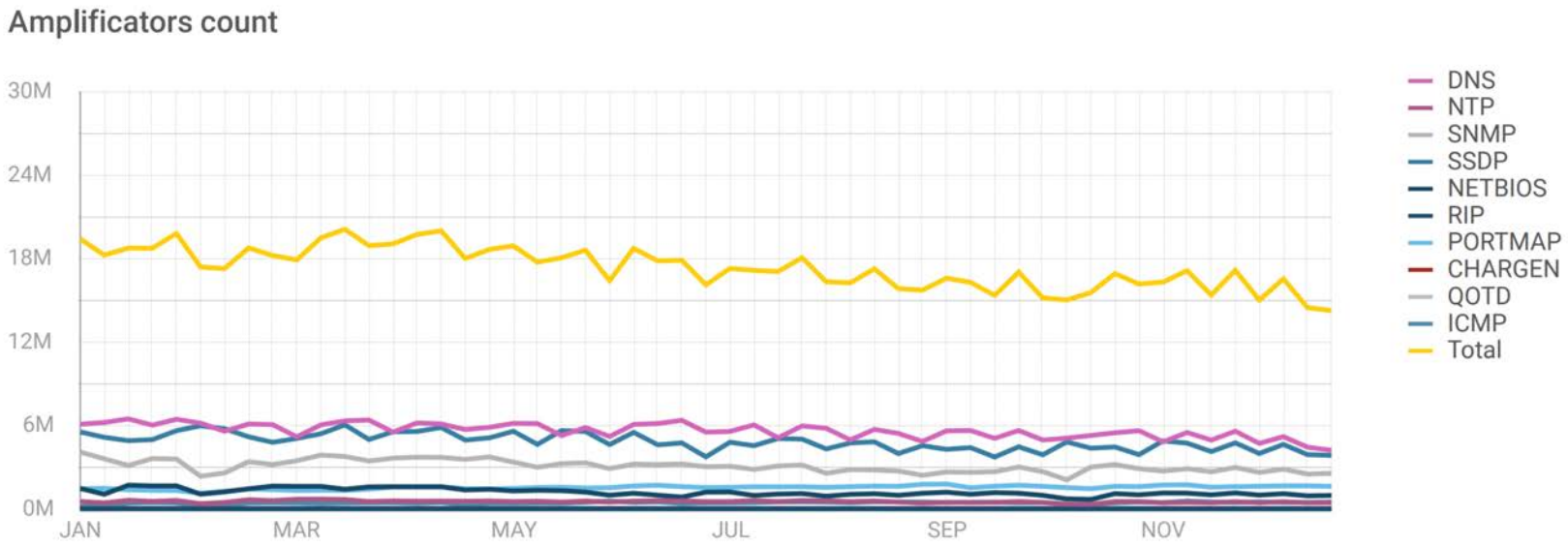
Anti Spoofing. Reboot.

Alexander Azimov <aa@qrator.net>

IP Spoofing

- Attacks on TCP stack;
- TCP floods (SYN, ACK,…);
- Reflection Attacks;
- Amplification Attacks.

DDoS Amplifiers



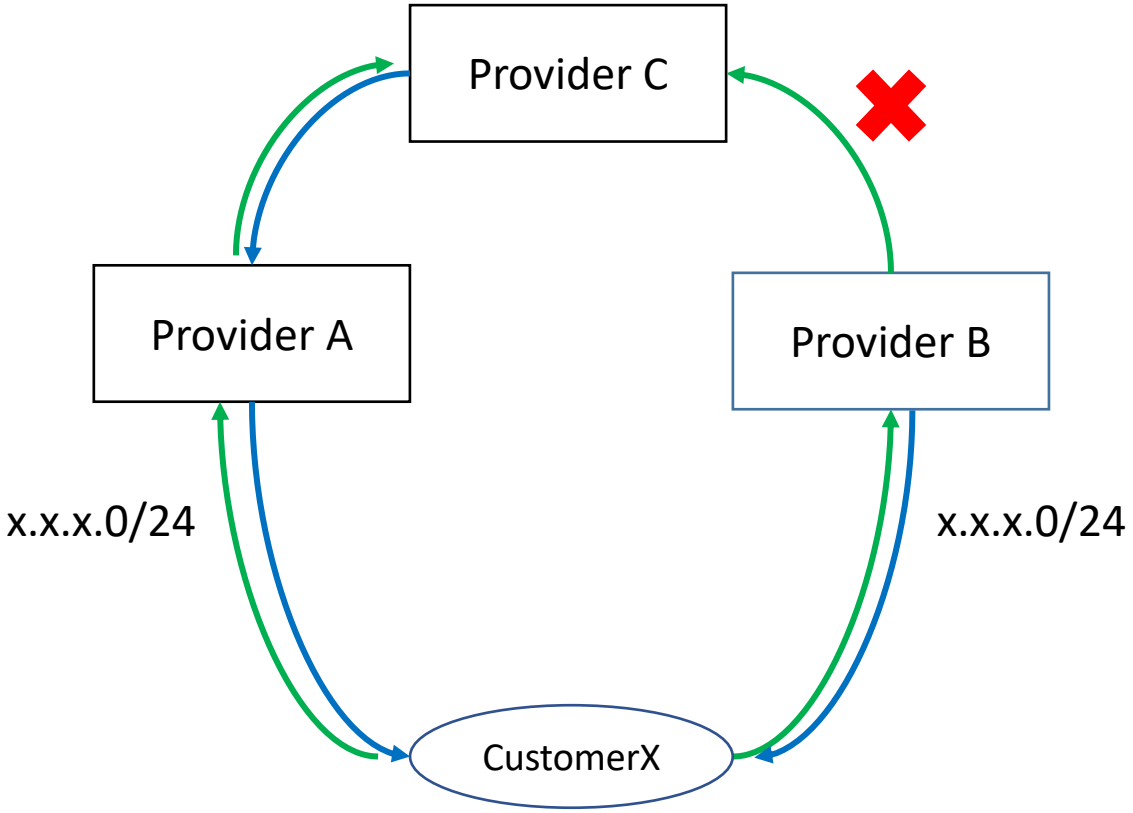
Source: [Qrator Labs annual report 2017]

BCP84: uRPF

https://tools.ietf.org/html/bcp84

- Strict mode;
- Feasible mode;
- Loose mode.

Strict Mode



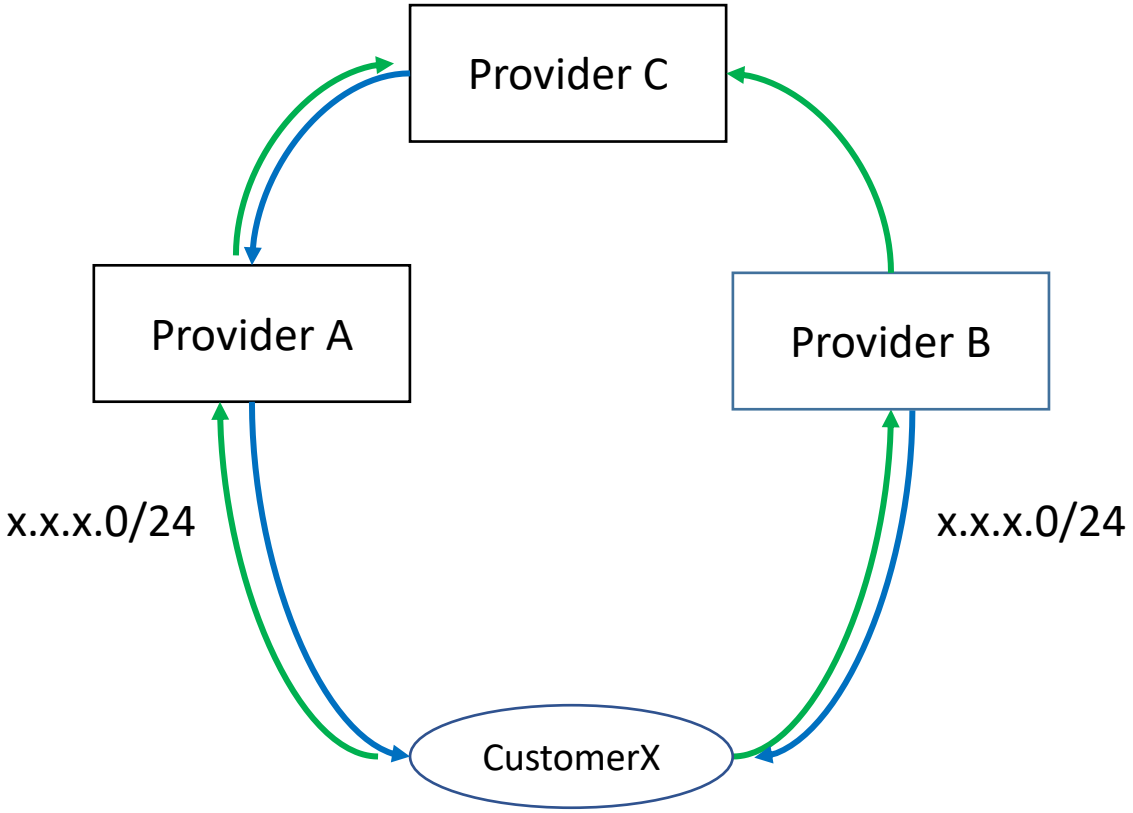
Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	X
C	A X

Rule: incoming interface = interface for the best route for SRC_IP

Loose Mode



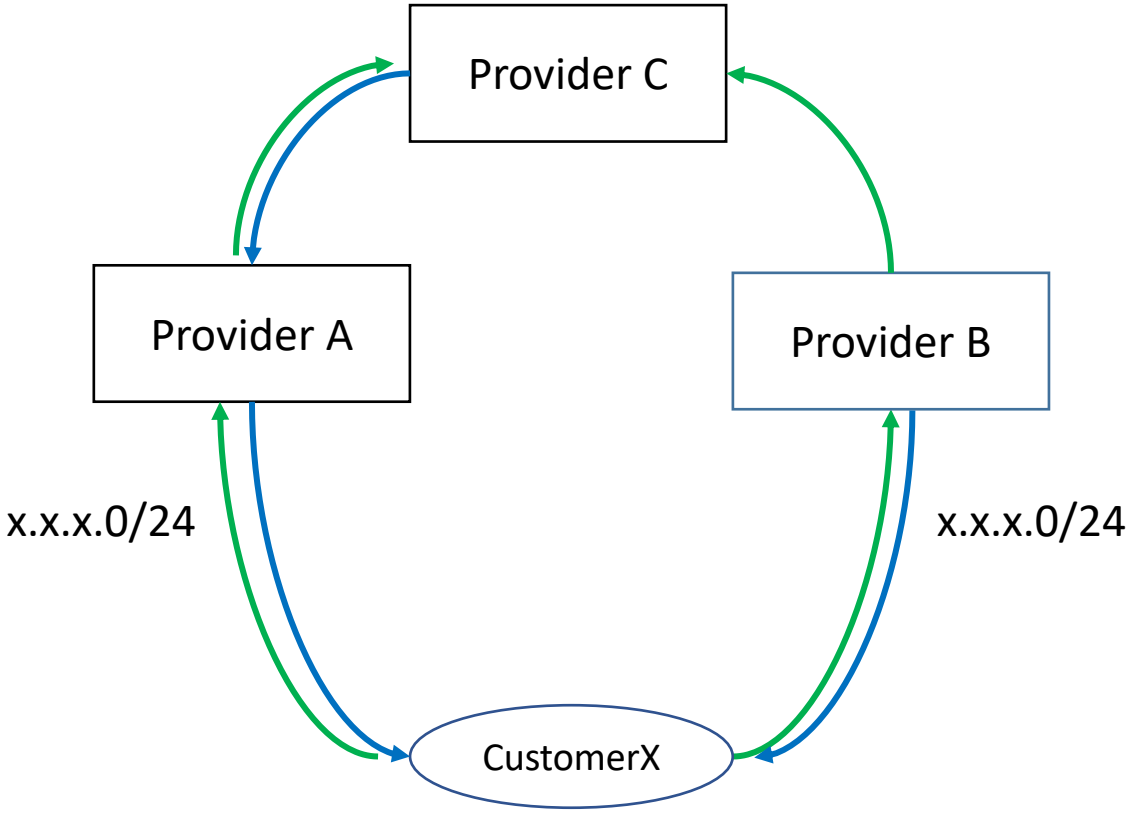
Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	X
C	A X

Rule: there is a route for SRC_IP

Feasible Mode



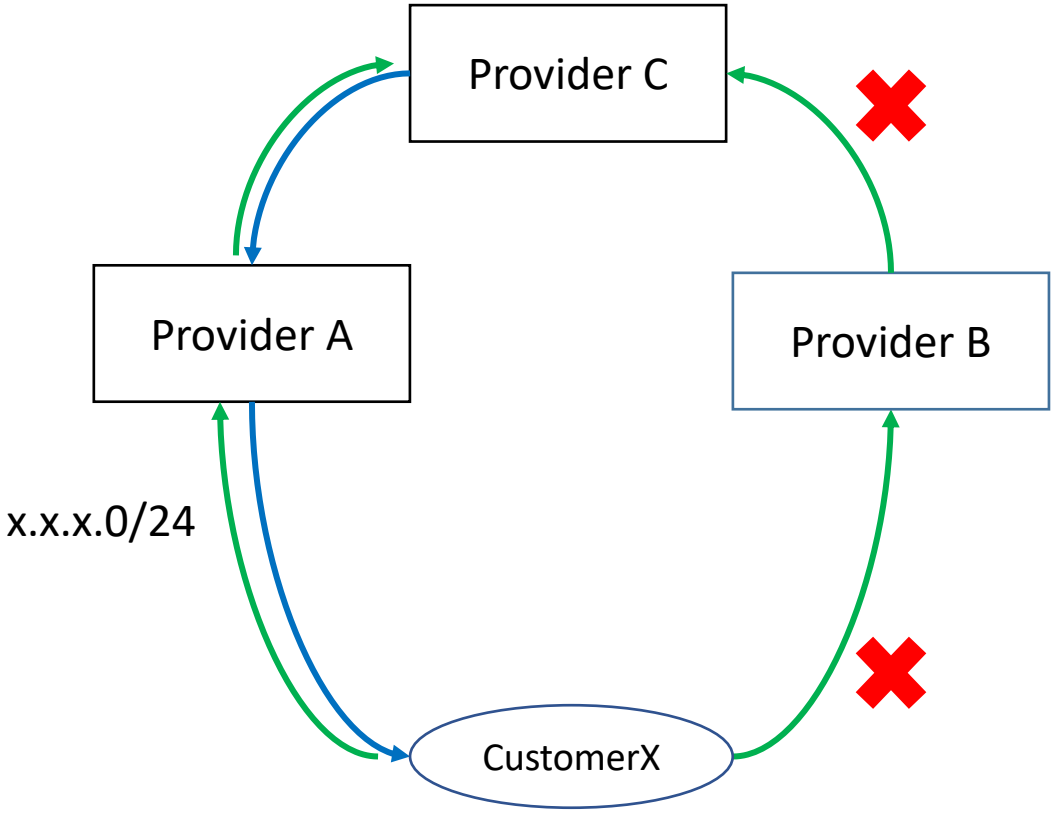
Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	X
C	A X

Rule: incoming interface = interface for ~~the best~~ route for SRC_IP

Feasible Mode



Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	C A X
C	A X

Rule: incoming interface = interface for ~~the best~~ route for SRC_IP

BCP84: uRPF

https://tools.ietf.org/html/bcp84

- Strict mode – not working;
- Loose mode – does nothing.
- Feasible mode – not working;

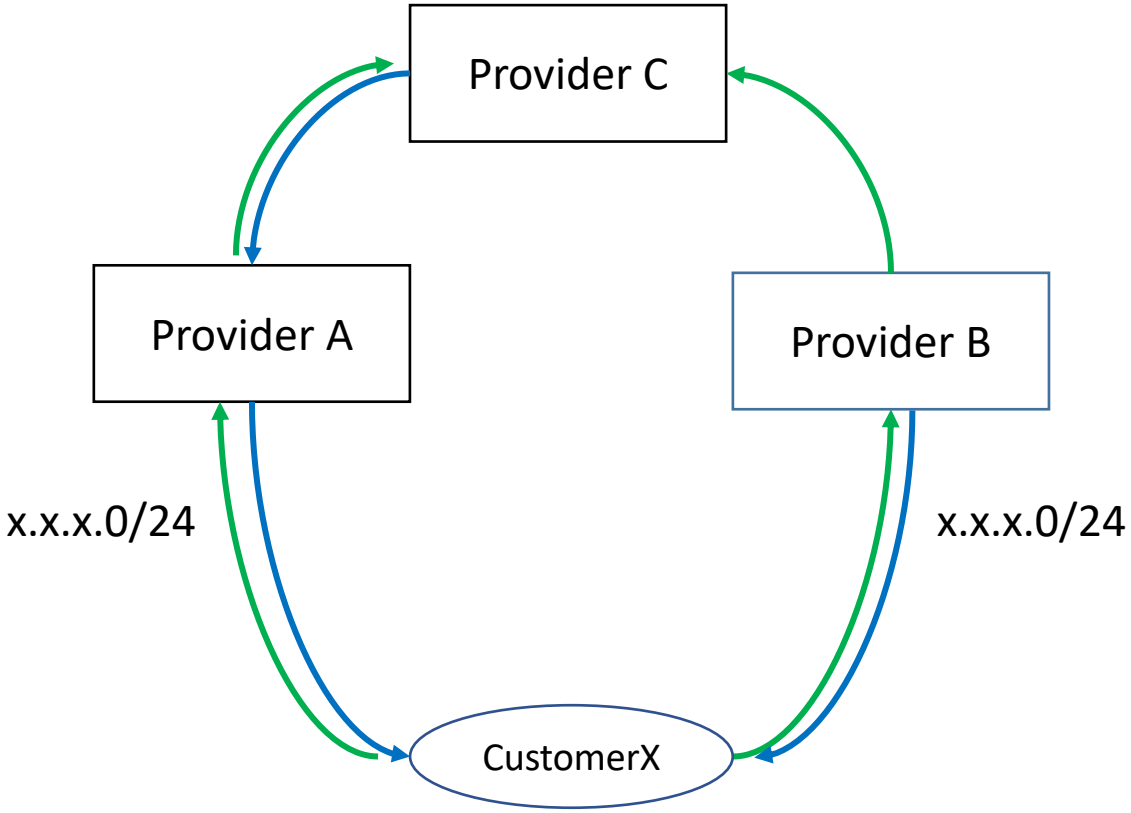
Problem Statement

A distance-vector protocol isn't the best way to propagate availability information.

Option №1: New SAFI

Hacking

Option №2: AS-SETs



Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	X
C	A X

Rule: Check that SRC_IP belongs to customer's AS_SET

Option №2: AS-SETs

Transformation of ingress filters into ACLs.

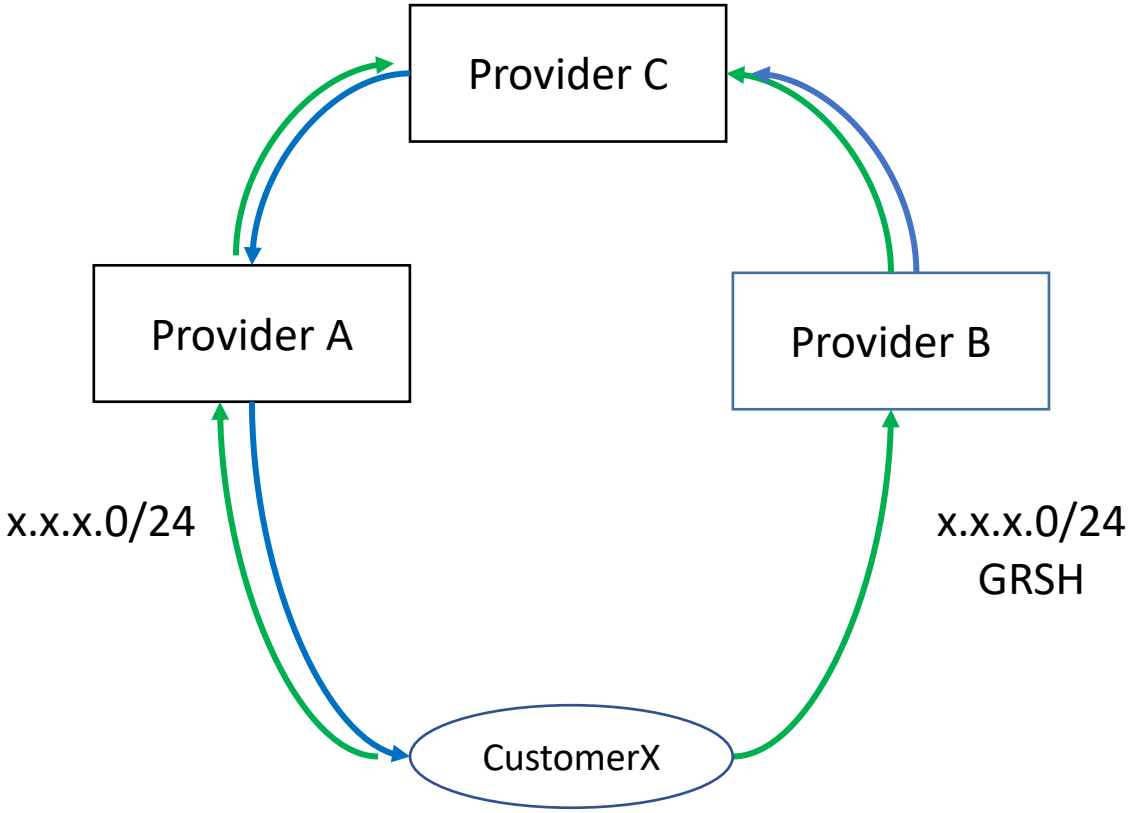
Positive:

- We do not need to change specification;
- We do not need to ship new software;
- Can be used by any ISP, isn't it?

Negative:

- AS-SETs are outdated, unauthorized;
- Scalability problems.

Option 3: GRSH + Feasible Mode



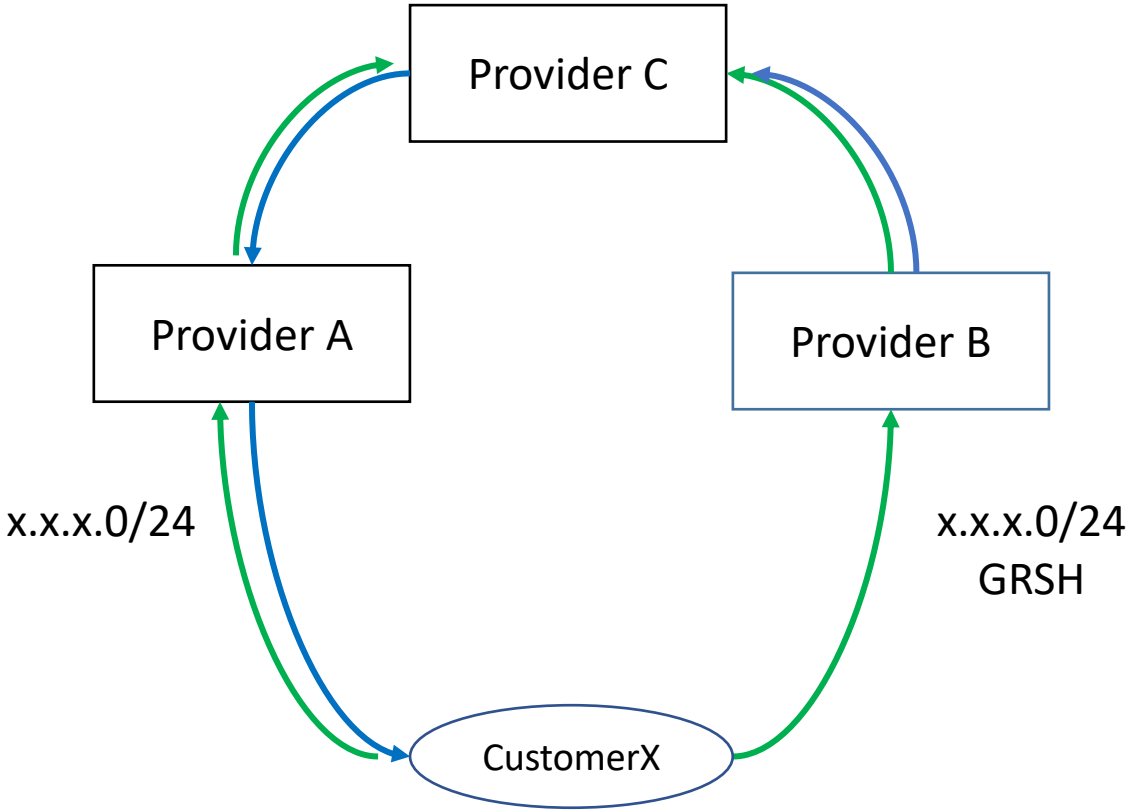
Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	C A X
C	A X

A new transit well-known community that sets LOCAL_PREF to 0.

Option 3: GRSH + Feasible Mode



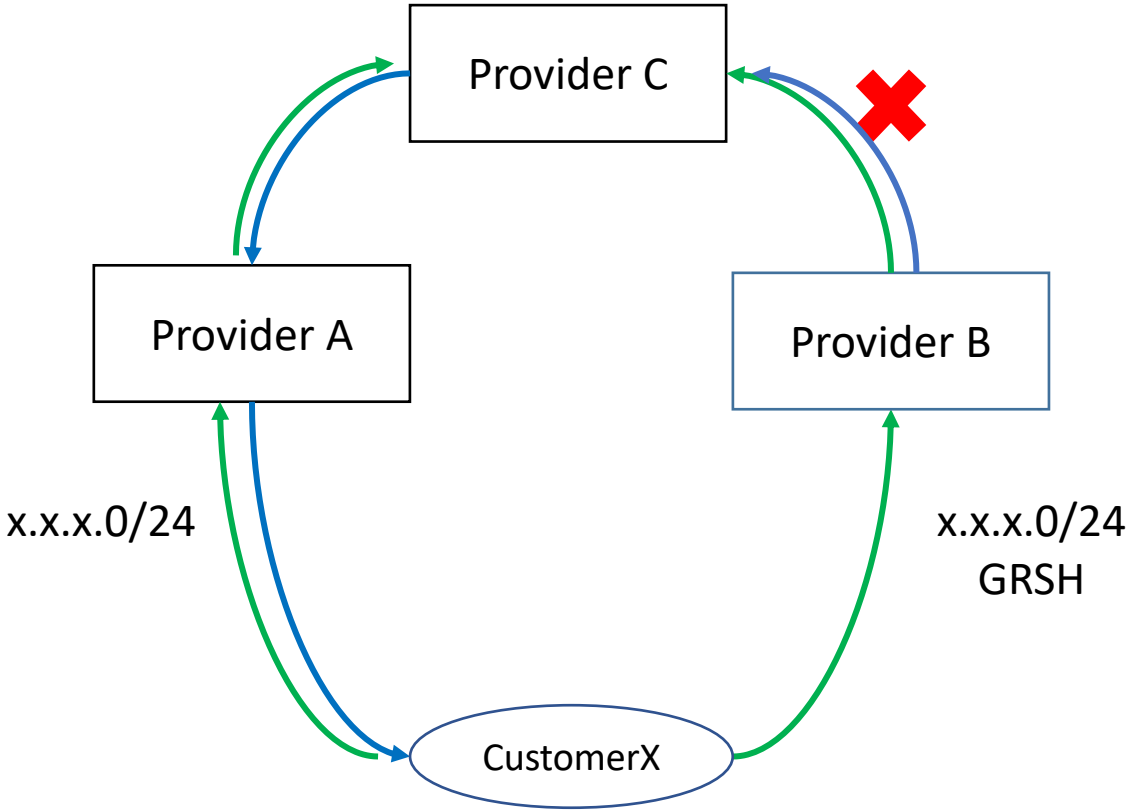
Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	C A X
C	A X

Provider B sees x.x.x.0/24 route, but doesn't use it.
x.x.x.0/24 route marked with GRSH – informational message

Option 3: GRSH + Feasible Mode



Ingress Traffic

Egress Traffic

Provider	AS_PATH
A	X
B	C A X
C	A X

Works only for multihomed ISPs…
But it more then 85% of all ISPs in the world!

Option 3: GRSH + Feasible Mode

GRACEFUL_SHTUTDOWN community creates informational message for directly connected peers.

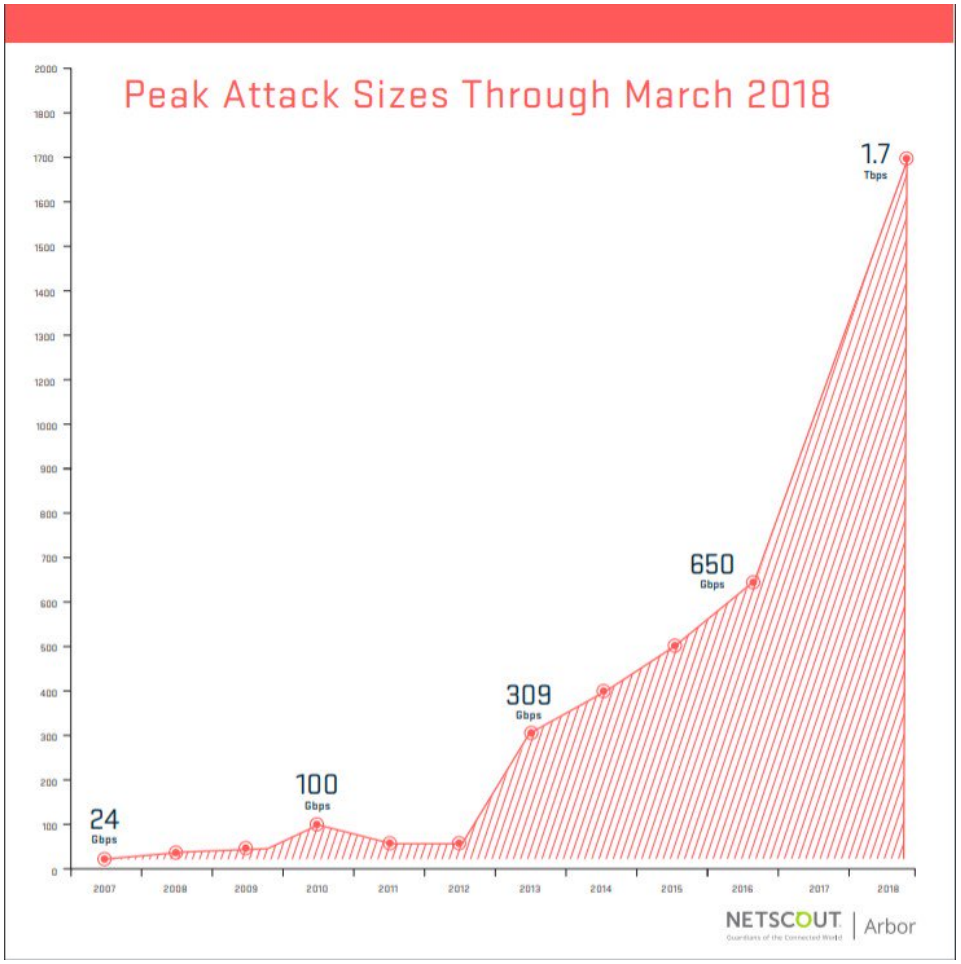
Positive:

- We do not need to change specification;
- We do not need to ship new software;
- We solve problem for multihomed of ISPs.

Negative:

- A lot of work with customers is required;
- Doesn’t work between transit ISPs.

Option 4: Do Nothing.



But are you prepared?

http://etc.ch/kfR6/

Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

https:// directpoll.com/r?XDbzPBd3ixYqg8Ahdffp0pN7Qjc4u9XCcBrHS6Z8g

Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.

Preview