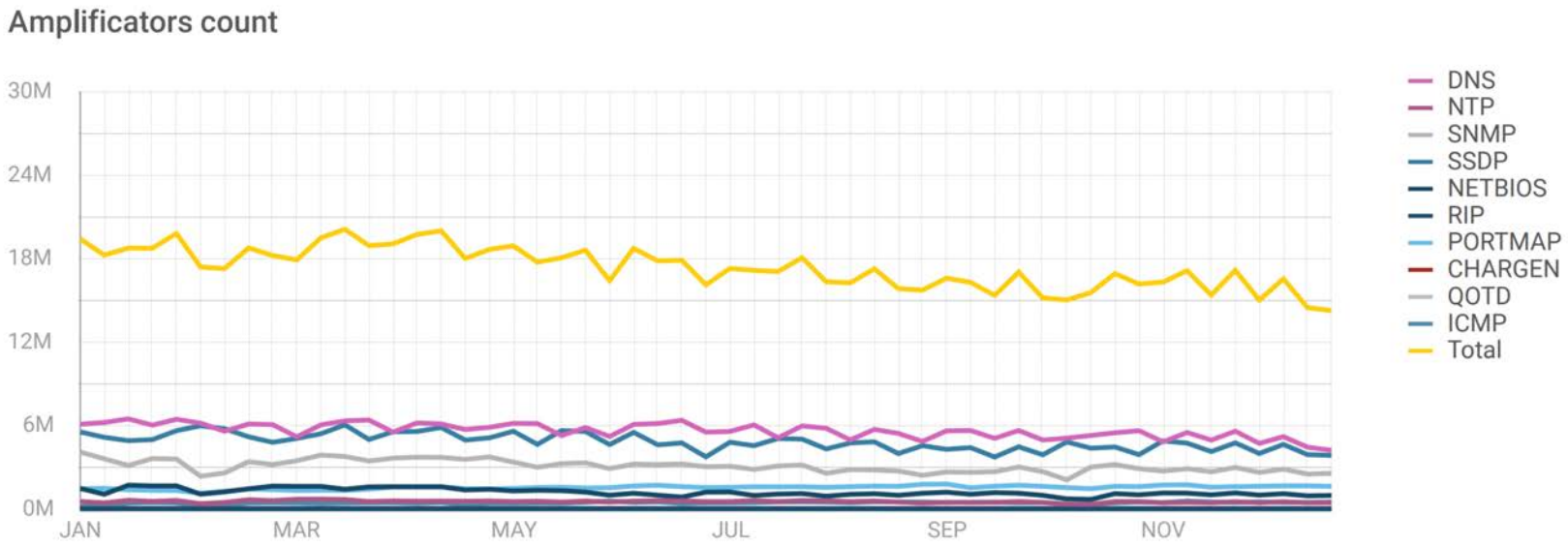
Anti Spoofing. Reboot.

Alexander Azimov <aa@qrator.net>

IP Spoofing

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

DDoS Amplifiers



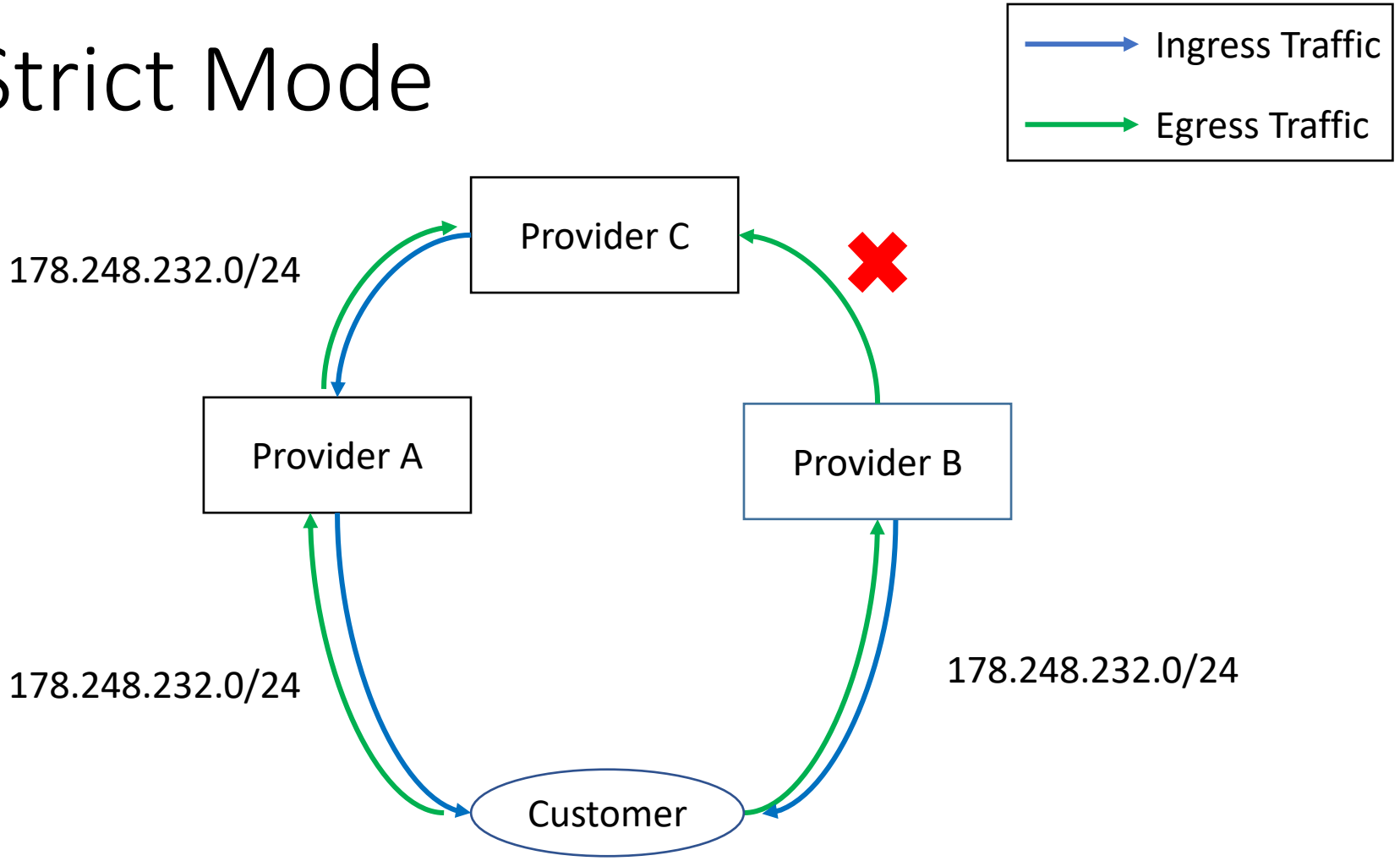
Source: [Qrator Labs annual report 2017]

BCP84: uRPF

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

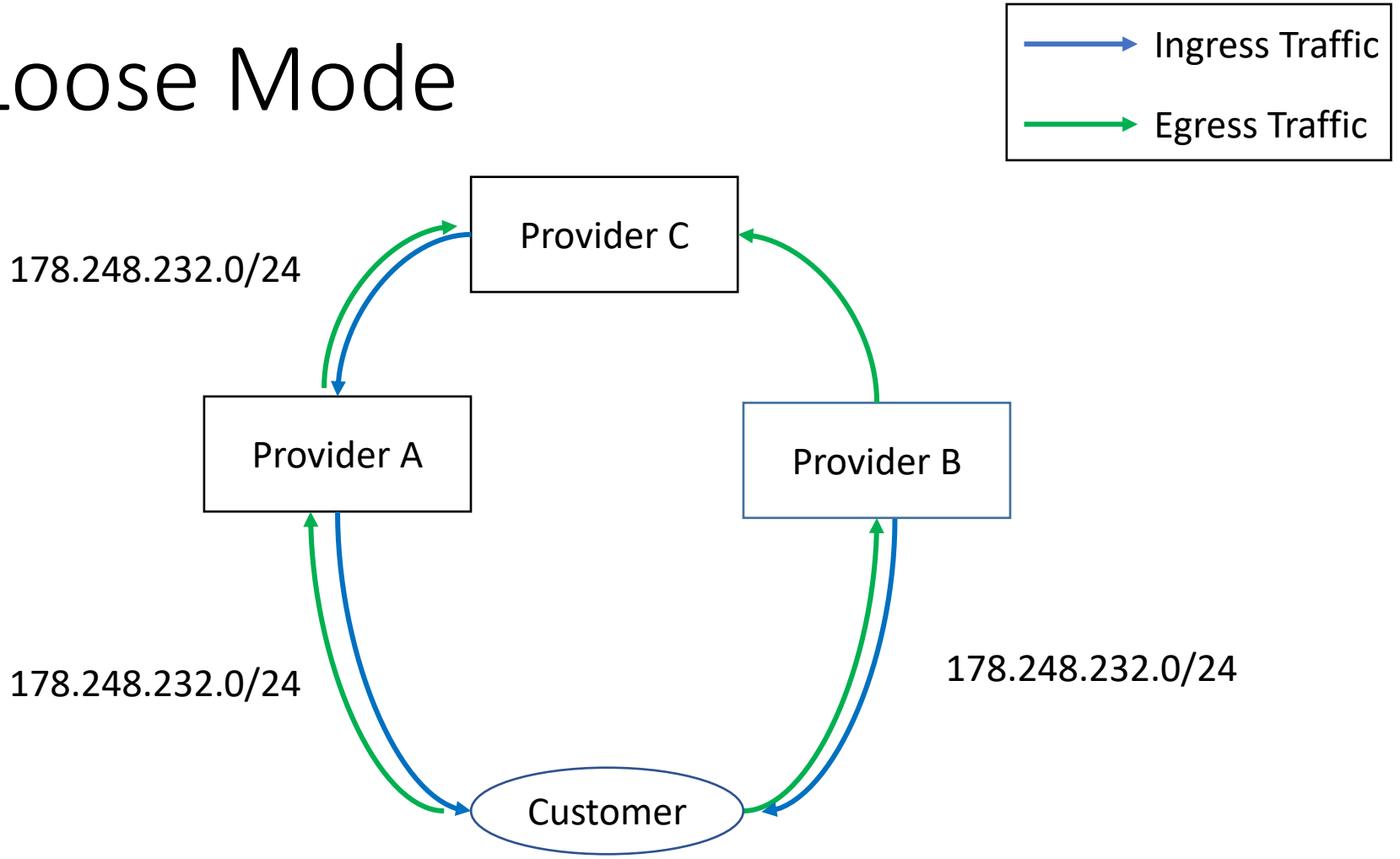
- Strict mode;
- Feasible mode;
- Loose mode.

Strict Mode



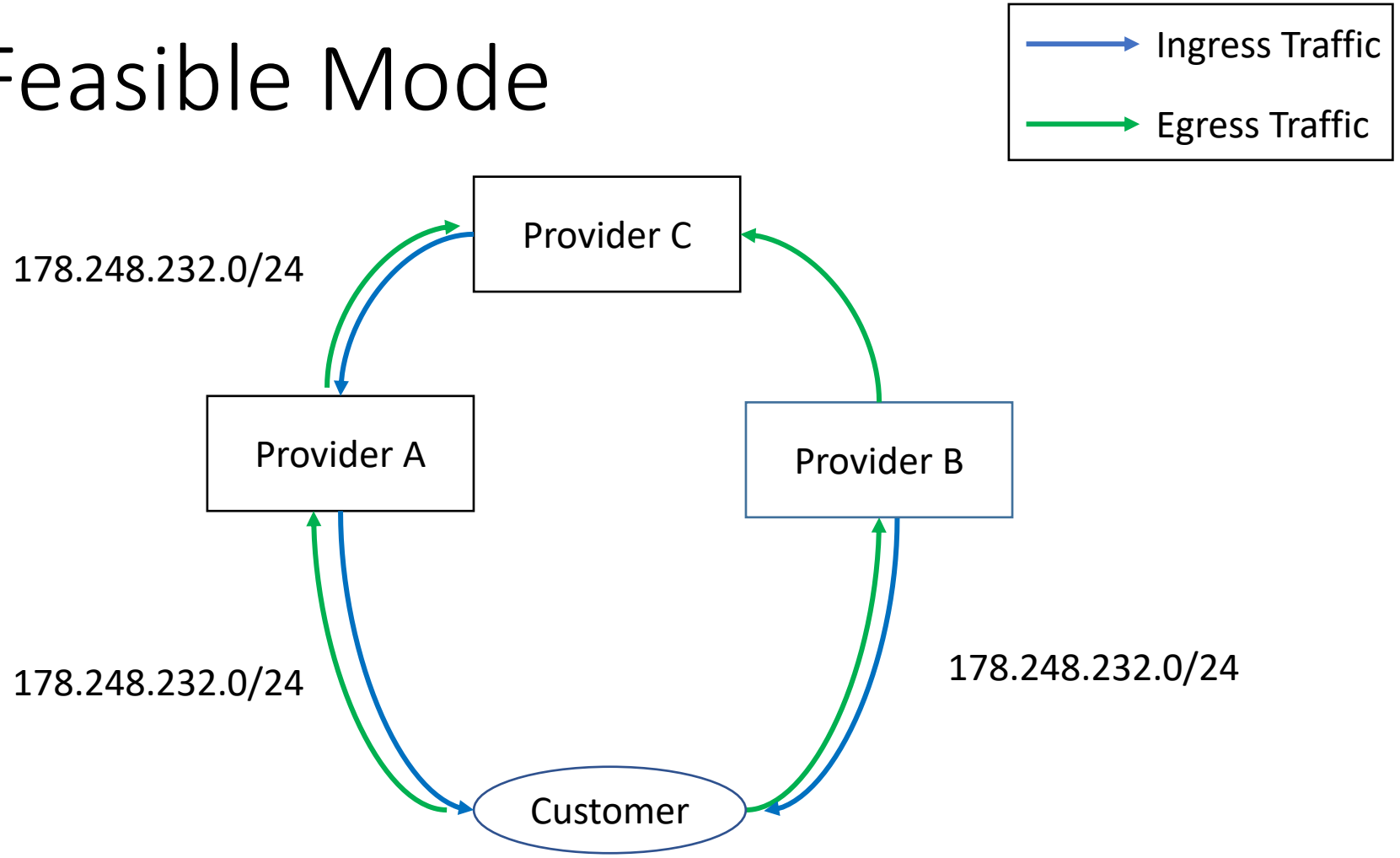
Rule: incoming interface = interface for the best route for SRC_IP

Loose Mode



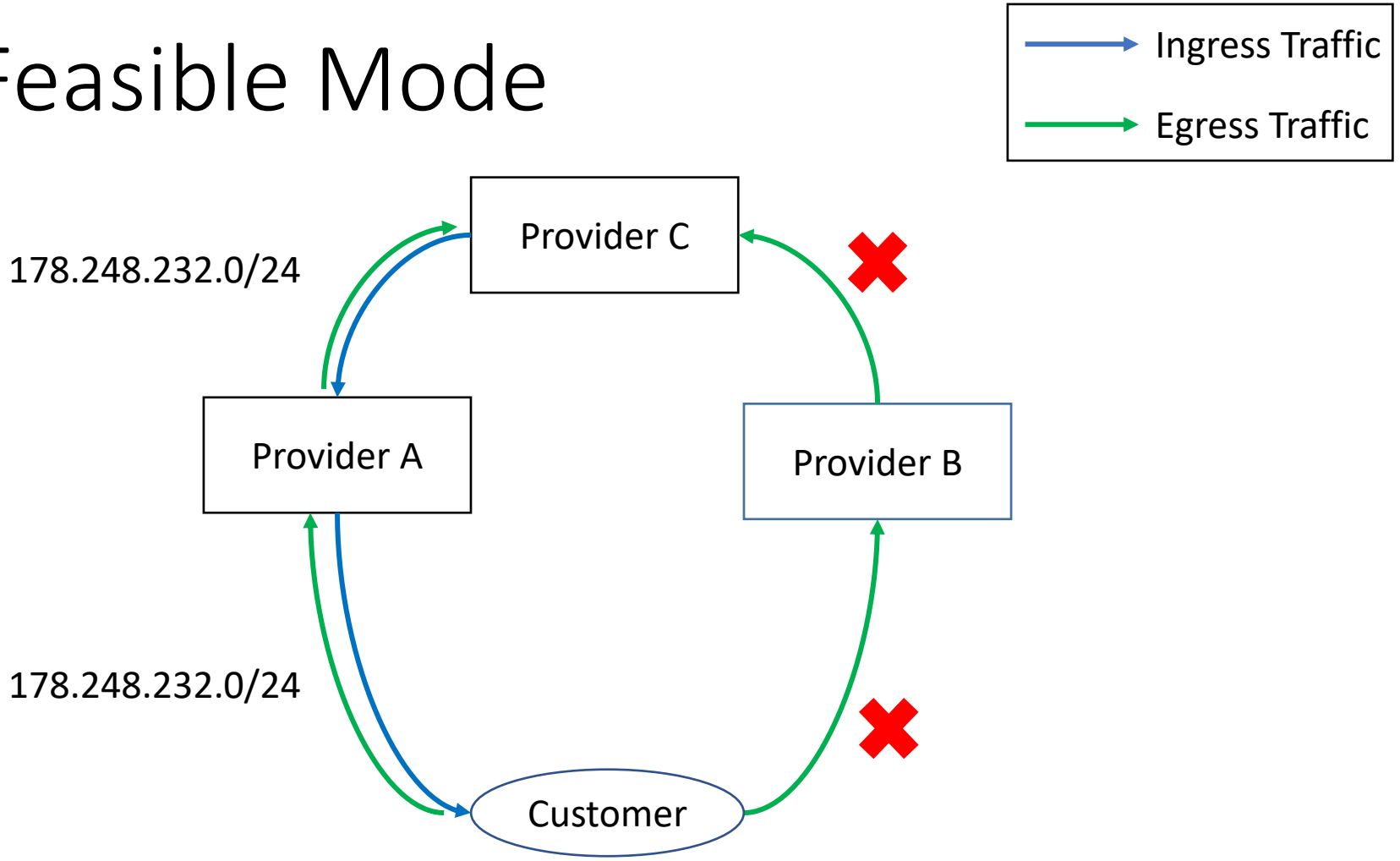
Rule: there is a route for SRC_IP

Feasible Mode



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

Feasible Mode

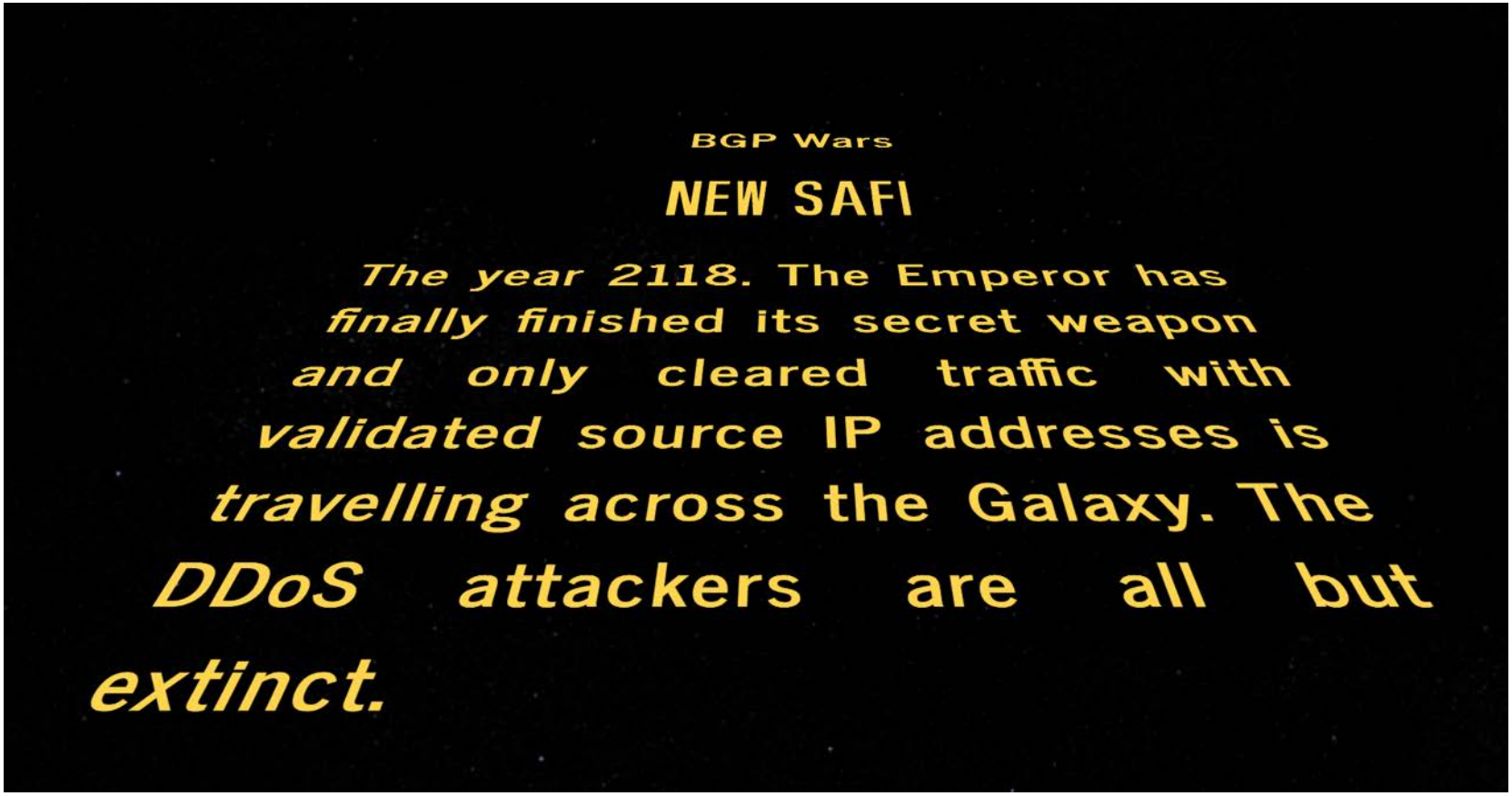


Rule: incoming interface = interface for ~~the best~~ route for SRC_IP

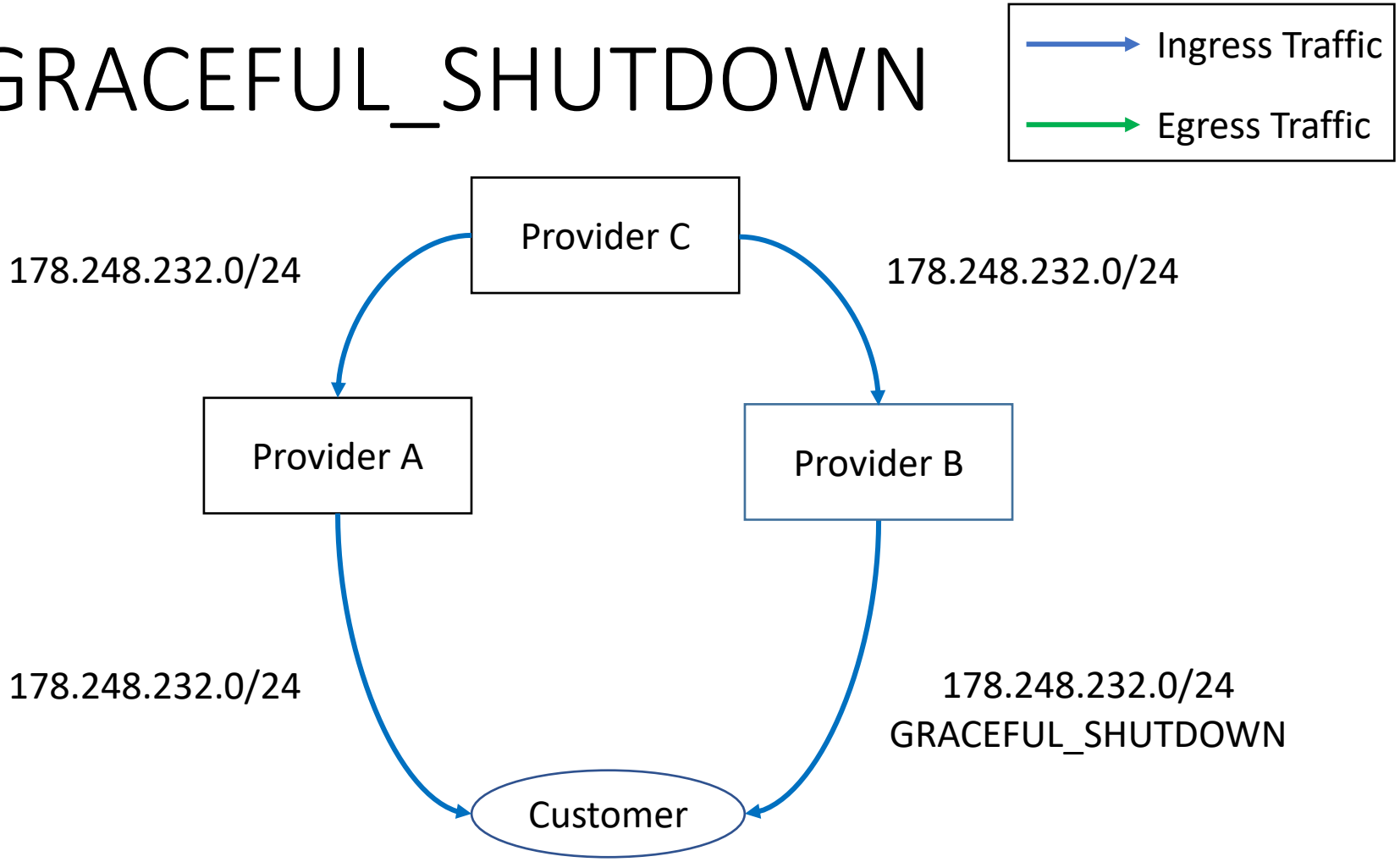
Problem Statement

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

Option №1: New SAFI

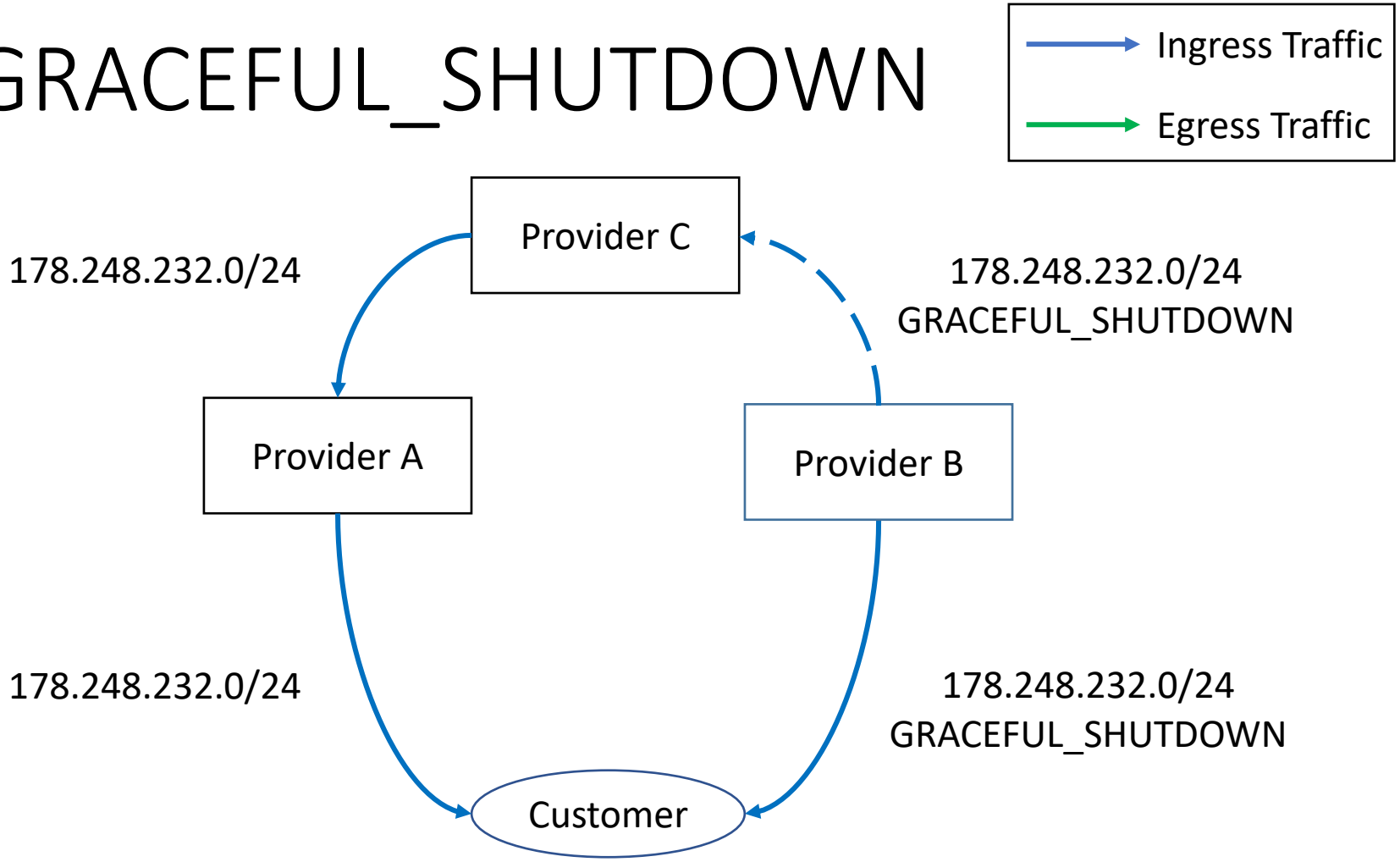


GRACEFUL_SHUTDOWN



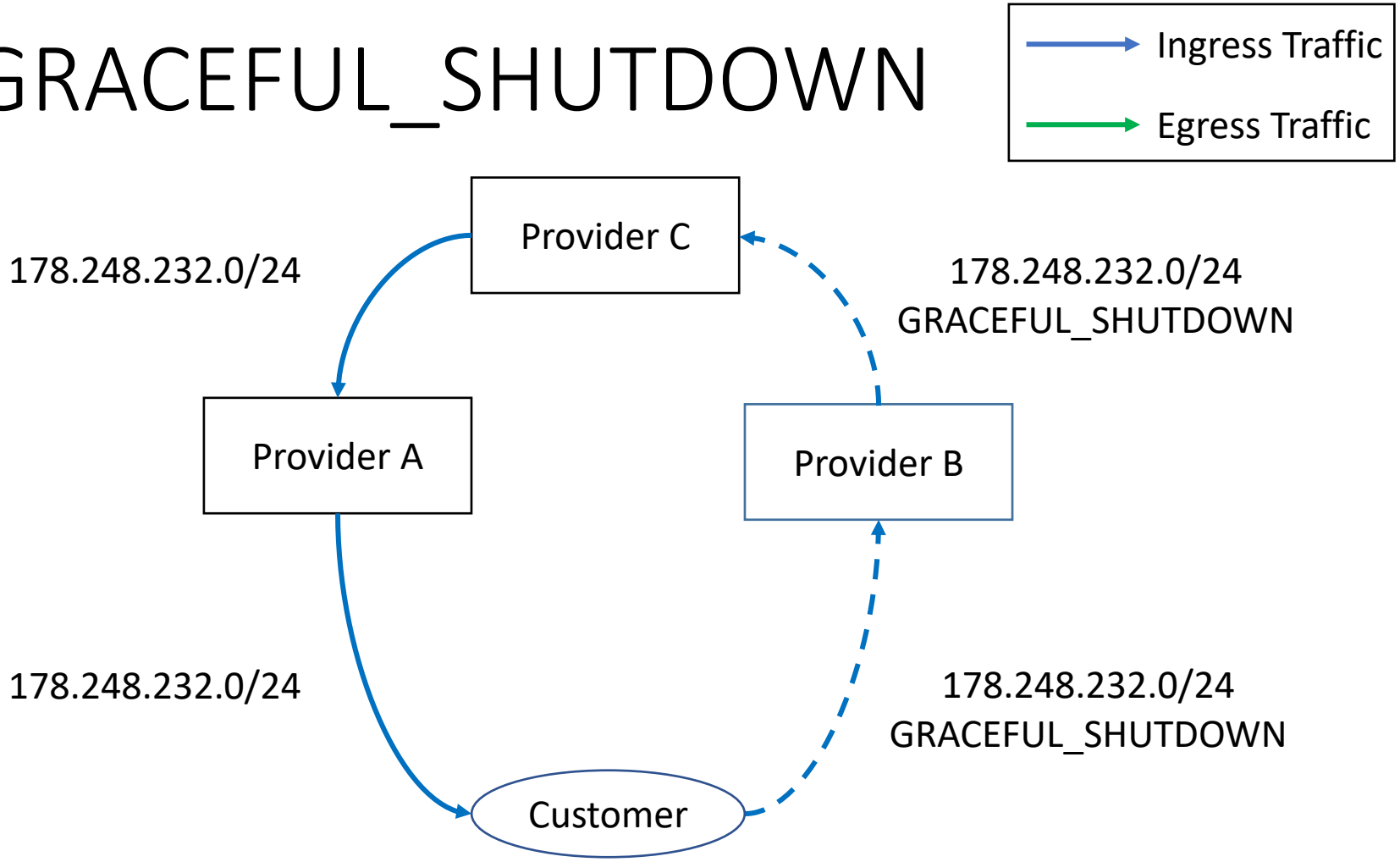
A new transit well-known community that sets LOCAL_PREF to 0.

GRACEFUL_SHUTDOWN



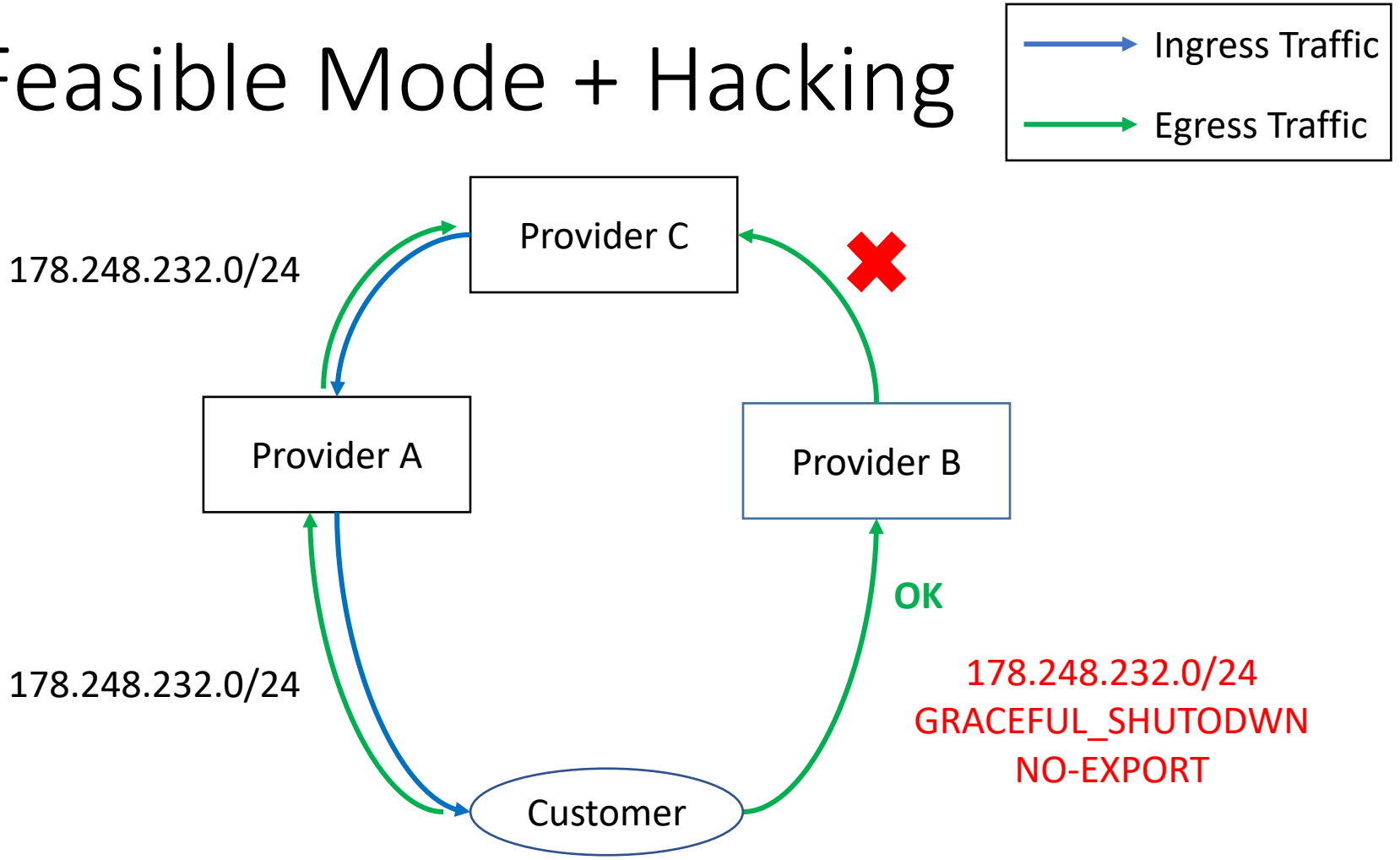
A new transit well-known community that sets LOCAL_PREF to 0.

GRACEFUL_SHUTDOWN



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

Feasible Mode + Hacking



Works only for stub ASNs.
But it's more than 85% of entire Internet!

Option 2: Hacking

GRACEFUL_SHTUTDOWN + NO-EXPORT communities can be used as informational message for directly connected peers.

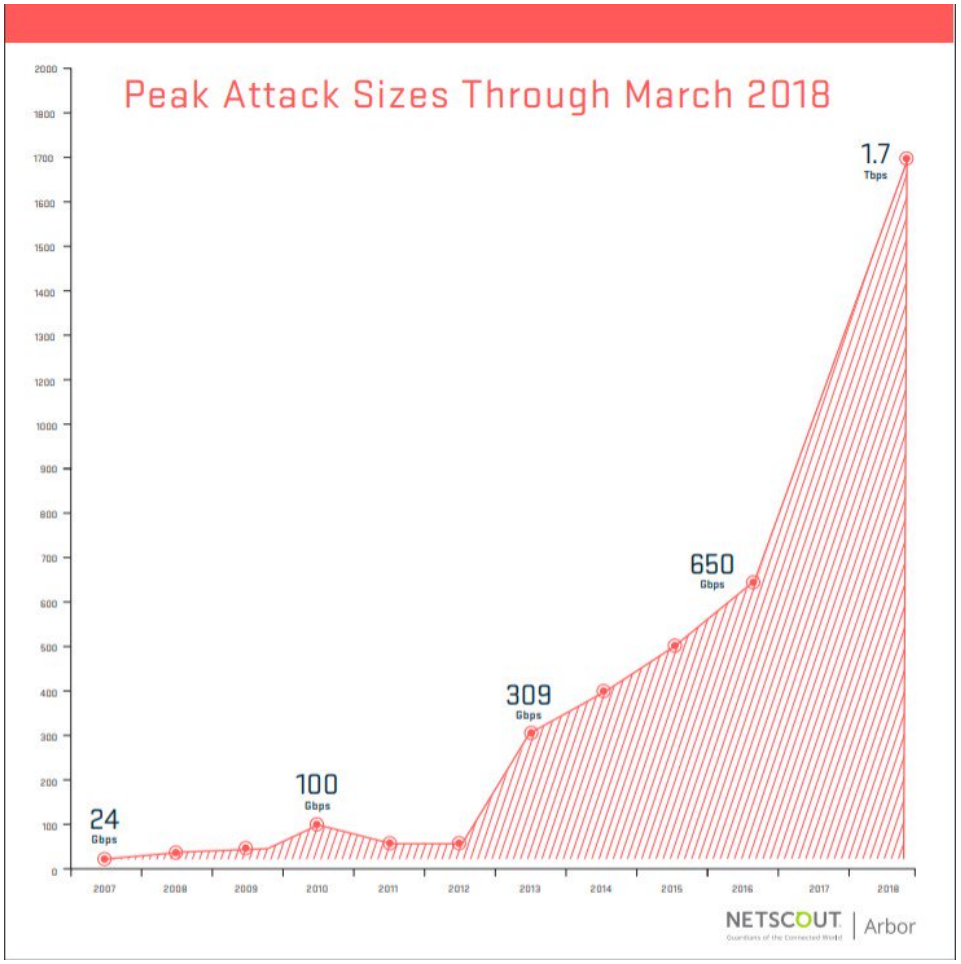
Positive:

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

Negative:

- A lot of work with customers is required;

Option 3: 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