Threat to BGP Policies: limited-scope more specific prefix injection

draft-francois-limited-scope-specifics-01

Pierre Francois
UCLouvain

Bruno Quoitin
UMons
Typical recognized BGP community values

- If you are my customer or a customer of my customers, you can tag
- 65000:XXX : Do not advertise to ASXXX
Legend

A BGP Prefix advertisement for p/P

An advertisement of a prefix more specific than p/P, say p/P+2
What can you do with these communities?

• Limit the scope of

• Assume A and B are providers of AS_Cust

• B allows such community tagging

• A and B are peers

• AS_Cust turns “don’t advertise to AS X” values into a only “advertise to A”
  Just put them all but A
Initial routing status
control-plane (only) driven forwarding

ISP A

ISP B

AS_Cust

$$

==

$$
Initial routing status
control-plane (only) driven forwarding

ISP A

ISP B

AS_Cust

==
Initial routing status
control-plane (only) driven forwarding

ISP A

ISP B

AS_Cust
Scope the more specific

ISP A

AS_Cust

ISP B
Scope the more specific
Scope the more specific

Only to ISP A!
Scope the more specific

ISP A

ISP B

AS_Cust

Only to ISP A!
Scope the more specific

Only to ISP A!
Scope the more specific

Only to ISP A!
Let's start playing: Scope advertisement of the more specific

ISP A does not propagate BGP paths for to its providers and peers.

It still does for

is likely to be installed in the FIB!
New paths in the network
New paths in the network
How to detect Data-plane

- Netflow
  - Am I transiting traffic from $X$ to $Y$?
  - Warning upon policy violating $(X,Y)$
How to detect Control plane

• Useless?
How to detect

• Concern about being playing the role of ISP
• Monitor their use