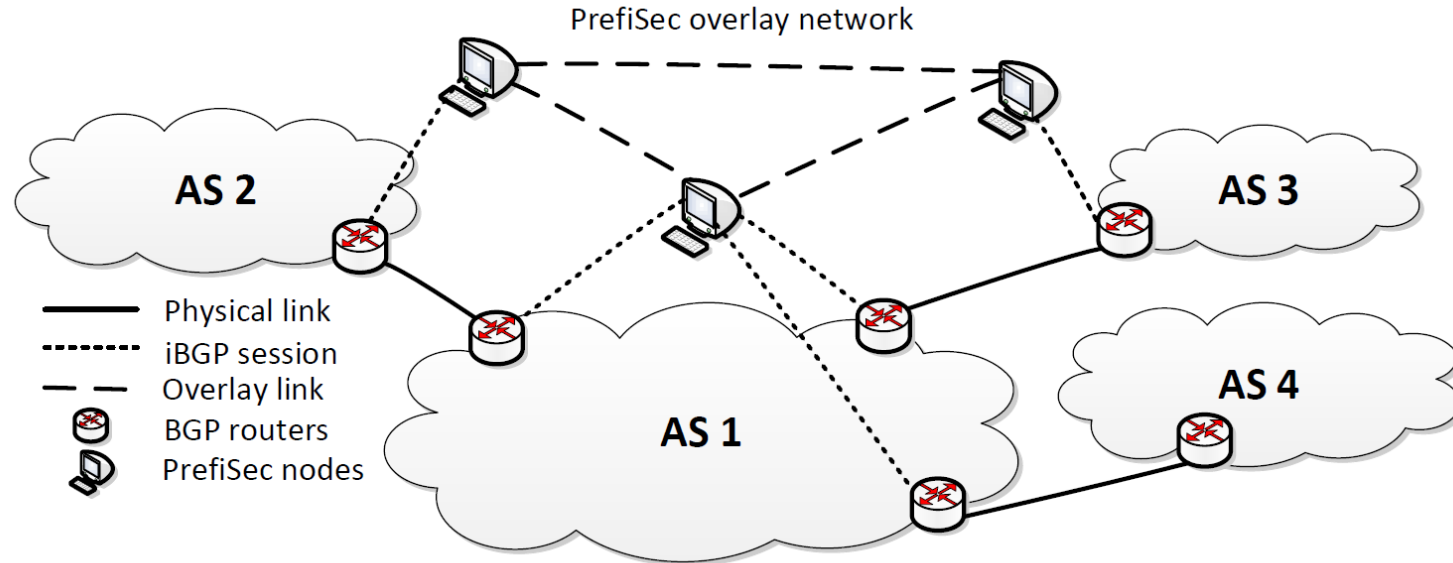
Contributions

- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

Contributions

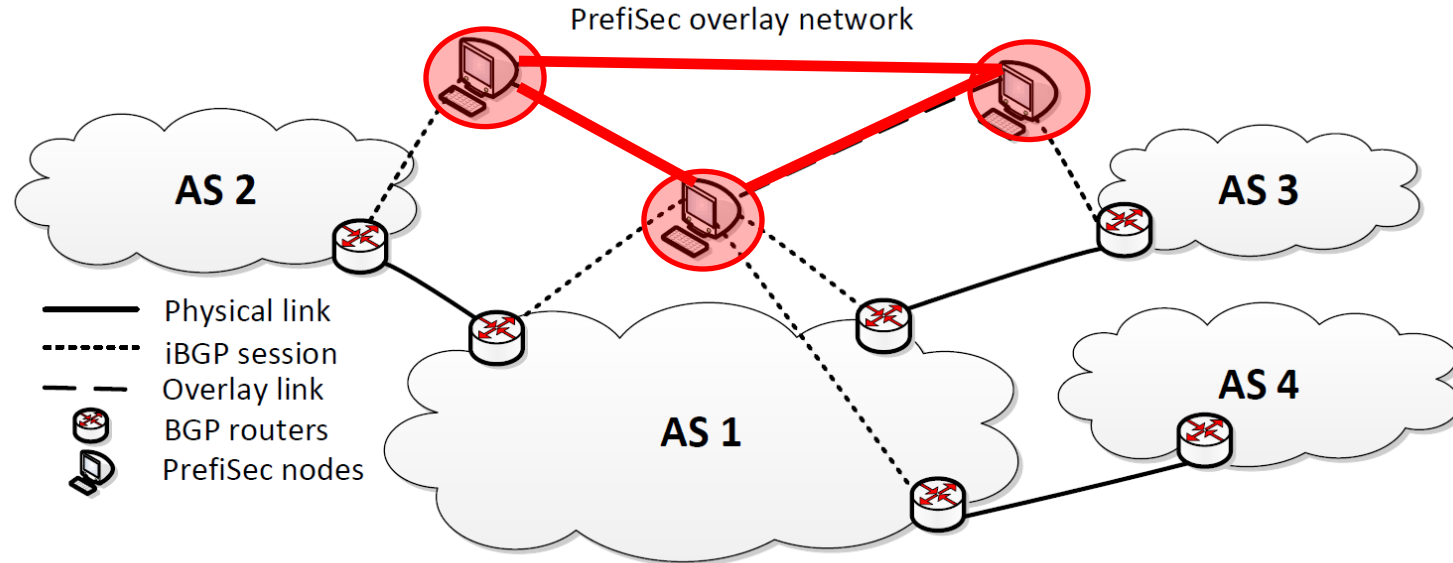
- PrefiSec, a distributed system framework that
 - Provides scalable and effective sharing of network information
 - Provides notification alerts and aggregated evidence information about wide range of attacks
 - Helps organizations keep their security footprints clean
- BGP-related attack detection
 - Prefix hijack detection policy
 - Subprefix hijack detection policy
 - Interception detection policy
- Edge-network based information
 - Prefix monitoring (e.g., scanning, spamming, cross-class detection, attack correlations)
- Data driven overhead analysis

PrefiSec Architecture



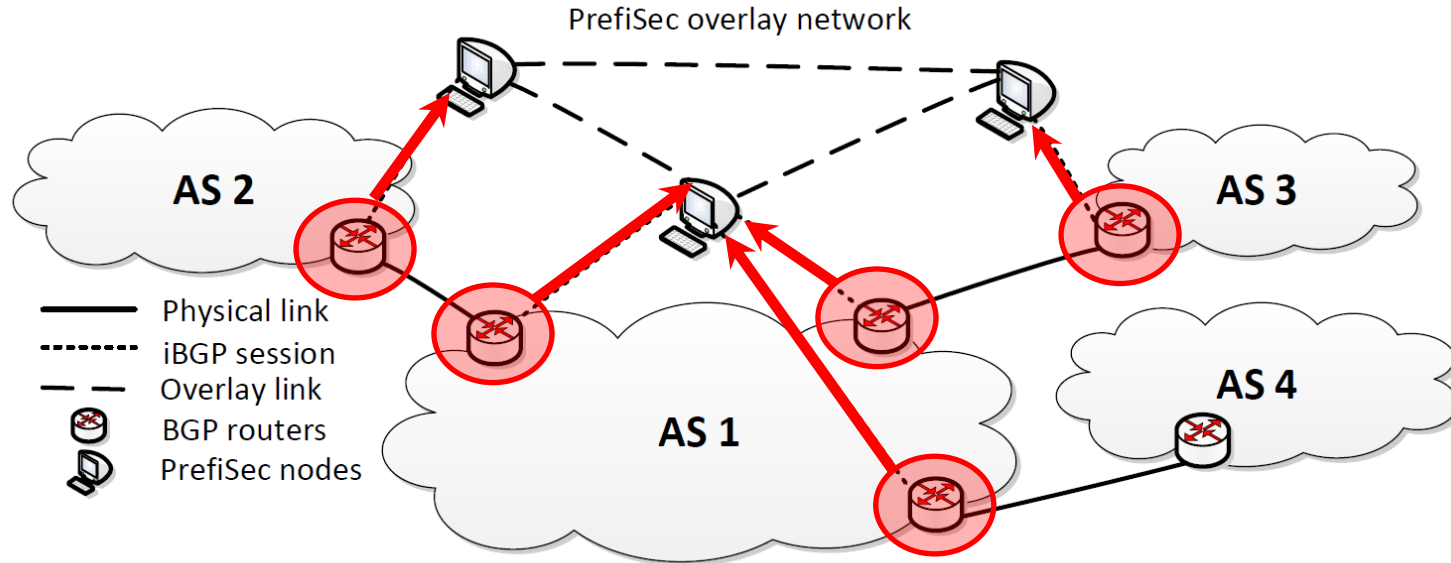
- Overlay network
 - Focus here on interdomain routing attacks

PrefiSec Architecture



- **Overlay network**
 - Focus here on interdomain routing attacks

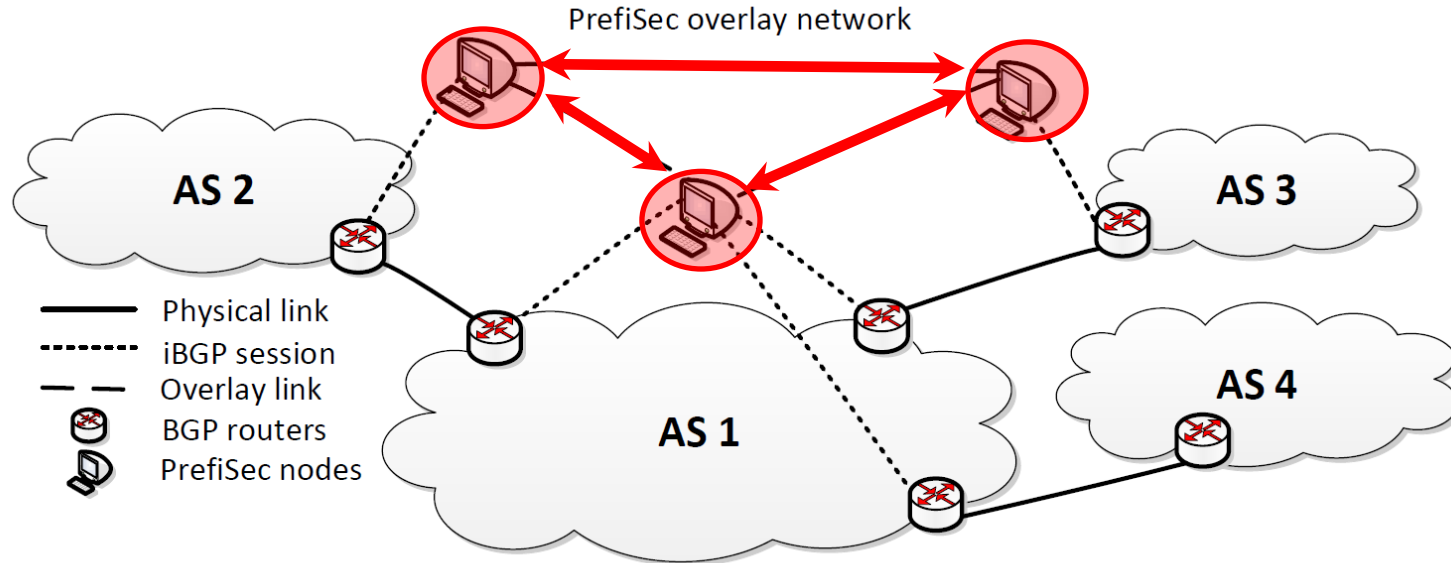
PrefiSec Architecture



- Overlay network
 - Focus here on interdomain routing attacks
- **ASes collect and share BGP updates**
 - E.g., collected at edge routers using RCP¹

¹N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. van der Merwe. The case for separating routing from routers. In Proc. ACM SIGCOMM FDNA, 2004

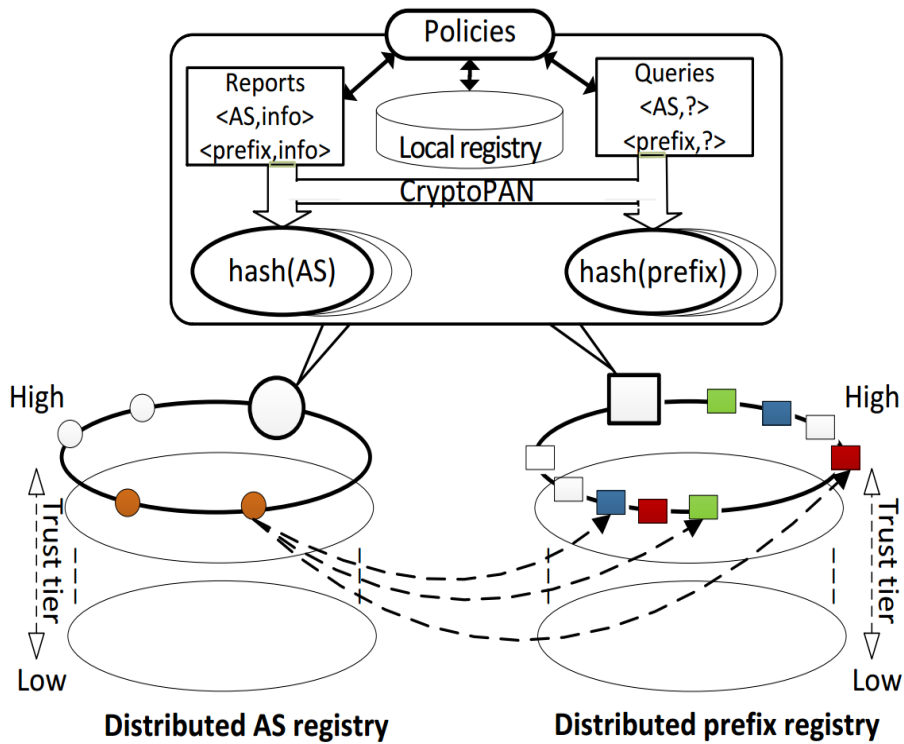
PrefiSec Architecture



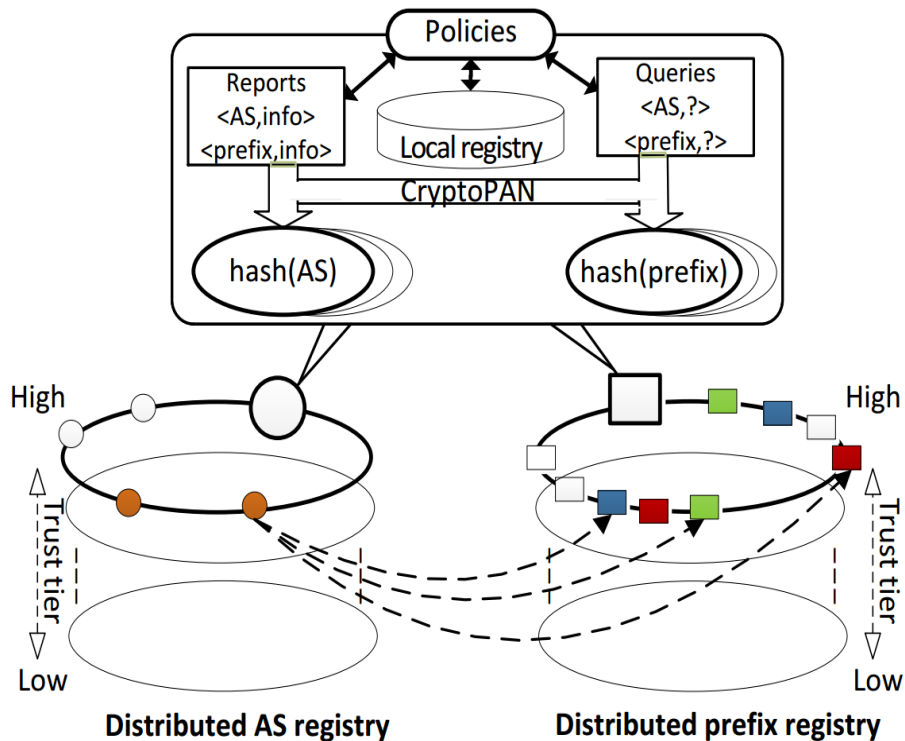
- Overlay network
 - Focus here on interdomain routing attacks
- ASes collect and **share BGP updates**
 - E.g., collected at edge routers using RCP¹

¹N. Feamster, H. Balakrishnan, J. Rexford, A. Shaikh, and J. van der Merwe. The case for separating routing from routers. In Proc. ACM SIGCOMM FDNA, 2004

Components and Structure

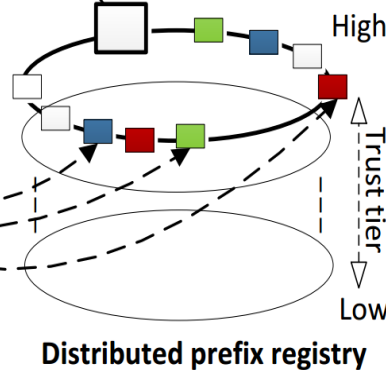
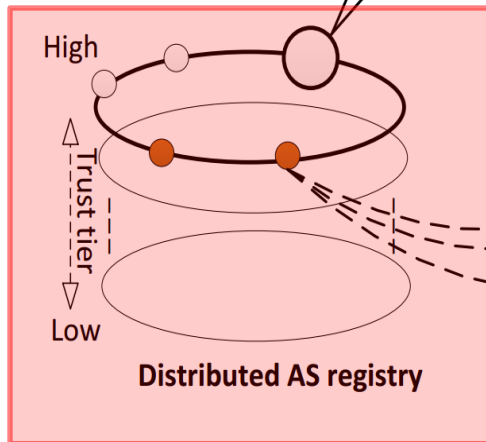
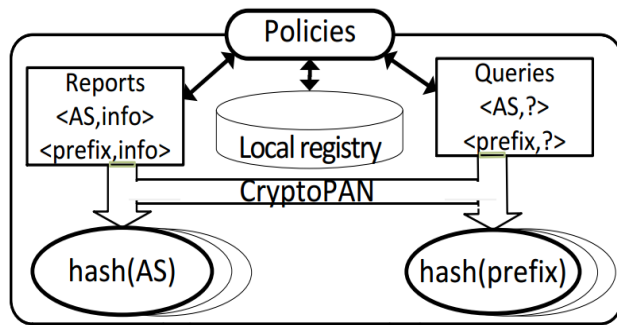


Components and Structure



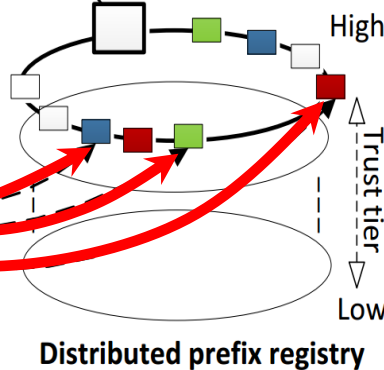
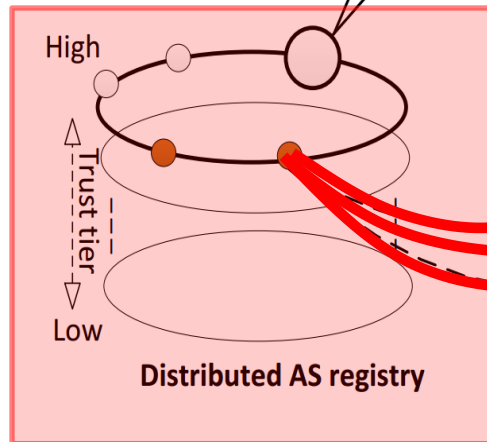
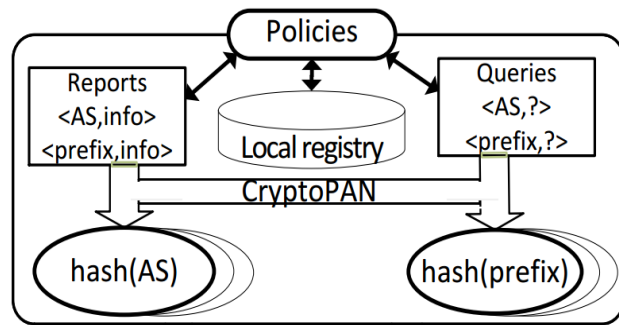
- AS registry
 - Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and Structure



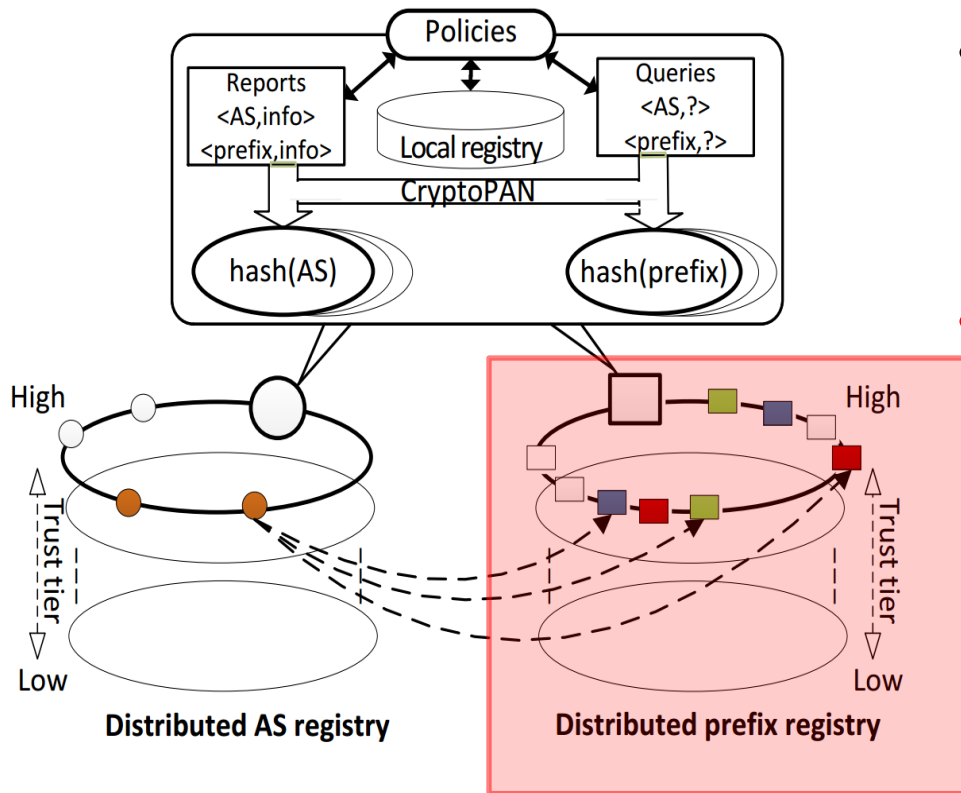
- **AS registry**
 - Information about ASes, their relationships, and AS-to-prefix mappings
- **Prefix registry**
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and Structure



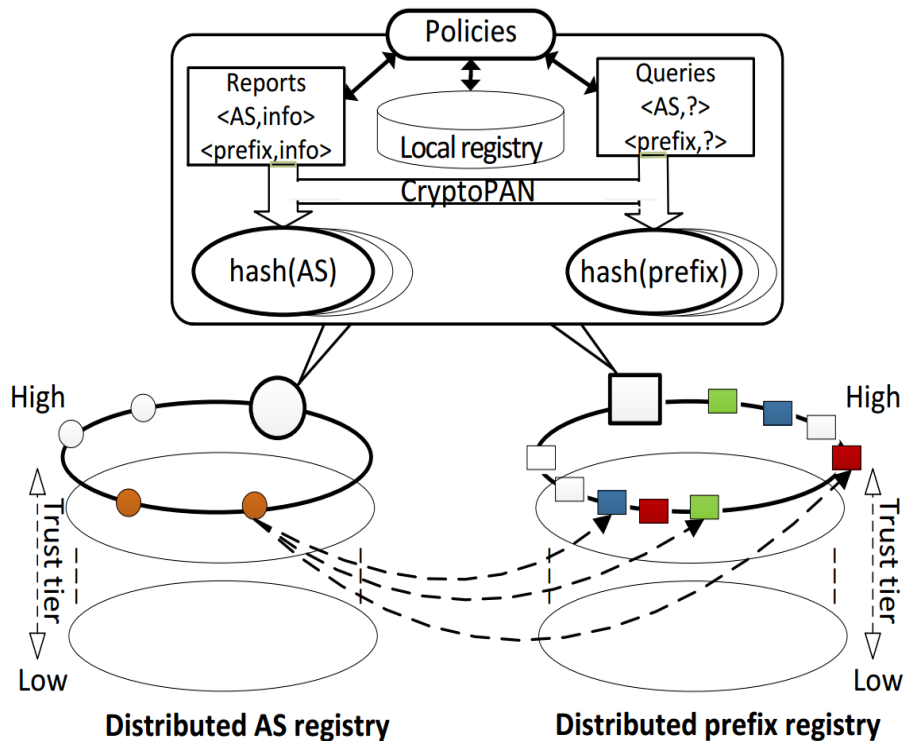
- **AS registry**
 - Information about ASes, their relationships, and **AS-to-prefix mappings**
- **Prefix registry**
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and Structure



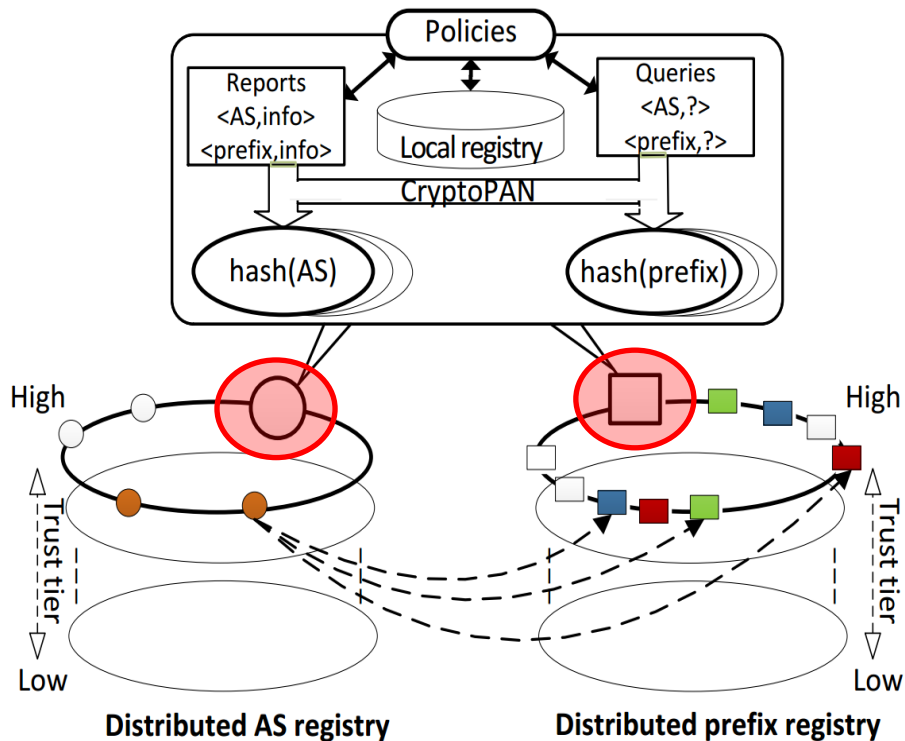
- **AS registry**
 - Information about ASes, their relationships, and AS-to-prefix mappings
- **Prefix registry**
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and Structure



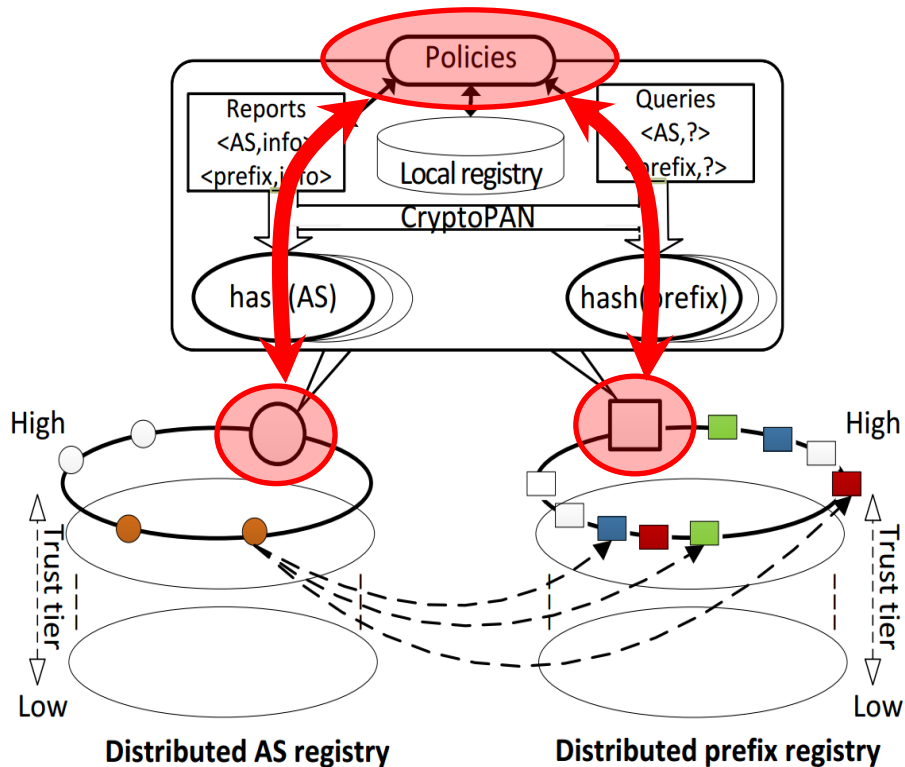
- AS registry
 - Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities

Components and Structure



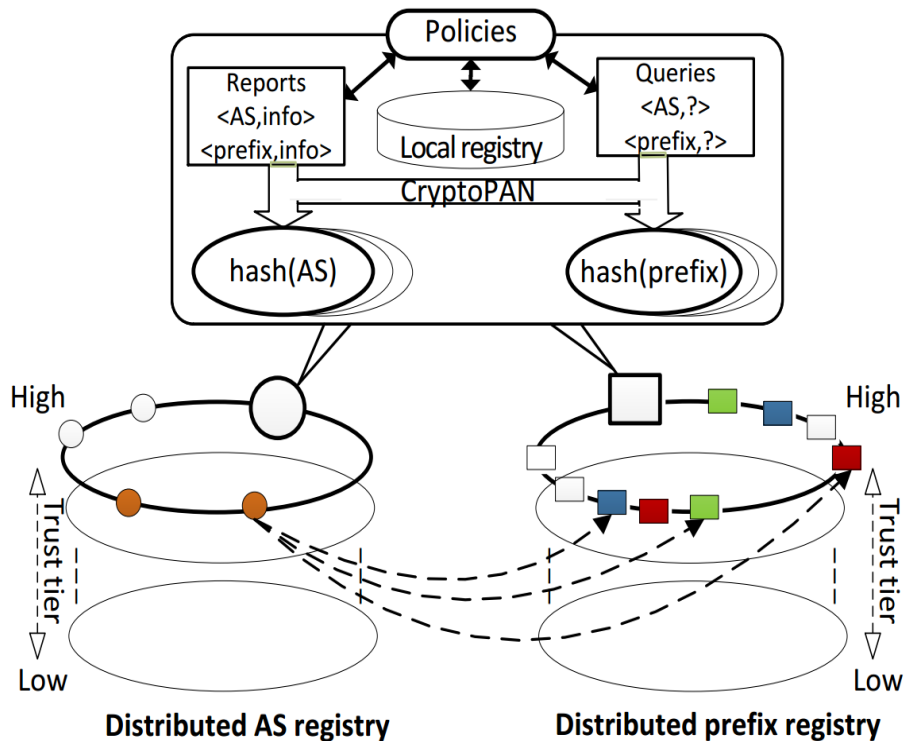
- AS registry
 - Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities
- Each member operates two nodes: one in each registry

Components and Structure



- AS registry
 - Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities
- Each member operates two nodes: one in each registry
- Policies leverage information from both registries

Components and Structure



- AS registry
 - Information about ASes, their relationships, and AS-to-prefix mappings
- Prefix registry
 - Prefix origin information (prefix-to-AS mapping), and edge-network activities
- Each member operates two nodes: one in each registry
- Policies leverage information from both registries
- **Every prefix and AS is assigned holder node in overlay network**

AS Registry: Holders and Longest Prefix

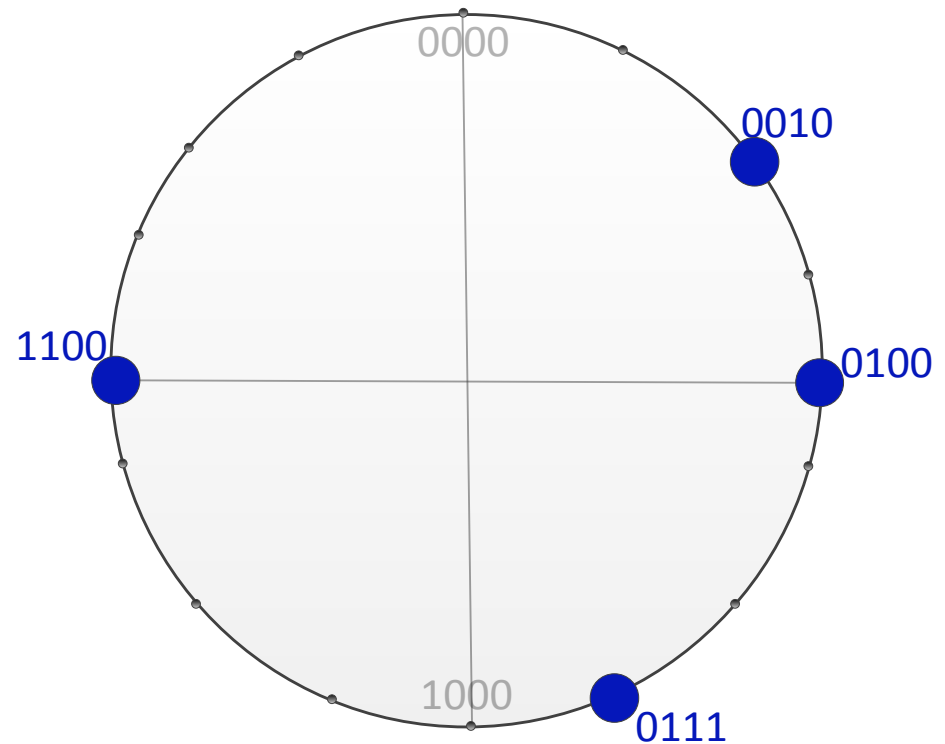
- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16

AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16

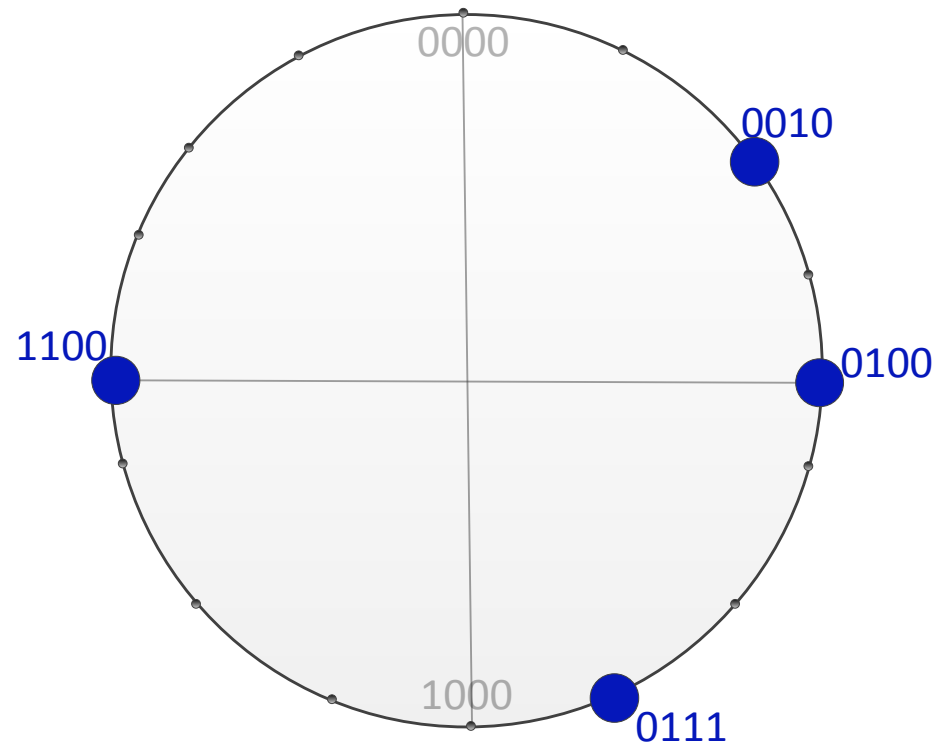
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16



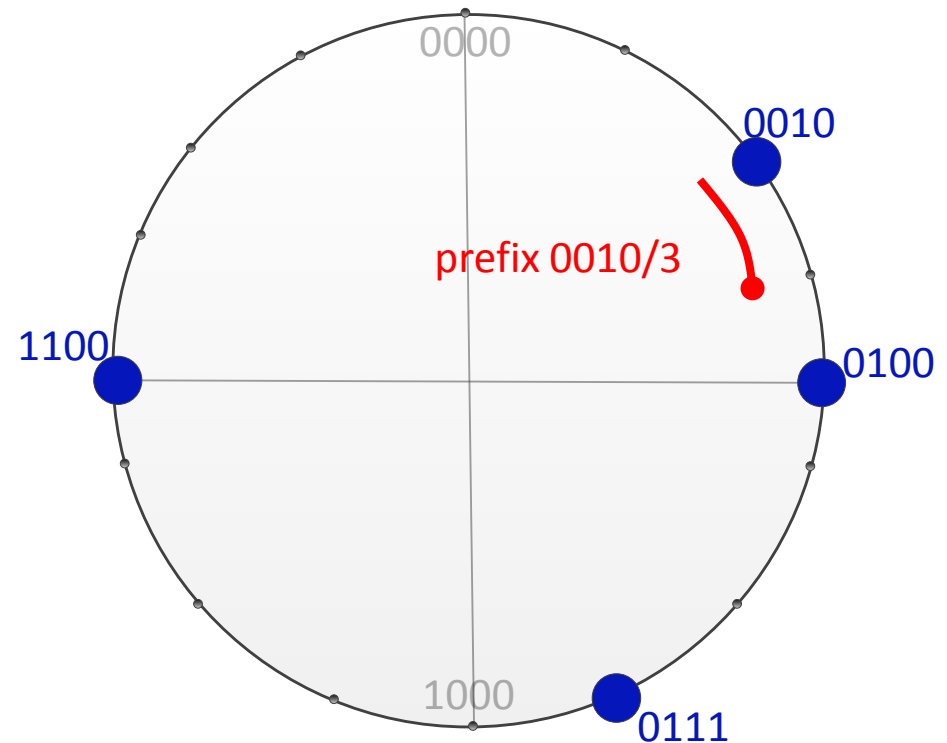
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16
- Holder assignment
 - The node responsible for the last IP address in the prefix



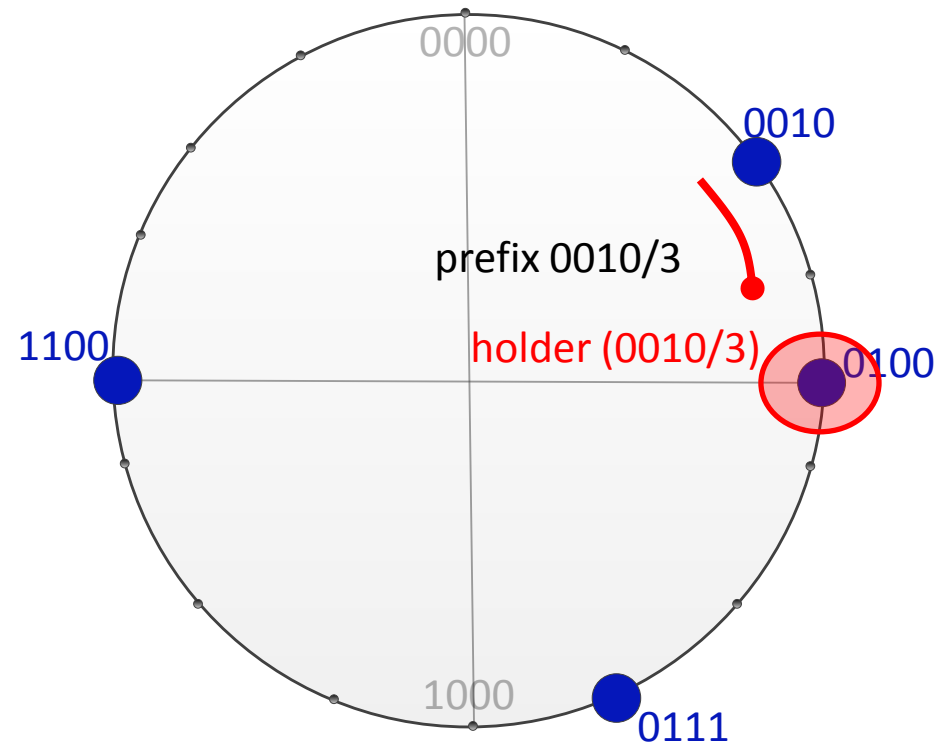
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16
- Holder assignment
 - The node responsible for the last IP address in the prefix



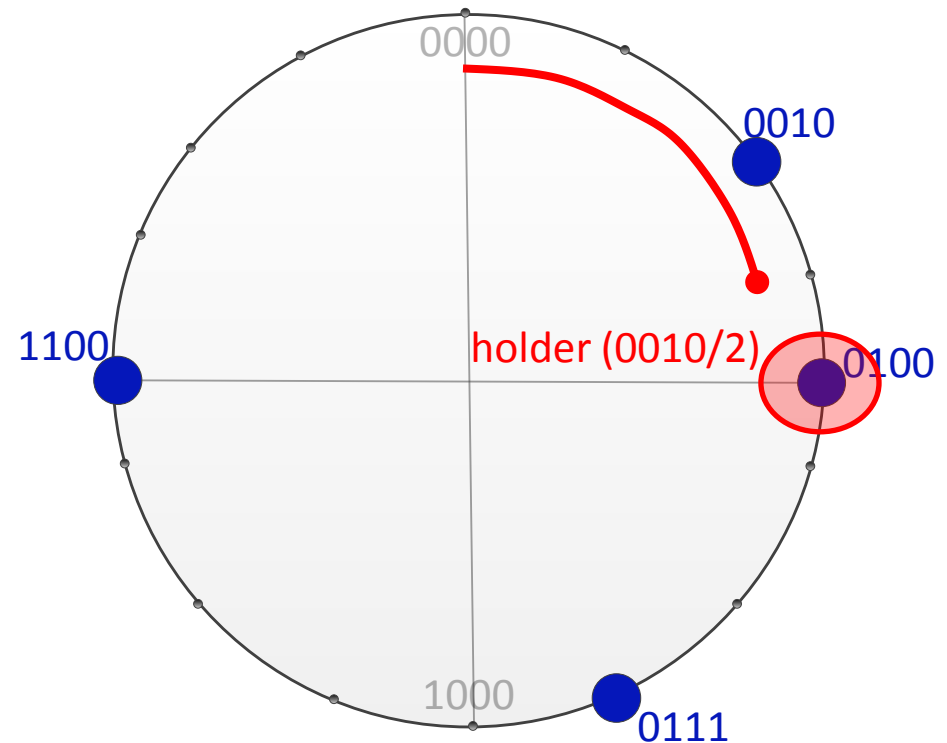
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16
- Holder assignment
 - The node responsible for the last IP address in the prefix



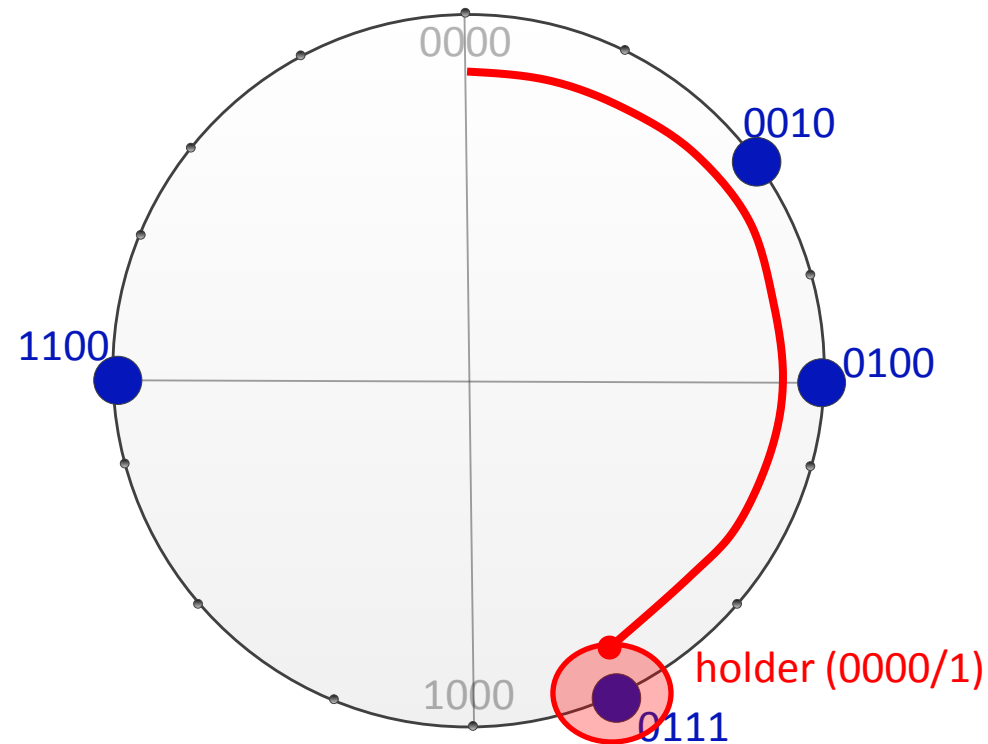
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16
- Holder assignment
 - The node responsible for the last IP address in the prefix



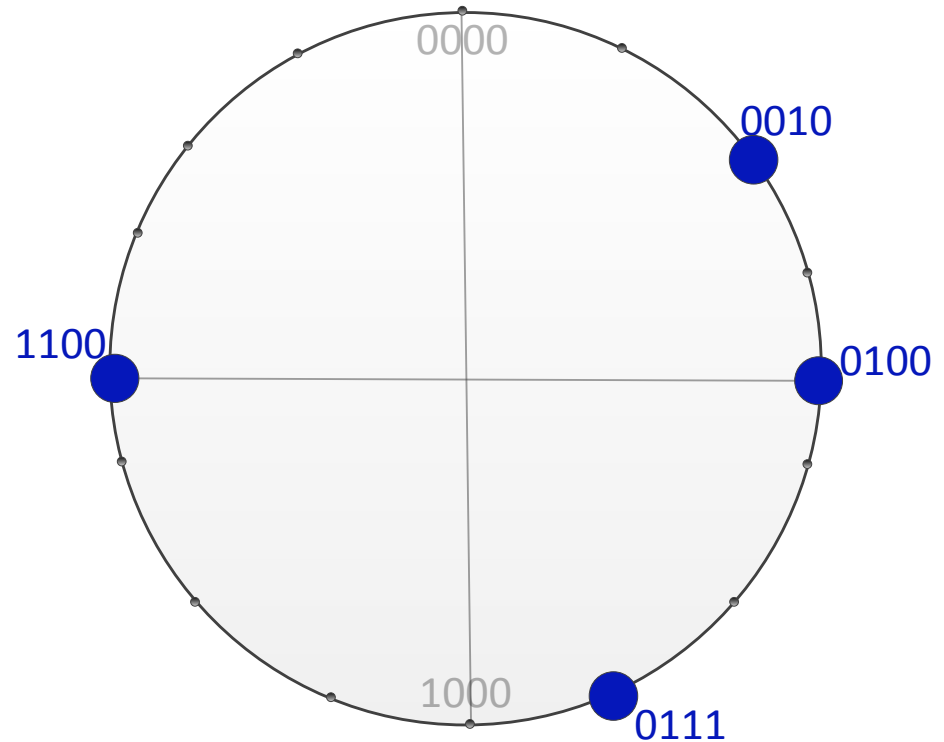
AS Registry: Holders and Longest Prefix

- Prefix registry
 - Uses distributed longest prefix matching algorithm
 - E.g., IP 12.12.12.12 maps to prefix 12.12.12.0/24; not prefix 12.12.0.0/16
- Holder assignment
 - The node responsible for the last IP address in the prefix



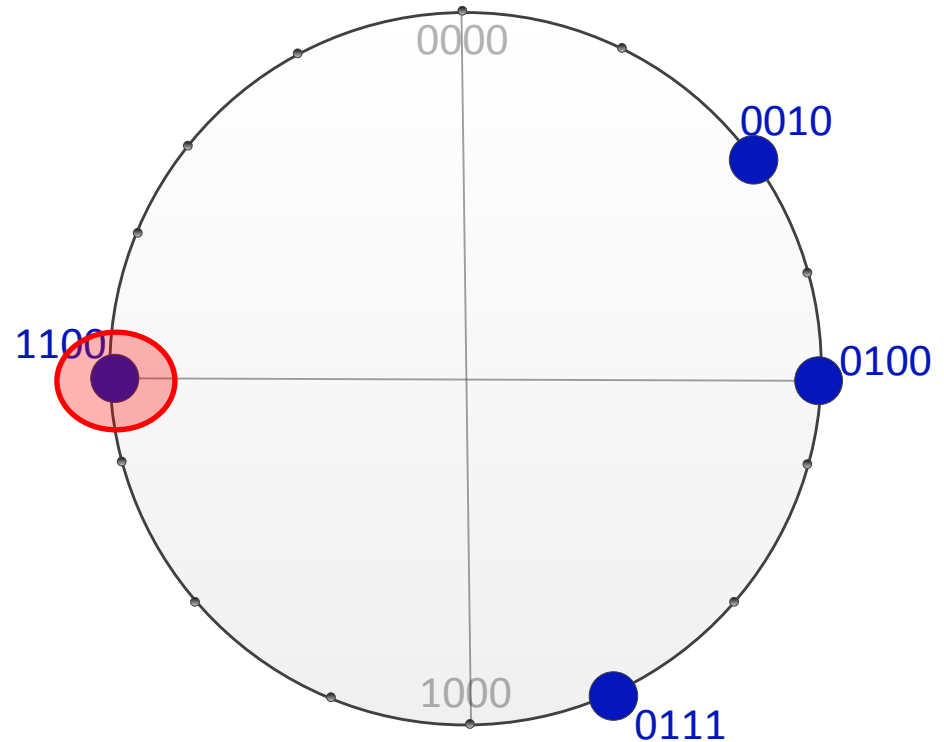
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



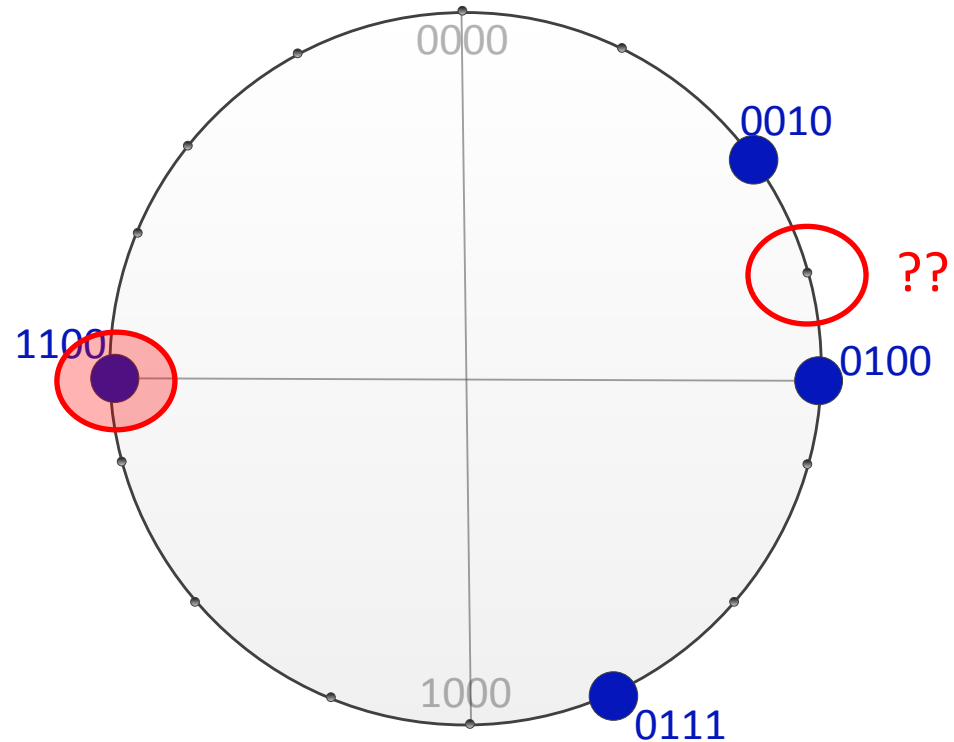
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



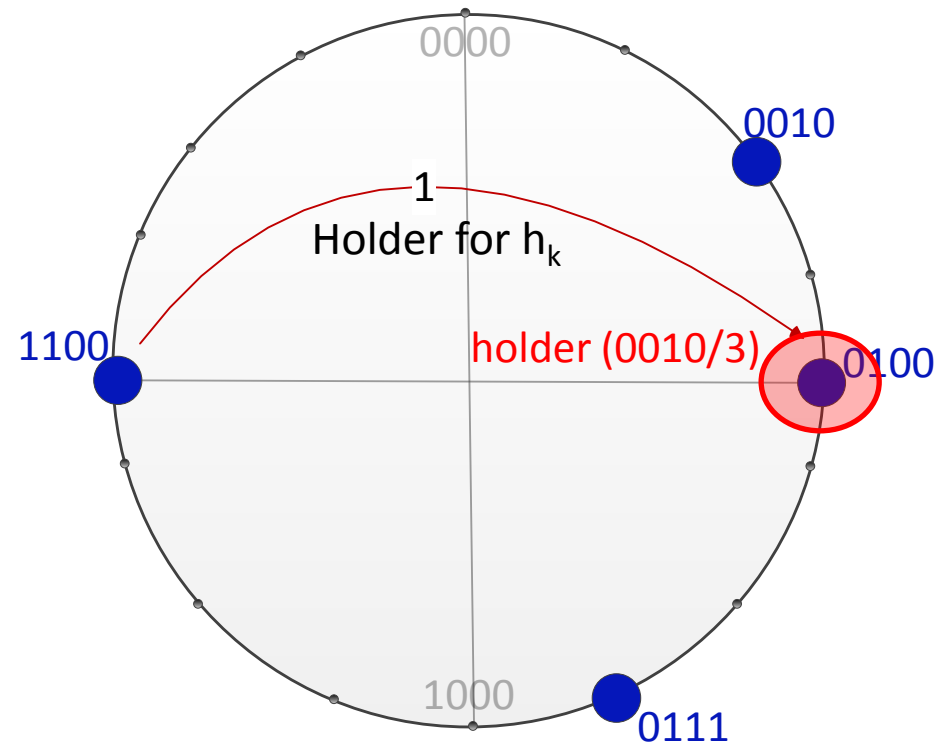
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



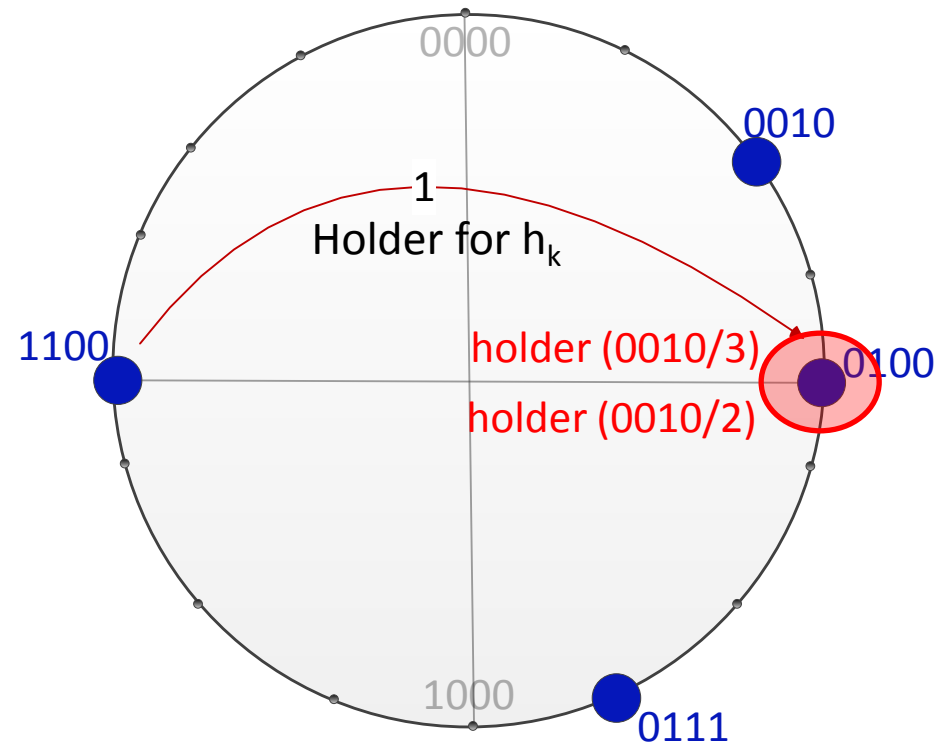
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



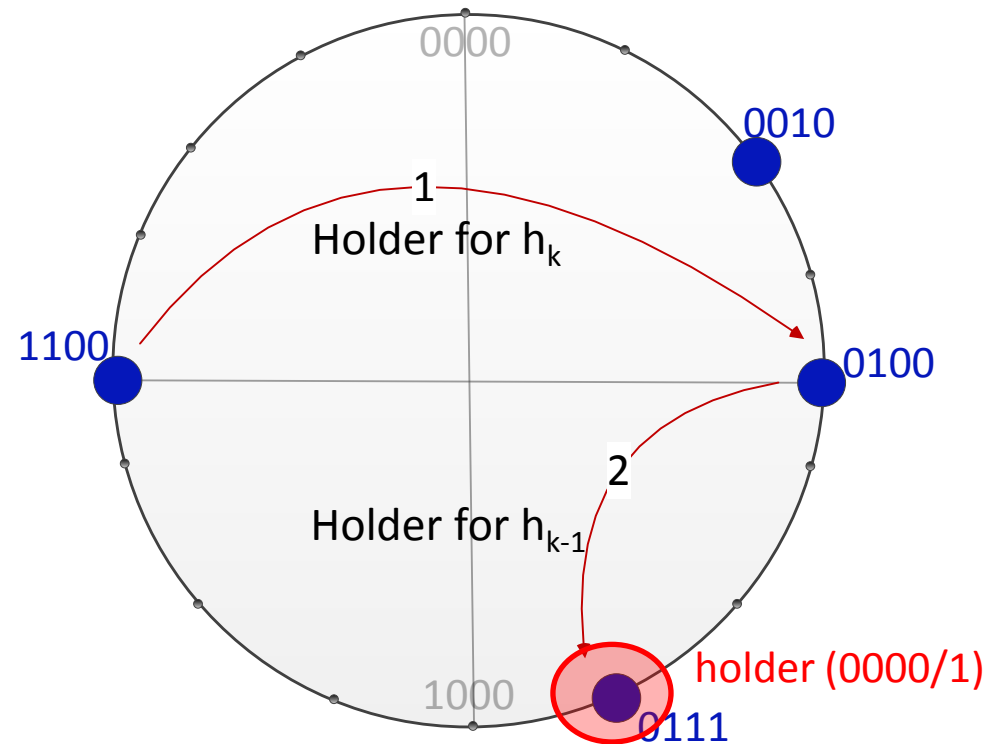
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



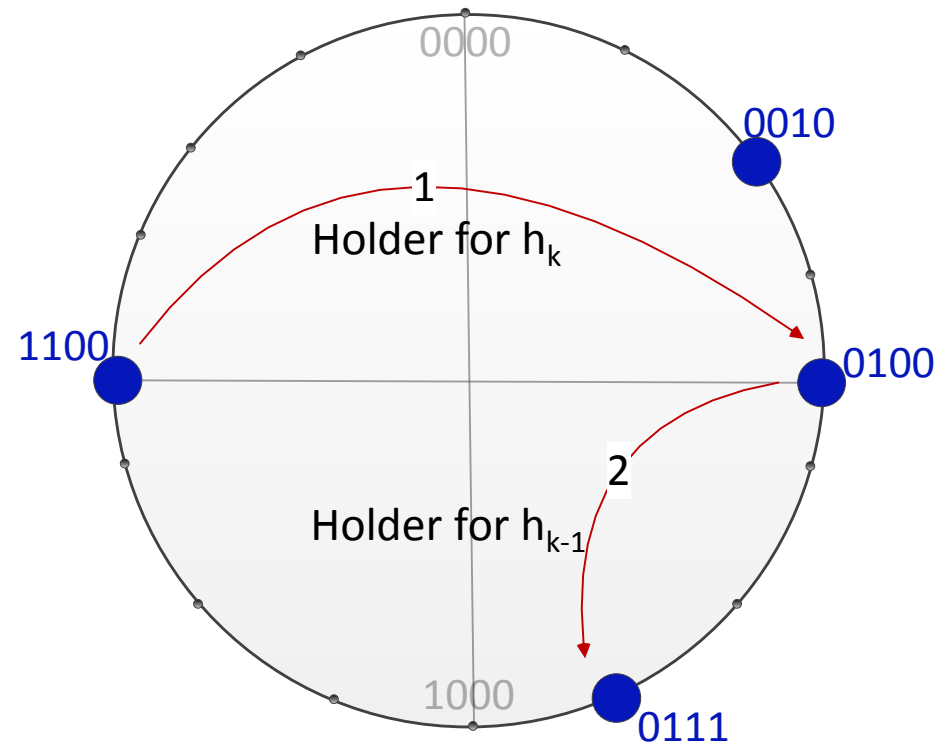
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$



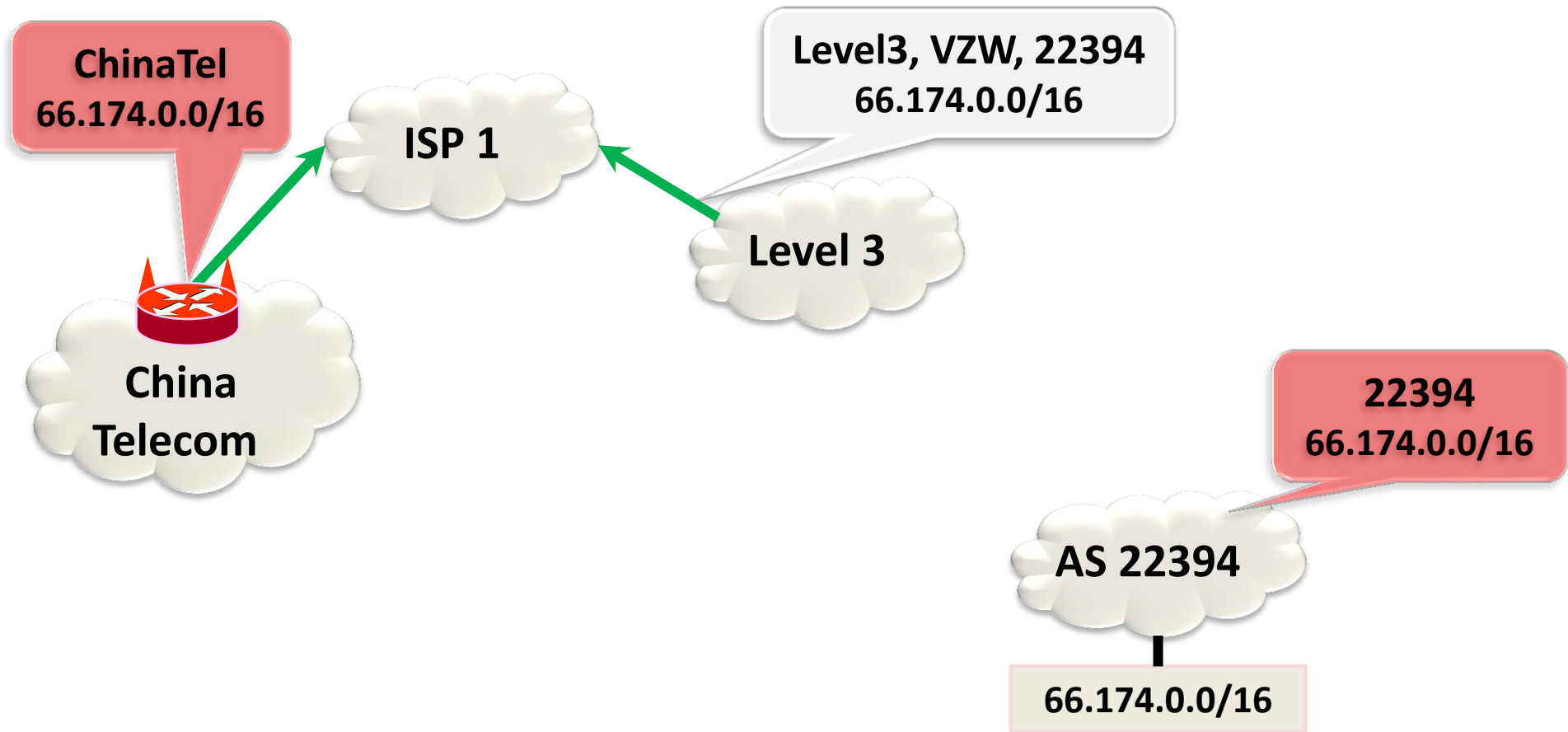
AS Registry: Holders and Longest Prefix

- Longest-prefix discovery
 - Forward the query to the candidate holder h_k of longest possible prefix of length k
 - If h_k is not aware of such prefix, it forwards the query to the next candidate holder h_{k-1} of prefix with length $(k-1)$





Prefix Hijack Detection

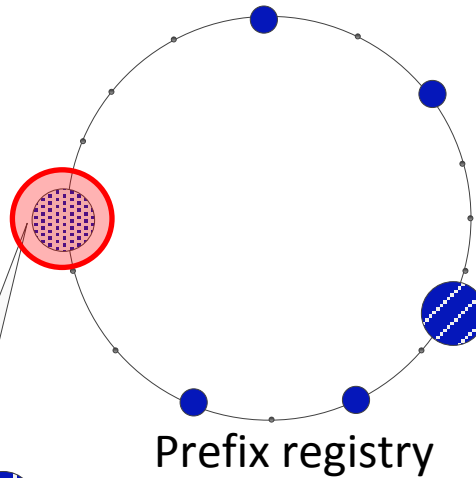
Prefix Hijack Detection



Hijack Detection Policy

1. Invoked when node detects:
- a. new prefix
 - b. new origin AS prefix
 - c. TTL for a prefix expires

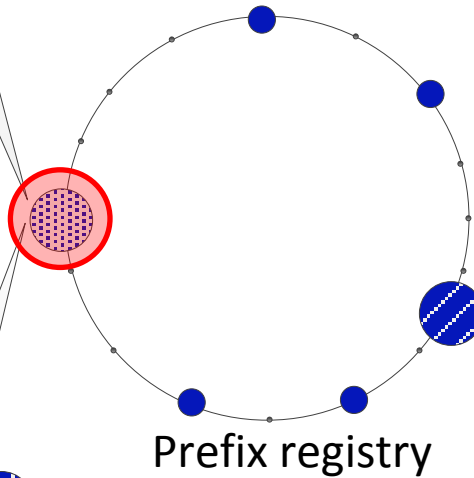
 Querying/reporting node  Holder node





Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires




 Querying/reporting node  Holder node

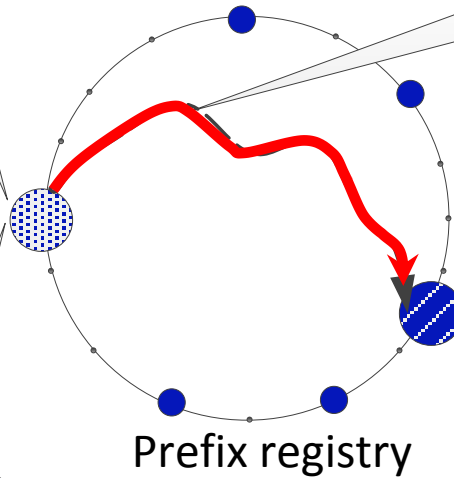
Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

3. Query/update routed over prefix overlay to holder node



 Querying/reporting node  Holder node

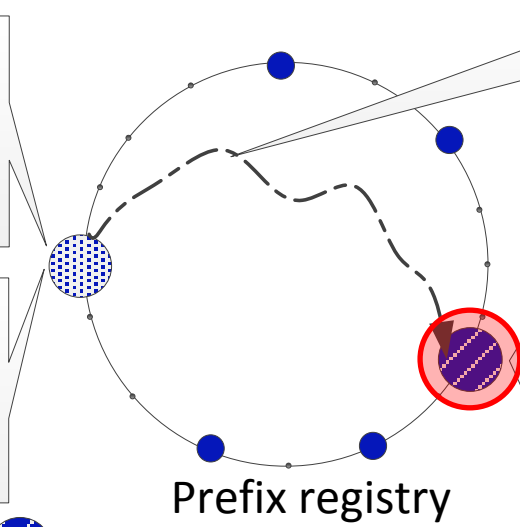


Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

 Querying/reporting node  Holder node





3. Query/update routed over prefix overlay to holder node

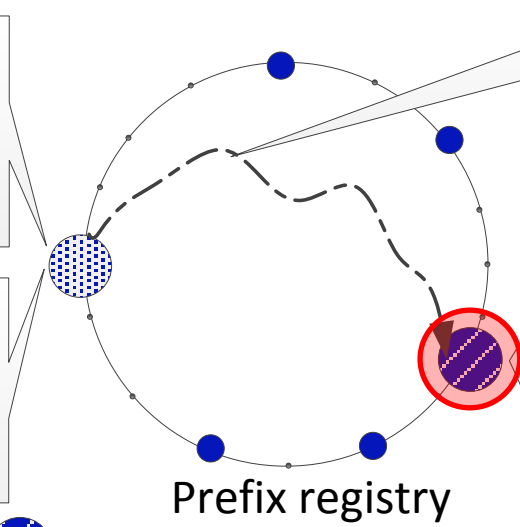
4. Process query/update
a. If no change in origin set, notify querying/reporting node
b. If change in origin set, notify current owners
c. If new prefix, invoke subprefix hijack detection procedure for prefix p/k

Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

 Querying/reporting node  Holder node



3. Query/update routed over prefix overlay to holder node

4. Process query/update

a. If no change in origin set, notify querying/reporting node



b. If change in origin set, notify current owners

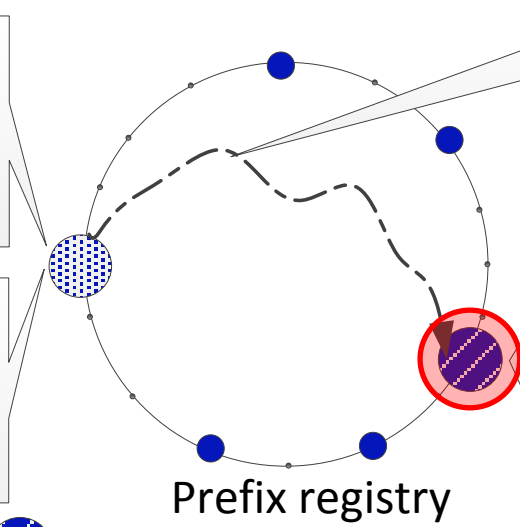
c. If new prefix, invoke subprefix hijack detection procedure for prefix p/k

Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

 Querying/reporting node  Holder node





3. Query/update routed over prefix overlay to holder node

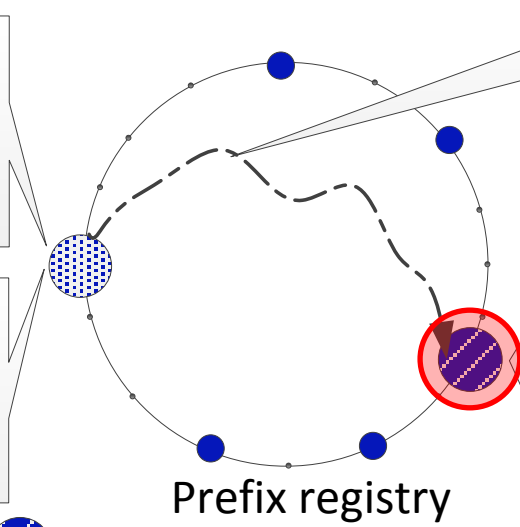
4. Process query/update
a. If no change in origin set, notify querying/reporting node
b. If change in origin set, notify current owners
c. If new prefix, invoke subprefix hijack detection procedure for prefix p/k

Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

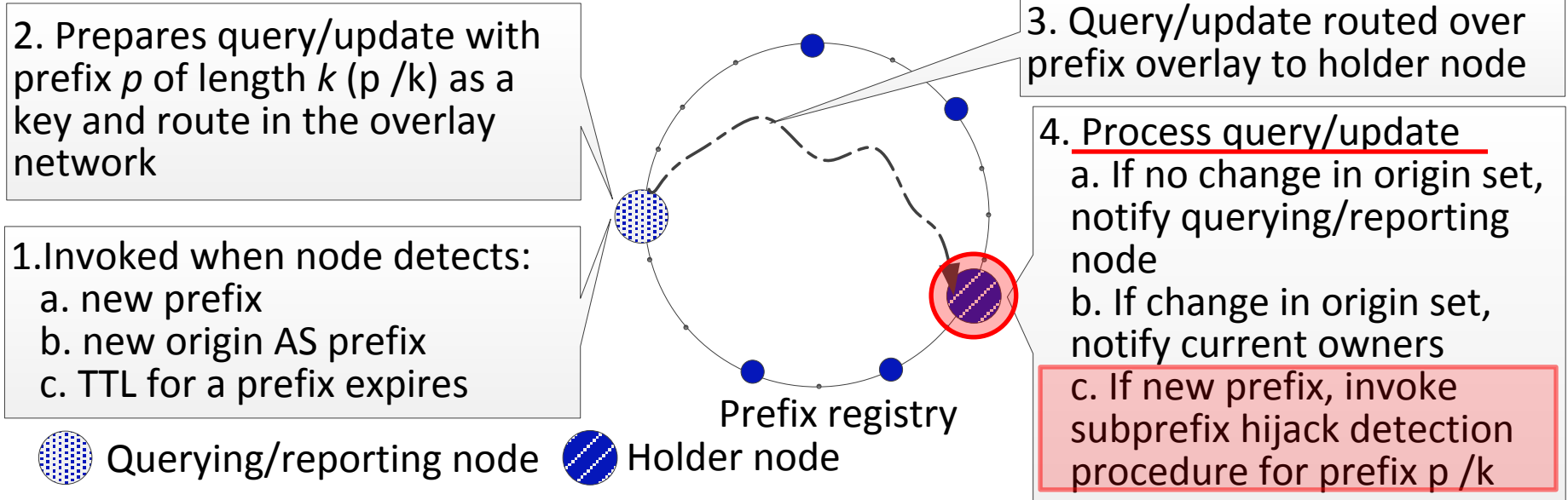
 Querying/reporting node  Holder node



3. Query/update routed over prefix overlay to holder node

4. Process query/update
a. If no change in origin set, notify querying/reporting node
b. If change in origin set, notify current owners
c. If new prefix, invoke subprefix hijack detection procedure for prefix p/k

Hijack Detection Policy





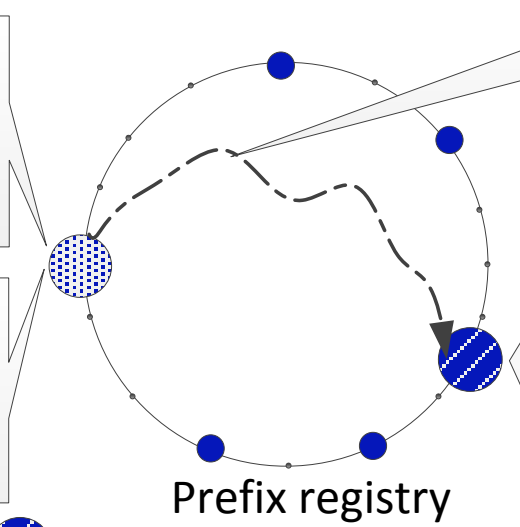
** See paper for sub-prefix detection policy

Hijack Detection Policy

2. Prepares query/update with prefix p of length k (p/k) as a key and route in the overlay network

1. Invoked when node detects:
a. new prefix
b. new origin AS prefix
c. TTL for a prefix expires

 Querying/reporting node  Holder node



3. Query/update routed over prefix overlay to holder node

4. Process query/update
a. If no change in origin set, notify querying/reporting node
b. If change in origin set, notify current owners
c. If new prefix, invoke subprefix hijack detection procedure for prefix p/k

** See paper for sub-prefix detection policy

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- **Overhead small compared to central systems such as PHAS**
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- Overhead small compared to central systems such as PHAS
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- Overhead small compared to central systems such as PHAS
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- Overhead small compared to central systems such as PHAS
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- Overhead small compared to central systems such as PHAS
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries
- Alerts scales very nicely with alliance size
 - With six alliance members, 138+1,354 queries would eventually result in prefix+subprefix hijack alerts

Case-based Overhead Analysis

Metrics	April 7, 2010 (day before incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	9,179,307	16,000,217	18,912,643	23,206,562
Announced prefixes	323,899	327,400	328,630	328,826
Prefix not seen	1,949	1,367	1,349	1,354
Prefix not seen (unique AS)	290	241	242	247
Origin not seen	209	130	134	138
Origin not seen in last 72h	1,302	3,594	3,874	2,735
Origin not seen in last 24h	3,200	5,840	6,184	4,746

Normal conditions

- Overhead small compared to central systems such as PHAS
 - PHAS would 23M updates forwarded to and processed at single node
 - PrefiSec: single node would make 209+1,949 prefix+subprefix queries
- Alerts scales very nicely with alliance size
 - With six alliance members, 138+1,354 queries would eventually result in prefix+subprefix hijack alerts

Case-based Overhead Analysis

- Day of incident

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident

- Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
- Plus similar (normal) day-to-day overhead

E.g., Non-ChinaTel alerts:

$$(10,330 + 30,245) - 39,094 = 1,481$$

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead

E.g., Non-ChinaTel alerts

$$(10,330 + 30,245) - 39,094 = 1,481$$

Total

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident

- Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
- Plus similar (normal) day-to-day overhead

E.g., Non-ChinaTel alerts

$$(10,330 + 30,245) - 39,094 = 1,481$$

ChinaTel

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead

E.g., Non-ChinaTel alerts

$$(10,330 + 30,245) - 39,094 = \underline{\underline{1,481}}$$

Case-based Overhead Analysis

Metrics	April 8, 2010 (day of incident)			
	1 node	2 nodes	4 nodes	6 nodes
Route announcements	10,177,068	19,371,838	23,388,253	31,265,557
Announced prefixes	331,348	332,922	333,825	336,526
Prefix not seen	10,554	10,346	10,332	10,330
Prefix not seen (unique AS)	273	250	261	263
Owner not seen	21,275	21,001	29,704	30,245
Owner not seen in last 72h	21,570	21,970	31,108	31,680
Owner not seen in last 24h	22,561	23,027	32,382	33,937

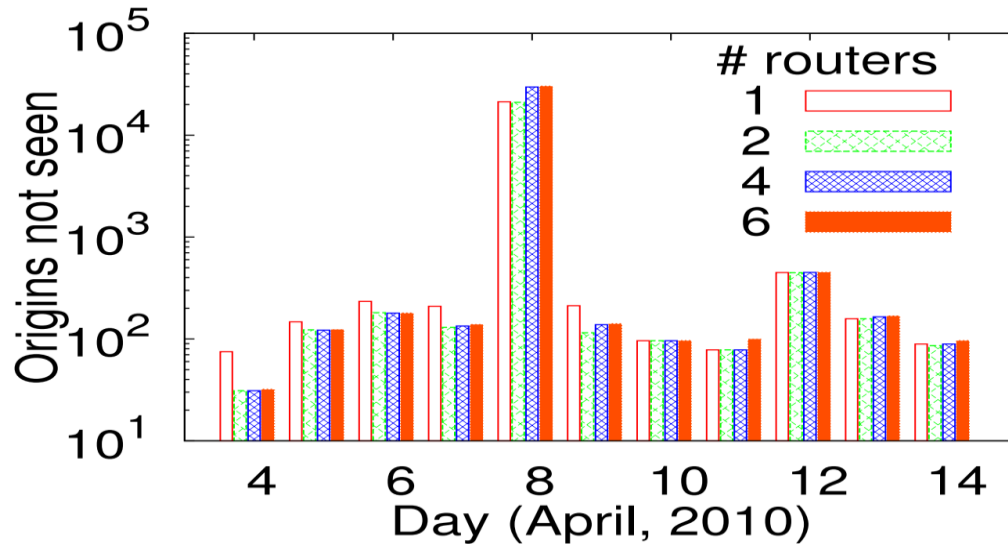
- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead

E.g., Non-ChinaTel alerts

$$(10,330+30,245) - 39,094 = \underline{\underline{1,481}}$$

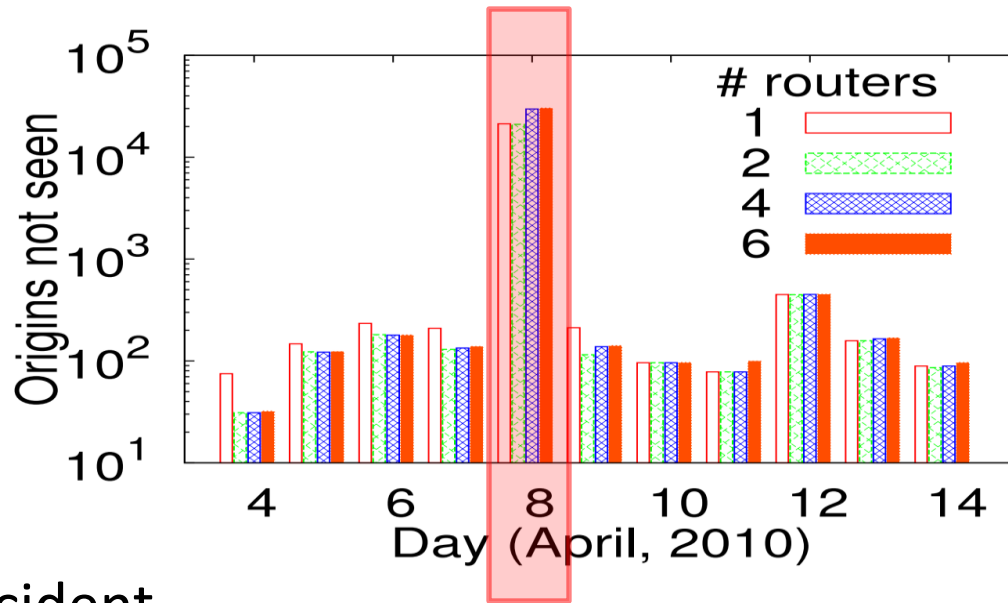
vs. 1,492 the day before the attack

Case-based Overhead Analysis



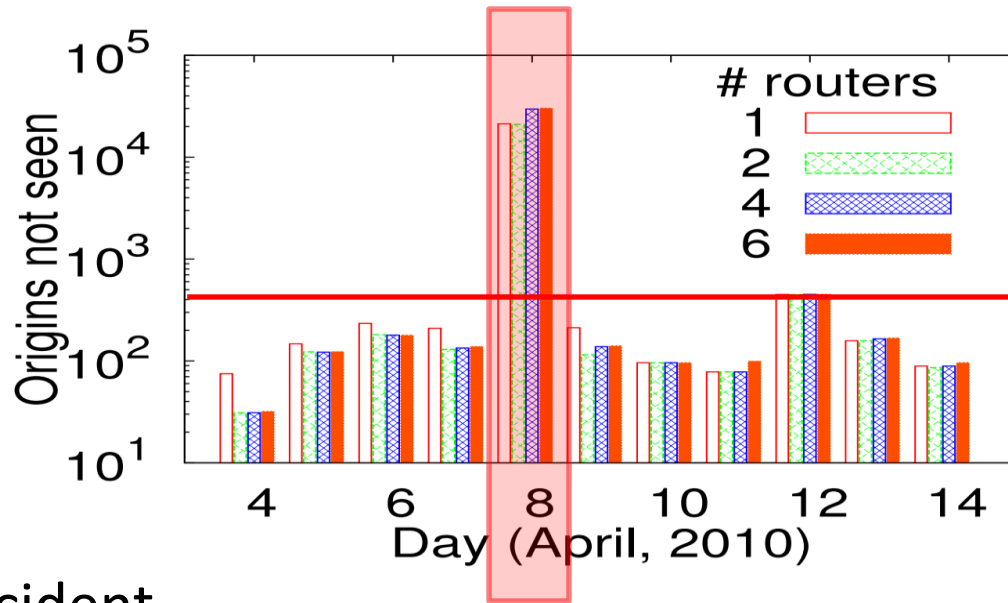
- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead
 - Overhead quickly decrease again after the attack

Case-based Overhead Analysis



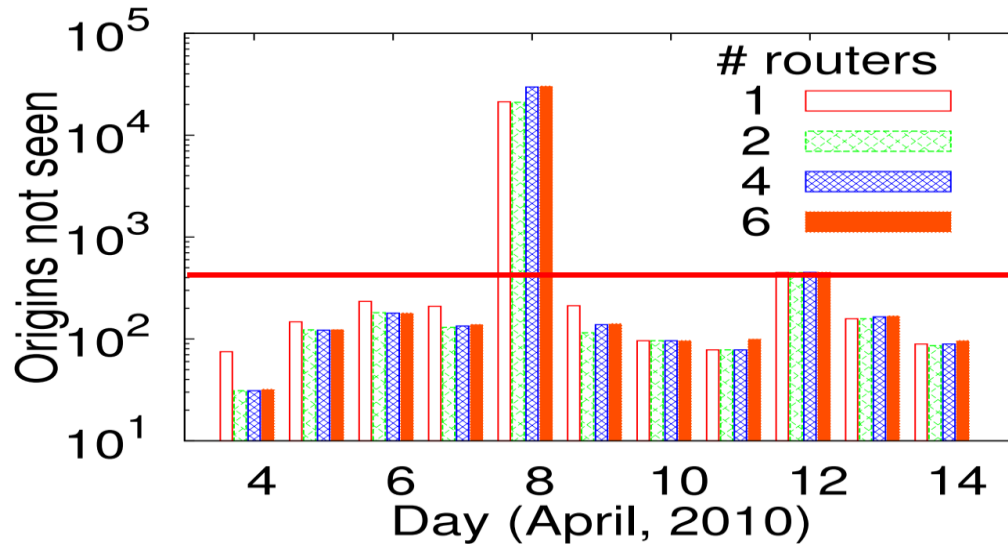
- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead
 - Overhead quickly decrease again after the attack

Case-based Overhead Analysis



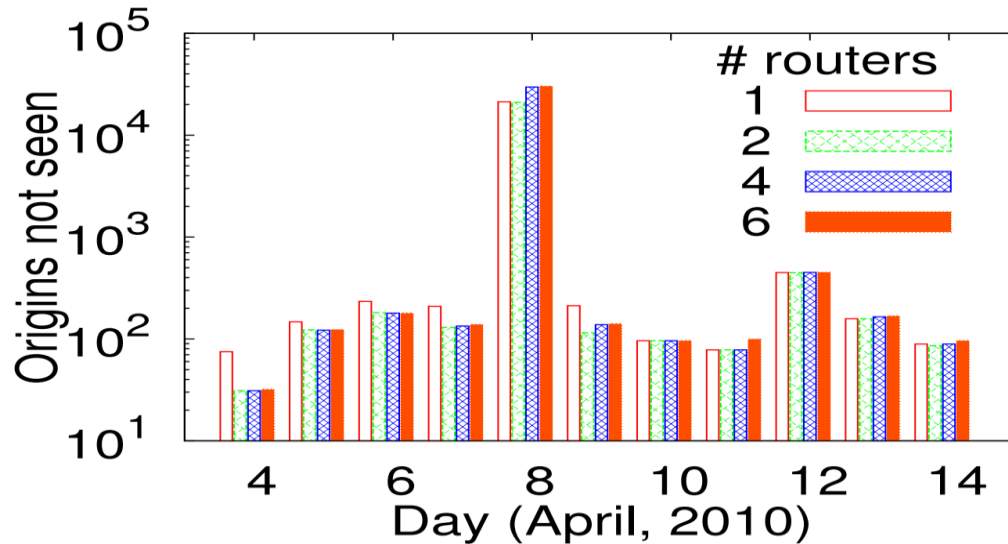
- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead
 - Overhead quickly decrease again after the attack

Case-based Overhead Analysis



- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead
 - Overhead quickly decrease again after the attack

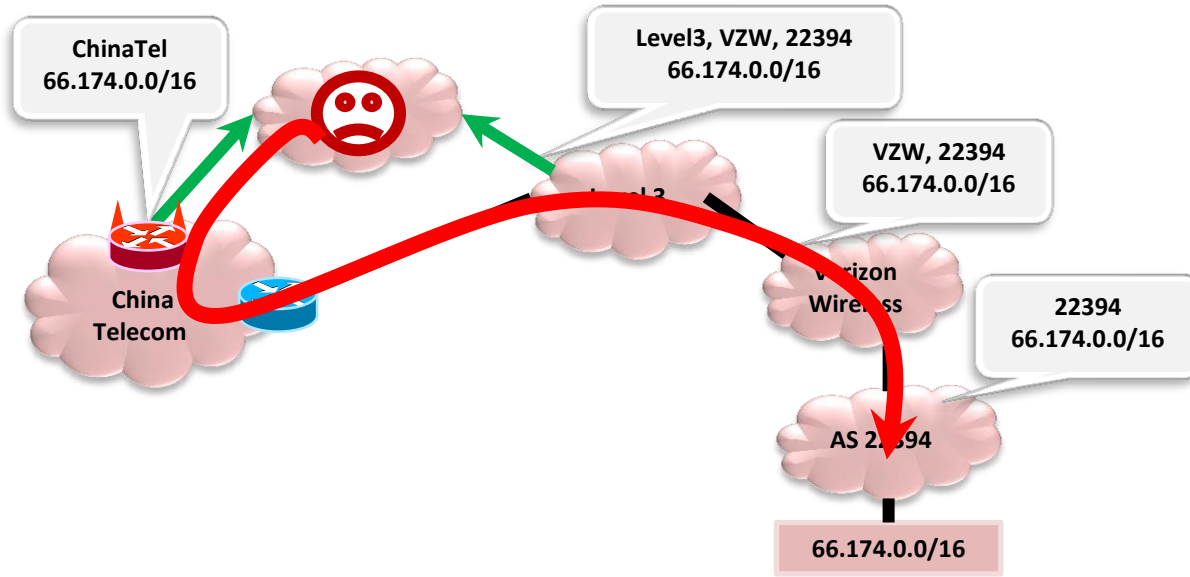
Case-based Overhead Analysis



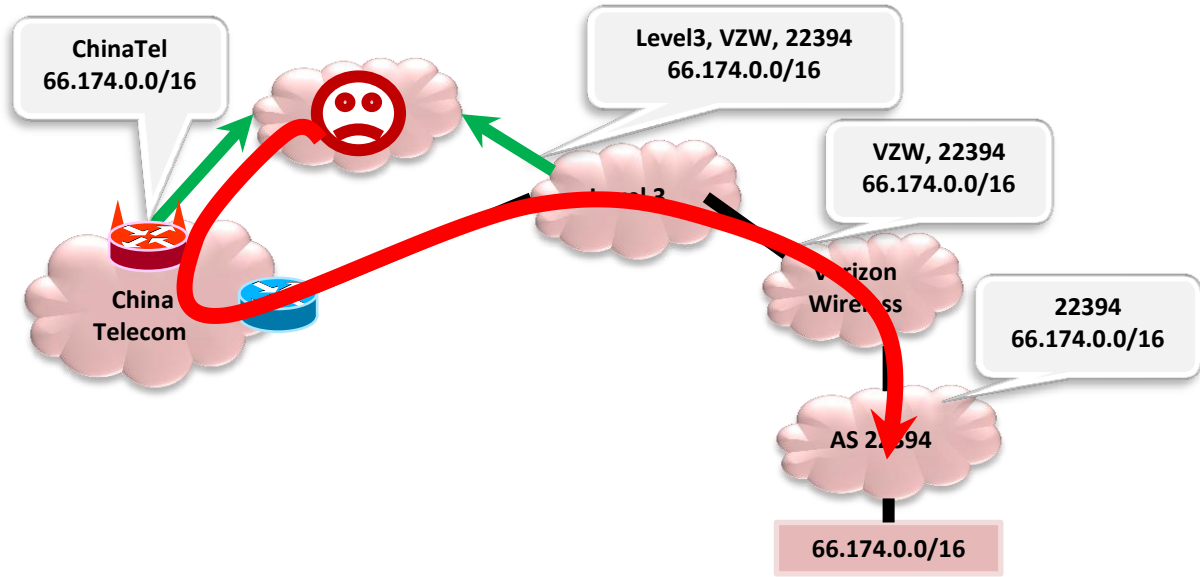
- Day of incident
 - Would raise alarms for all 39,094 unique prefixes that had the specific signature associated with incorrect prefix announcements
 - Plus similar (normal) day-to-day overhead
 - Overhead quickly decrease again after the attack
 - Effectively handle increased load
 - Holders aggregate information and can sanity check claims
 - Only holders communicate with owners of hijacked prefixes
 - Further overhead reductions by aggregating over ASes

Interception Detection Policy

Interception Detection Policy



Interception Detection Policy

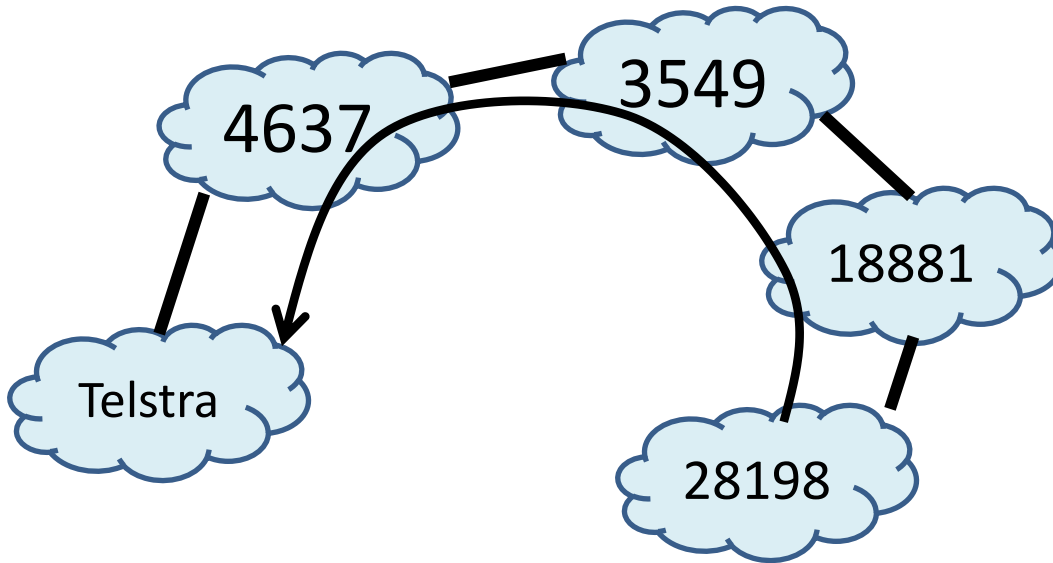


Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

Interception Detection Policy

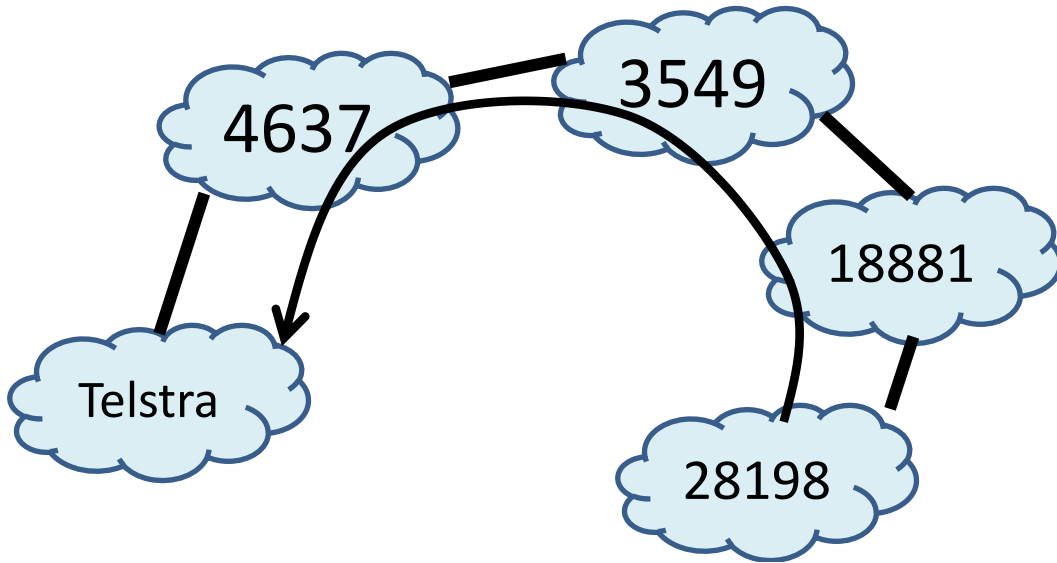


Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

Interception Detection Policy



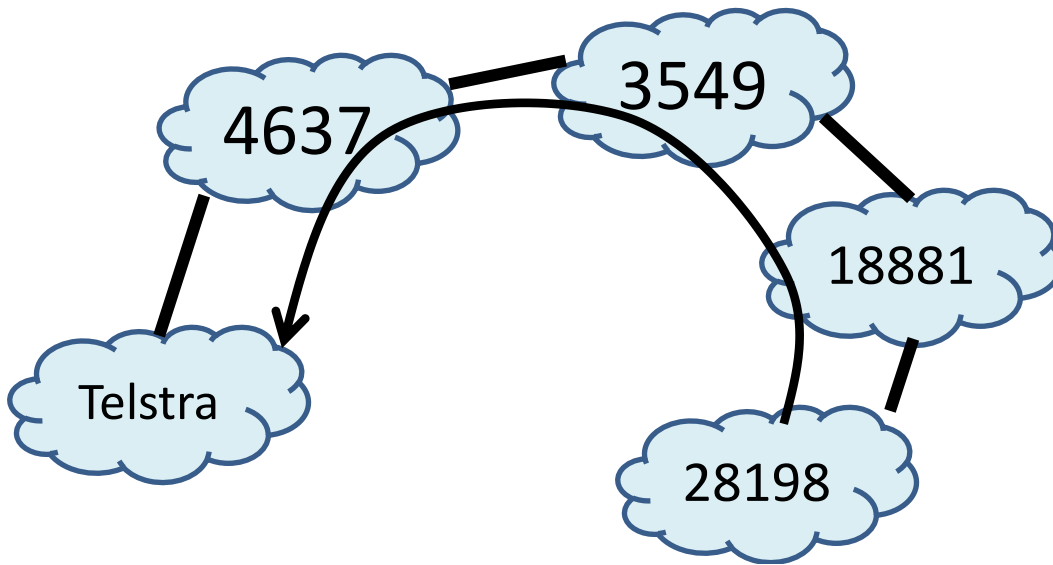
Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

Interception Detection Policy



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

Traceroute:

... (initial hops)

9. telstraglobal.net (134.159.63.202) 164.905 ms

10. impsat.net.br (189.125.6.194) 337.434 ms

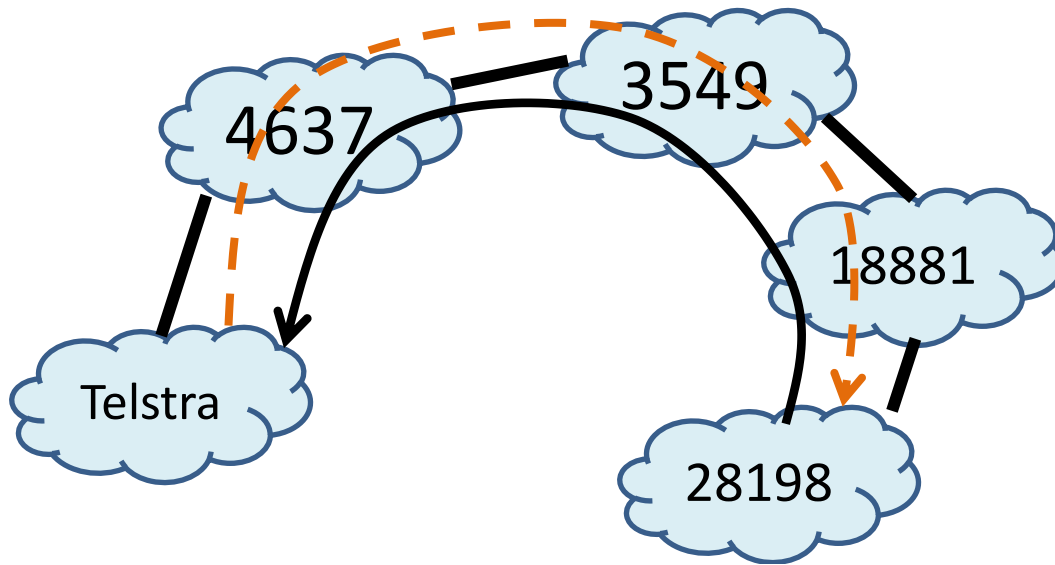
11. spo.gvt.net.br (187.115.214.217) 332.926 ms

12. spo.gvt.net.br (189.59.248.109) 373.021 ms

13. host.gvt.net.br (189.59.249.245) 343.685 ms

14. isimples.com.br (177.52.48.1) 341.172 ms

Interception Detection Policy



Interception typically results in differences between

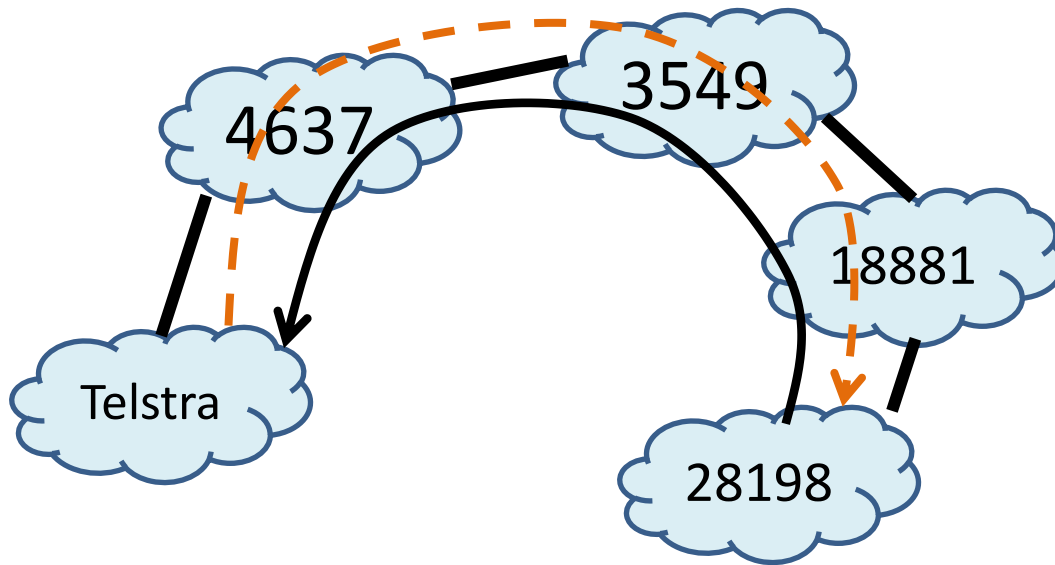
- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637
4637 4637 3549 3549 3549 18881 18881 18881 18881 28198

Interception Detection Policy



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

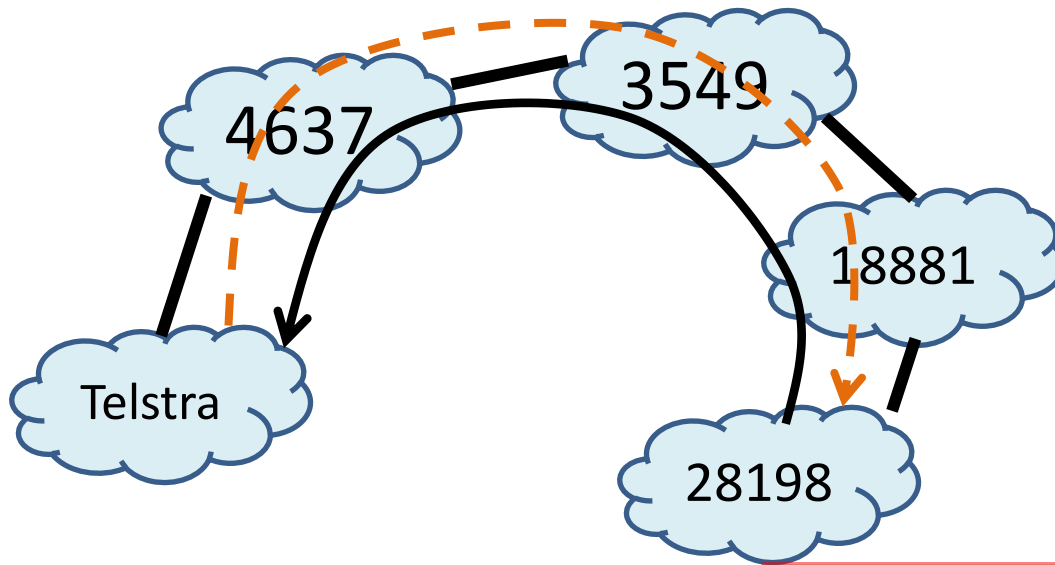
Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637
4637 4637 3549 3549 3549 18881 18881 18881 18881 28198

Traceroute-PATH: 1221 4637 3549 18881 28198

Interception Detection Policy



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

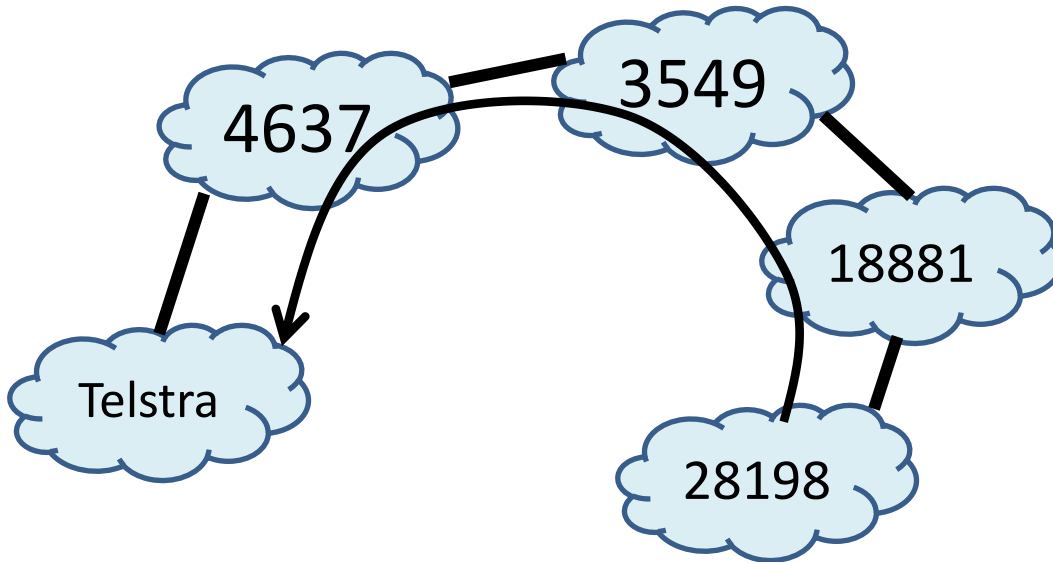
Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21 **1221 4637 3549 18881 28198**

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637
4637 4637 3549 3549 3549 18881 18881 18881 18881 28198

Traceroute-PATH: **1221 4637 3549 18881 28198**

Legit Path Discrepancies



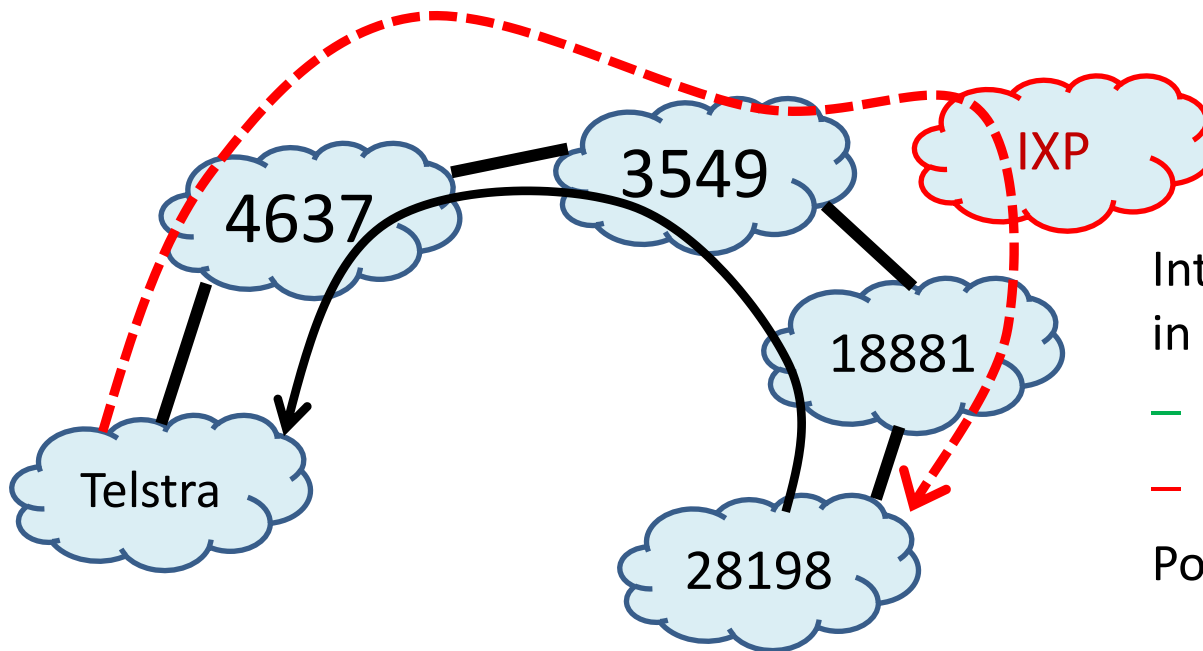
Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21|1221 4637 3549 18881 28198

Legit Path Discrepancies



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

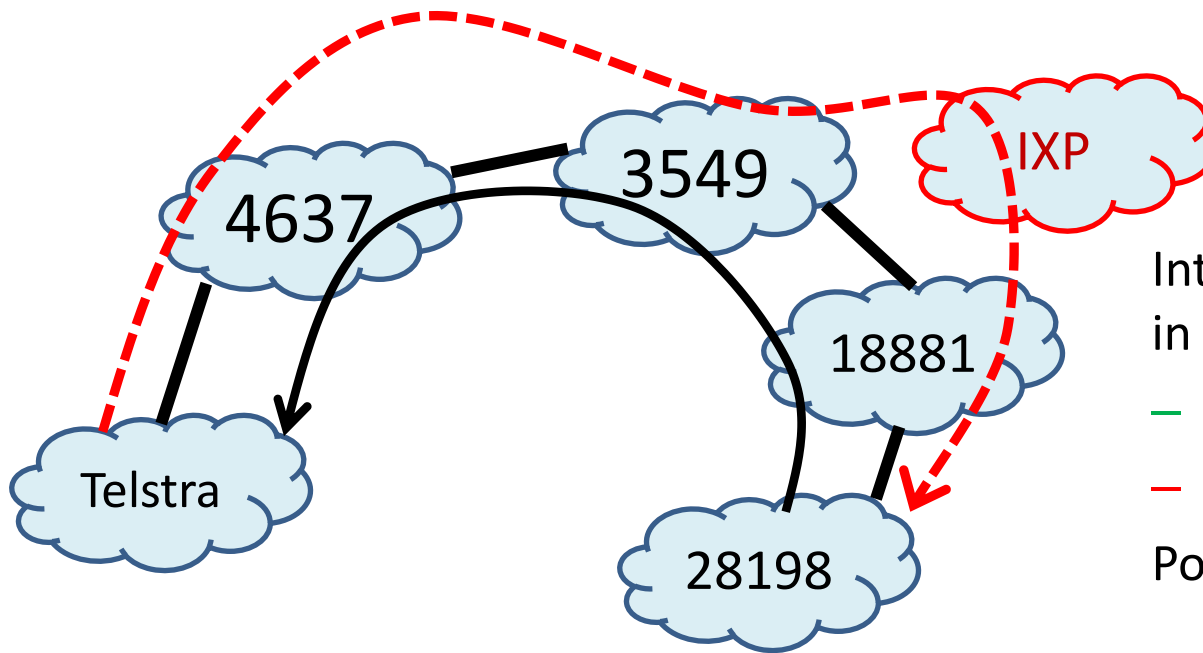
Policy checks if legit reason(s)

AS-PATH: 177.52.48.0/21|1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637

4637 4637 3549 3549 3549 IXP 18881 18881 18881 18881 28198

Legit Path Discrepancies



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

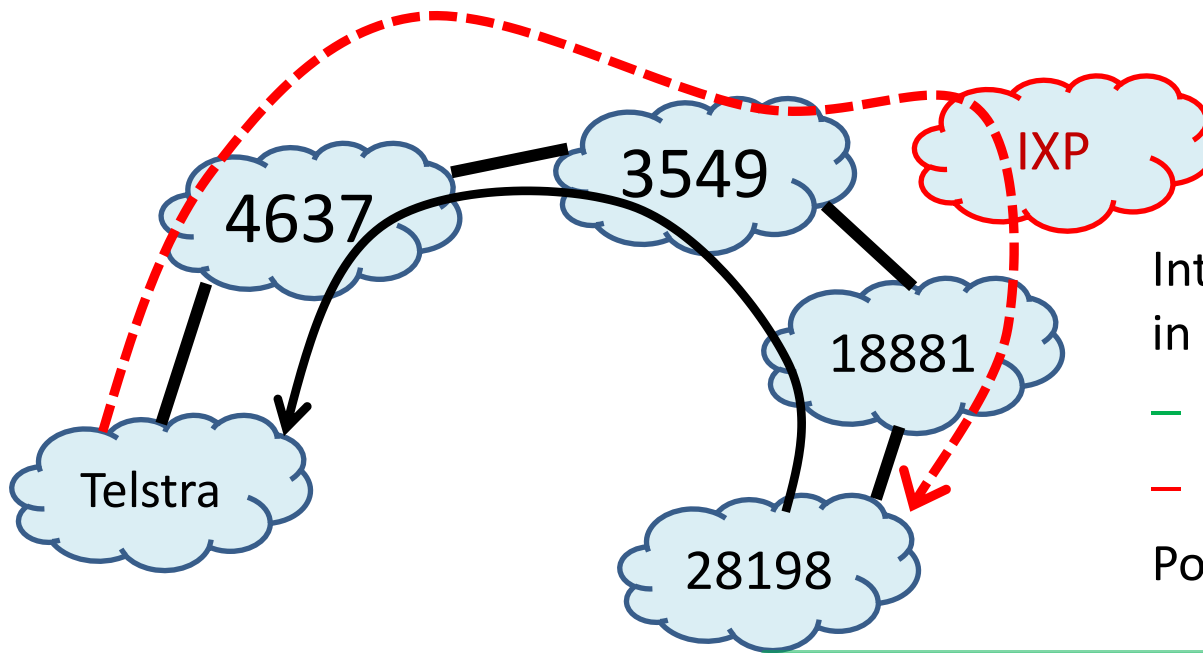
AS-PATH: 177.52.48.0/21|1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637

4637 4637 3549 3549 3549 IXP 18881 18881 18881 18881 28198

Traceroute-PATH: 1221 4637 3549 IXP 18881 28198

Legit Path Discrepancies



Interception typically results in differences between

- Announced AS-PATH
- Data path (traffic)

Policy checks if legit reason(s)

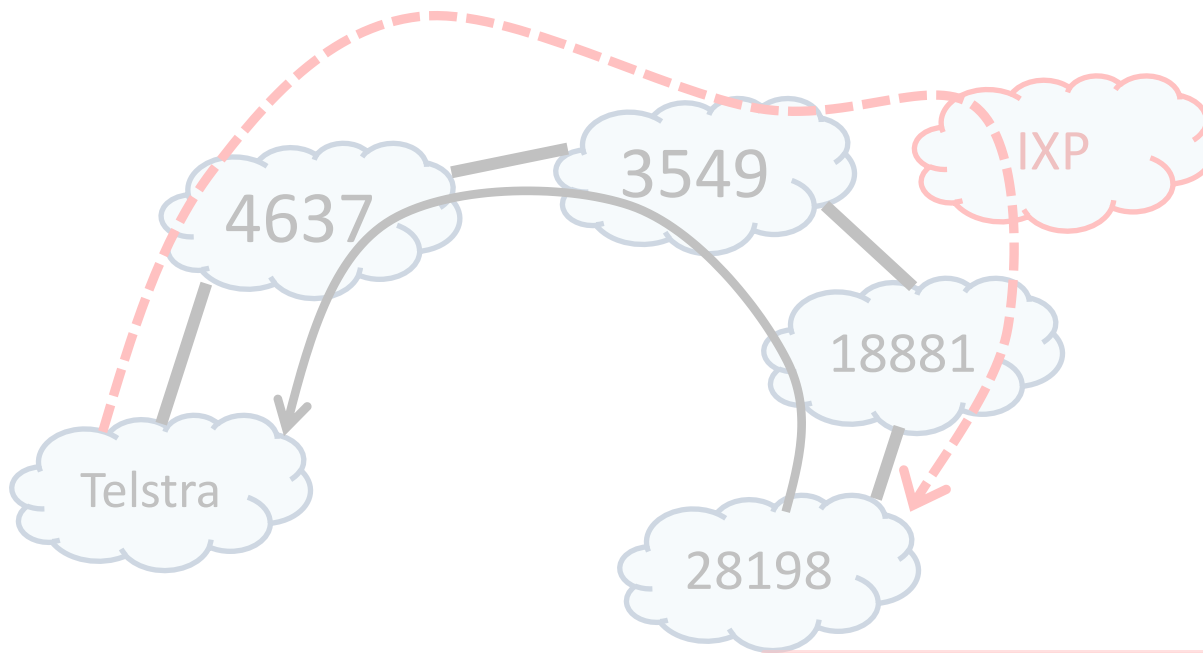
AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637

4637 4637 3549 3549 3549 IXP 18881 18881 18881 18881 28198

Traceroute-PATH: 1221 4637 3549 IXP 18881 28198

Legit Path Discrepancies



- Other legit reasons
 - Multiple origin ASes
 - Loops
 - Missing AS hops
 - Alias IP addresses
 - Sibling relationships

AS-PATH: 177.52.48.0/21 | 1221 4637 3549 18881 28198

AS HOPS in traceroute: 1221 1221 1221 1221 4637 4637 4637

4637 4637 3549 3549 3549 IXP 18881 18881 18881 18881 28198

Traceroute-PATH: 1221 4637 3549 IXP 18881 28198

Case-based Analysis

- Other legit reasons
 - Multiple origin ASes
 - Loops
 - Missing AS hops
 - Alias IP addresses
 - Sibling relationships
- We use PrefiSec to identify suspicious and non-suspicious path inconsistencies
- Evaluation using three public Routeviews servers and nearby public traceroute servers hosted by
 - Global Crossing (Palo Alto, CA)
 - Telstra (Sydney, Australia)
 - Hurricane Electric (San Jose, CA)

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^6$	$3.5 \cdot 10^6$	$3.6 \cdot 10^6$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Seen announcements

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

When new AS-PATH,
perform traceroute

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

When new AS-PATH,
perform traceroute

Successful traceroutes

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Successful traceroutes

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Apply one rule at a time

Successful traceroutes

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Apply one rule at a time

Direct/subset matches

Path Comparison Analysis

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Apply one rule at a time

Legit reasons PrefiSec identifies (@holders)

- Legit reasons allow significant reduction of candidates

Path Comparison Analysis

Apply one rule at a time

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Seen other times

- Legit reasons allow significant reduction of candidates
- History further reductions

Path Comparison Analysis

Apply one rule at a time

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Example reduction
96.7%

- Legit reasons allow significant reduction of candidates
- History further reductions

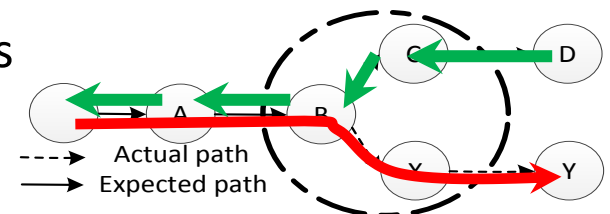
Path Comparison Analysis

Apply one rule at a time

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Unresolved AS triples

- Legit reasons allow significant reduction of candidates
- History further reductions
- **Involved AS triples even less**



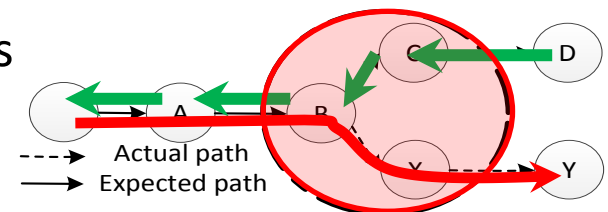
Path Comparison Analysis

Apply one rule at a time

	Telstra	Global	Hurricane
Announcements	$3.6 \cdot 10^7$	$3.5 \cdot 10^7$	$3.6 \cdot 10^7$
Traceroutes (new route)	102,689	63,434	60,628
No data (new route)	506	60,045	3,200
Successful traceroutes	102,183	3,389	60,627
Direct matches	12,387	704	16,374
Subset matches	62,952	947	13,267
IXP matches	2,672	11	30,071
MOAS matches	309	NA	445
Loop matches	2,271	108	1,021
Missing hop matches	2,730	689	6,886
Alias matches	11,650	276	7,020
Sibling matches	1,764	27	243
Past matches	4,209	363	1,916
Future matches	487	23	515
Unresolved traceroutes	3,333	244	9,464
Unresolved triples	539	82	1,422

Unresolved AS triples

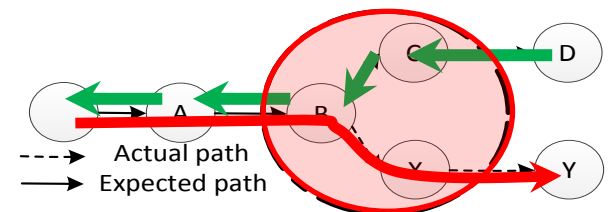
- Legit reasons allow significant reduction of candidates
- History further reductions
- **Involved AS triples even less**



Redundancy in Unique Triples

				Redundancy in triples		
	Server	Traceroute	Triples	History	Sharing	Hybrid
Week 1	Telstra	66,985	372	—	12%	—
	Global	55,144	292	—	15%	—
	Hurricane	—	—	—	—	—
Week 2	Telstra	102,689	539	32%	14%	41%
	Global	63,434	82	27%	26%	38%
	Hurricane	60,628	1,422	4%	6%	7%
Week 3	Telstra	77,012	492	45%	16%	54%
	Global	—	—	—	—	—
	Hurricane	56,518	1,244	35%	6%	39%

Unique triples



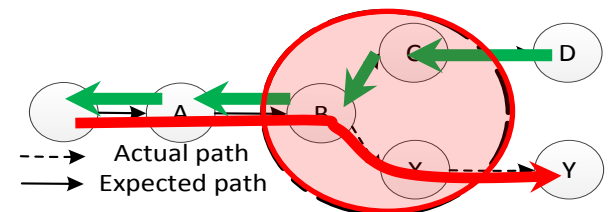
Redundancy in Unique Triples

				Redundancy in triples		
	Server	Traceroute	Triples	History	Sharing	Hybrid
Week 1	Telstra	66,985	372	—	12%	—
	Global	55,144	292	—	15%	—
	Hurricane	—	—	—	—	—
Week 2	Telstra	102,689	539	32%	14%	41%
	Global	63,434	82	27%	26%	38%
	Hurricane	60,628	1,422	4%	6%	7%
Week 3	Telstra	77,012	492	45%	16%	54%
	Global	—	—	—	—	—
	Hurricane	56,518	1,244	35%	6%	39%

Unique triples

Significant advantage to

- maintaining history at the holder nodes, and
- sharing information across organizations



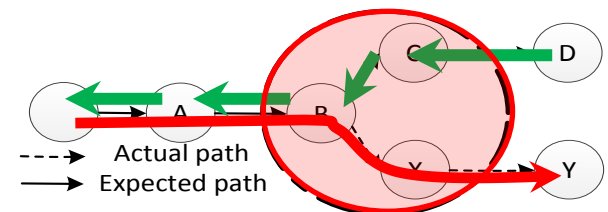
Redundancy in Unique Triples

				Redundancy in triples		
	Server	Traceroute	Triples	History	Sharing	Hybrid
Week 1	Telstra	66,985	372	—	12%	—
	Global	55,144	292	—	15%	—
	Hurricane	—	—	—	—	—
Week 2	Telstra	102,689	539	32%	14%	41%
	Global	63,434	82	27%	26%	38%
	Hurricane	60,628	1,422	4%	6%	7%
Week 3	Telstra	77,012	492	45%	16%	54%
	Global	—	—	—	—	—
	Hurricane	56,518	1,244	35%	6%	39%

Observed by the same server in past weeks

Significant advantage to

- maintaining history at the holder nodes, and
- sharing information across organizations



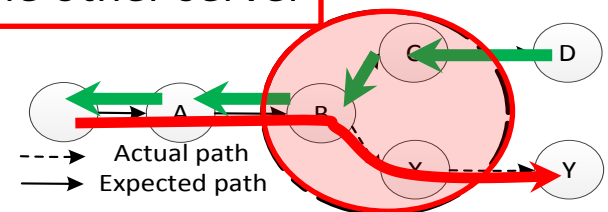
Redundancy in Unique Triples

				Redundancy in triples		
	Server	Traceroute	Triples	History	Sharing	Hybrid
Week 1	Telstra	66,985	372	–	12%	–
	Global	55,144	292	–	15%	–
	Hurricane	–	–	–	–	–
Week 2	Telstra	102,689	539	32%	14%	41%
	Global	63,434	82	27%	26%	38%
	Hurricane	60,628	1,422	4%	6%	7%
Week 3	Telstra	77,012	492	45%	16%	54%
	Global	–	–	–	–	–
	Hurricane	56,518	1,244	35%	6%	39%

Also seen by at least one of the other server

Significant advantage to

- maintaining history at the holder nodes, and
- sharing information across organizations



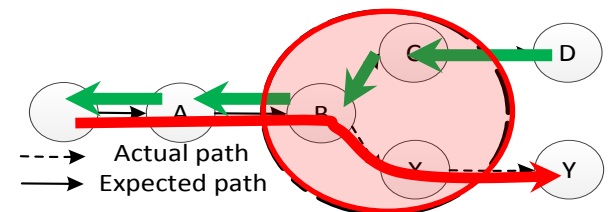
Redundancy in Unique Triples

				Redundancy in triples		
	Server	Traceroute	Triples	History	Sharing	Hybrid
Week 1	Telstra	66,985	372	—	12%	—
	Global	55,144	292	—	15%	—
	Hurricane	—	—	—	—	—
Week 2	Telstra	102,689	539	32%	14%	41%
	Global	63,434	82	27%	26%	38%
	Hurricane	60,628	1,422	4%	6%	7%
Week 3	Telstra	77,012	492	45%	16%	54%
	Global	—	—	—	—	—
	Hurricane	56,518	1,244	35%	6%	39%

Hybrid

Significant advantage to

- maintaining history at the holder nodes, and
- sharing information across organizations



Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Conclusion

- Presented design and data-driven overhead analysis of PrefiSec, a collaborative distributed system
- PrefiSec helps maintain information about the activity associated with prefixes and ASes
- Using public wide-area BGP-announcements, traceroutes, and simulations, we show that system is scalable with limited overhead
- Analysis is based on publicly available data and ASes are not required to share any sensitive information

Linköping University

expanding reality



PrefiSec: A Distributed Alliance Framework for Collaborative BGP Monitoring and Prefix-based Security

Questions?

Rahul Hiran

rahul.hiran@liu.se