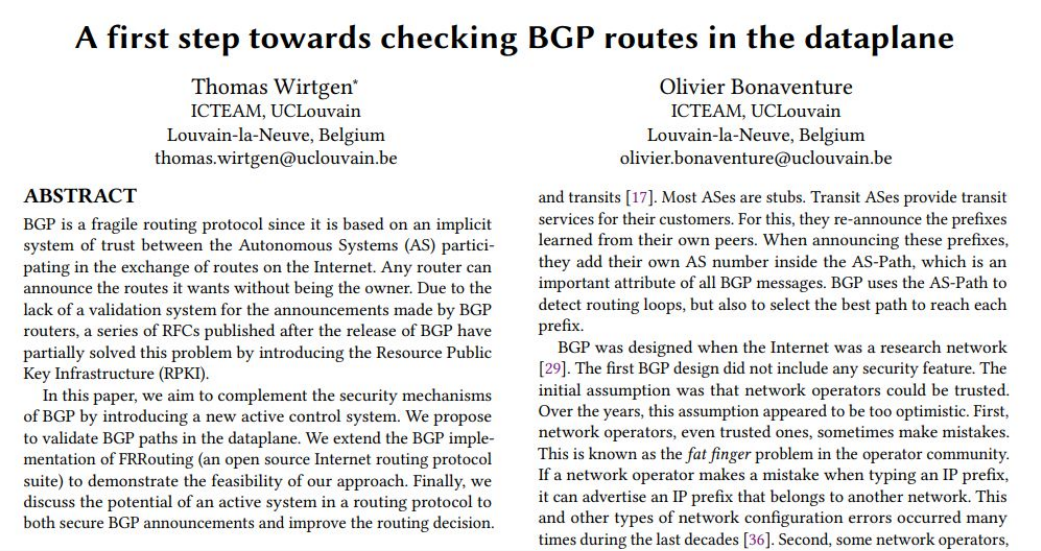
A first step towards checking BGP routes in the dataplane

Thomas Wirtgen and Olivier Bonaventure

Before starting



A first step towards checking BGP routes in the dataplane

Thomas Wirtgen*
ICTEAM, UCLouvain
Louvain-la-Neuve, Belgium
thomas.wirtgen@uclouvain.be

Olivier Bonaventure
ICTEAM, UCLouvain
Louvain-la-Neuve, Belgium
olivier.bonaventure@uclouvain.be

ABSTRACT

BGP is a fragile routing protocol since it is based on an implicit system of trust between the Autonomous Systems (AS) participating in the exchange of routes on the Internet. Any router can announce the routes it wants without being the owner. Due to the lack of a validation system for the announcements made by BGP routers, a series of RFCs published after the release of BGP have partially solved this problem by introducing the Resource Public Key Infrastructure (RPKI).

In this paper, we aim to complement the security mechanisms of BGP by introducing a new active control system. We propose to validate BGP paths in the dataplane. We extend the BGP implementation of FRRouting (an open source Internet routing protocol suite) to demonstrate the feasibility of our approach. Finally, we discuss the potential of an active system in a routing protocol to both secure BGP announcements and improve the routing decision.

and transits [17]. Most ASes are stubs. Transit ASes provide transit services for their customers. For this, they re-announce the prefixes learned from their own peers. When announcing these prefixes, they add their own AS number inside the AS-Path, which is an important attribute of all BGP messages. BGP uses the AS-Path to detect routing loops, but also to select the best path to reach each prefix.

BGP was designed when the Internet was a research network [29]. The first BGP design did not include any security feature. The initial assumption was that network operators could be trusted. Over the years, this assumption appeared to be too optimistic. First, network operators, even trusted ones, sometimes make mistakes. This is known as the *fat finger* problem in the operator community. If a network operator makes a mistake when typing an IP prefix, it can advertise an IP prefix that belongs to another network. This and other types of network configuration errors occurred many times during the last decades [36]. Second, some network operators,

Paper submitted on May 2022.

Accepted for FIRA 22’ SIGCOMM Workshop.

Why checking routes in the dataplane ?

When a router receives a new route, it is not sure if the sender is legitimate

BGP was designed without regard to security

The lack of security mechanism in BGP against **attackers**

Pakistan Blocks YouTube Video Access

By SADAQAT JAN – **4 days ago**

ISLAMABAD, Pakistan (AP) — Pakistan's government has banned access to the video-sharing Web site YouTube because of anti-Islamic movies that users have posted on the site, an official said Sunday.

Catalin Cimpanu | February 14, 2022

KlaySwap crypto users lose funds after BGP hijack

Cybercrime | News | Technology

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

Chinese ISP hijacks the Internet

Posted by Andree Toonk - April 8, 2010 - Hijack - 25 Comments

This morning many BGPmon.net users received an alert regarding a possible prefix hijack by a Chinese network. AS23724 is one of the Data Centers operated by China Telecom, China's largest ISP. Normally AS23724 CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation only originates about 40 prefixes, however today for about 15 minutes they originated about ~37,000 unique prefixes that are not assigned to them. This is what we typically call a prefix hijack. This incident follows another concerning incident from China 2 weeks ago. Although it

Doug Madory
@DougMadory

As of 00:19 UTC on 6-Jul, AS3356 started announcing 2000::/12, the largest IPv6 (or IPv4 for that matter) prefix in the global routing table.

Jerome Fleury
@jerome_fzx

So Airtel AS9498 announced the entire IPv6 block 2400::/12 for a week and no-one notices until @strickx finds out and they confirm it was a typo of /127. Below is @GTTCOMM happily accepting the prefix. The state of routing security is 🏠.
stat.ripe.net/widget/bgplay#...

The lack of security mechanism in BGP against **misconfigurations**

Pakistan Blocks YouTube Video Access

By SADAQAT JAN – **4 days ago**

ISLAMABAD, Pakistan (AP) — Pakistan's government has banned access to the video-sharing Web site YouTube because of anti-Islamic movies that users have posted on the site, an official said Sunday.

Catalin Cimpanu | February 14, 2022

KlaySwap crypto users lose funds after BGP hijack

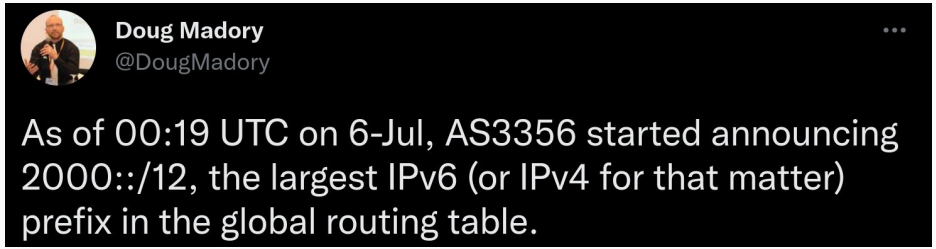
Cybercrime | News | Technology

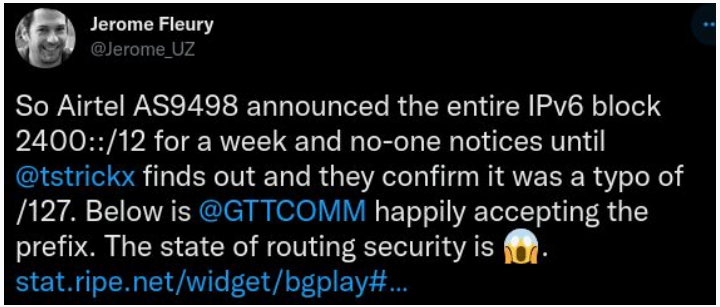
Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

Chinese ISP hijacks the Internet

Posted by Andree Toonk - April 8, 2010 - Hijack - 25 Comments

This morning many BGPmon.net users received an alert regarding a possible prefix hijack by a Chinese network. AS23724 is one of the Data Centers operated by China Telecom, China's largest ISP. Normally AS23724 CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation only originates about 40 prefixes, however today for about 15 minutes they originated about ~37,000 unique prefixes that are not assigned to them. This is what we typically call a prefix hijack. This incident follows another concerning incident from China 2 weeks ago. Although it





The lack of security mechanism in BGP

Extensions has been proposed to secure BGP :

- RPKI Route Origin Authorizations (ROAs): RFC6811
  - Slowly getting adopted
- BGPSec: RFC8205
  - Not deployed
- Pretty Good BGP
  - Not adopted
- etc.

The lack of security mechanism in BGP

Extensions has been proposed to secure BGP :

- RPKI Route Origin Authorizations (ROAs): RFC6811
  - Slowly getting adopted
- BGPSec: RFC8205
  - Not deployed
- Pretty Good BGP
  - Not adopted
- etc.

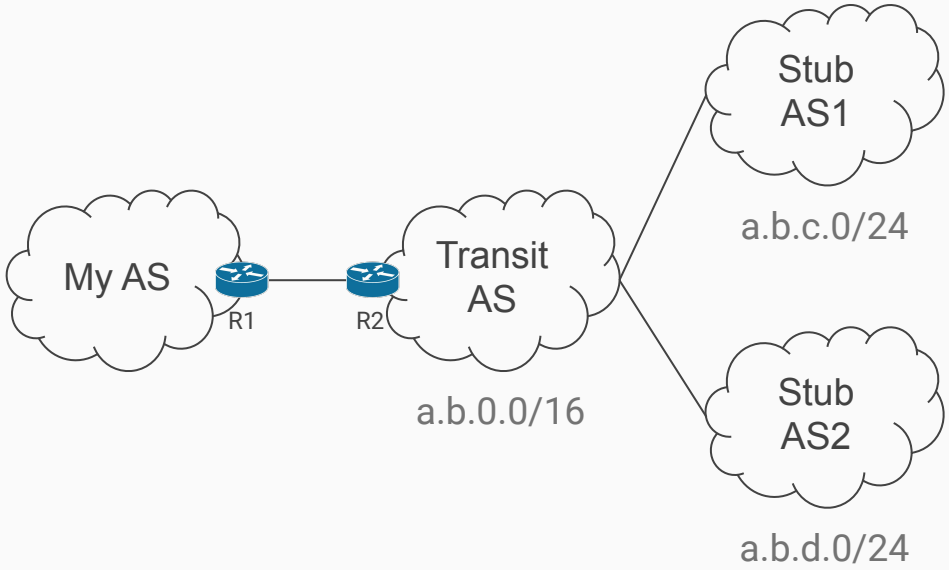
These extensions do not solve all security issues !

The lack of security mechanism in BGP

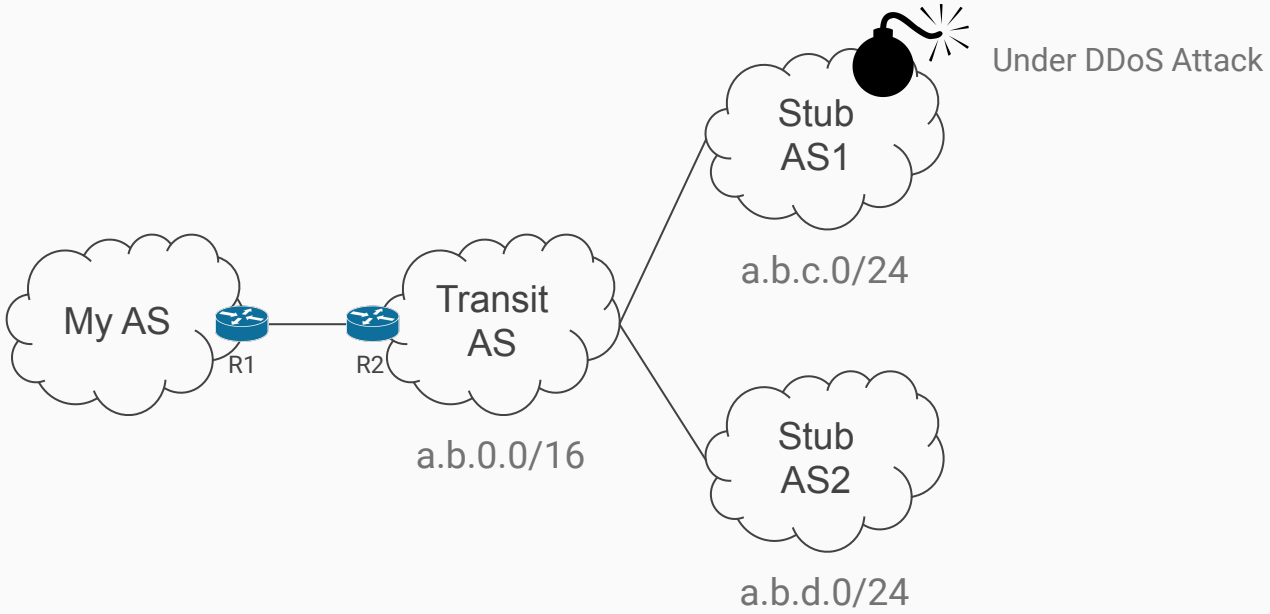
Extensions has been proposed to secure BGP :

- RPKI Route Origin Authorizations (ROAs): RFC6811
  - Slowly getting adopted
- BGPSec: RFC8205
  - Not deployed
- Pretty Good BGP
  - Not adopted
- **Our solution: Contact a destination to the target prefix to check if the route is reachable in the dataplane**

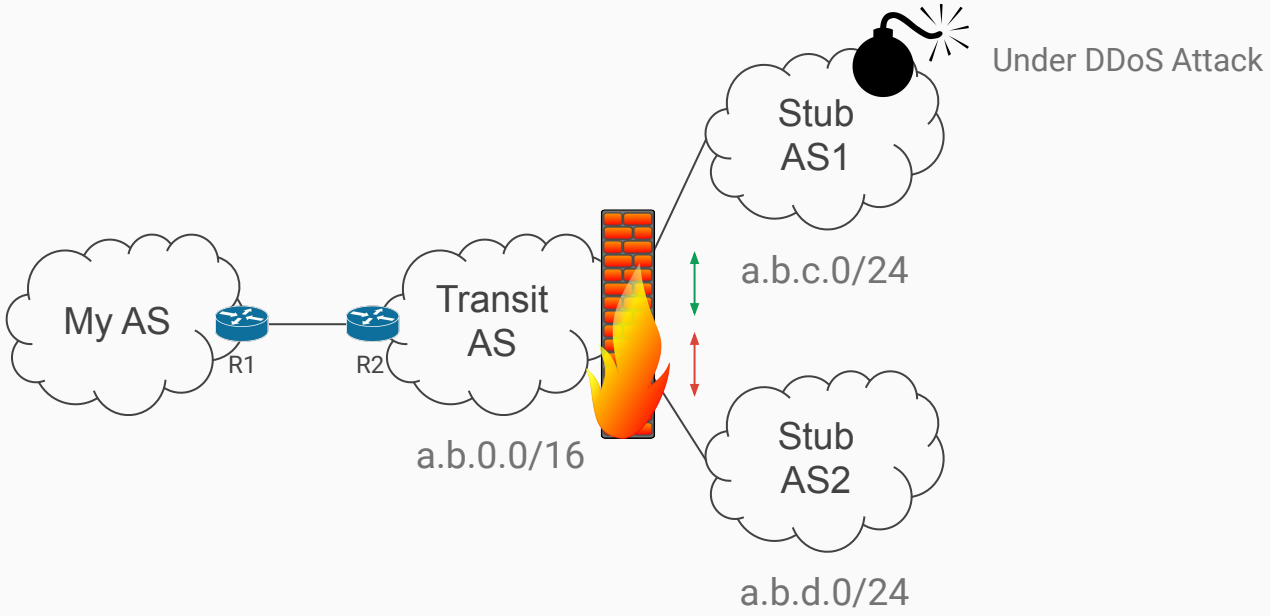
The lack of security mechanism in BGP



The lack of security mechanism in BGP



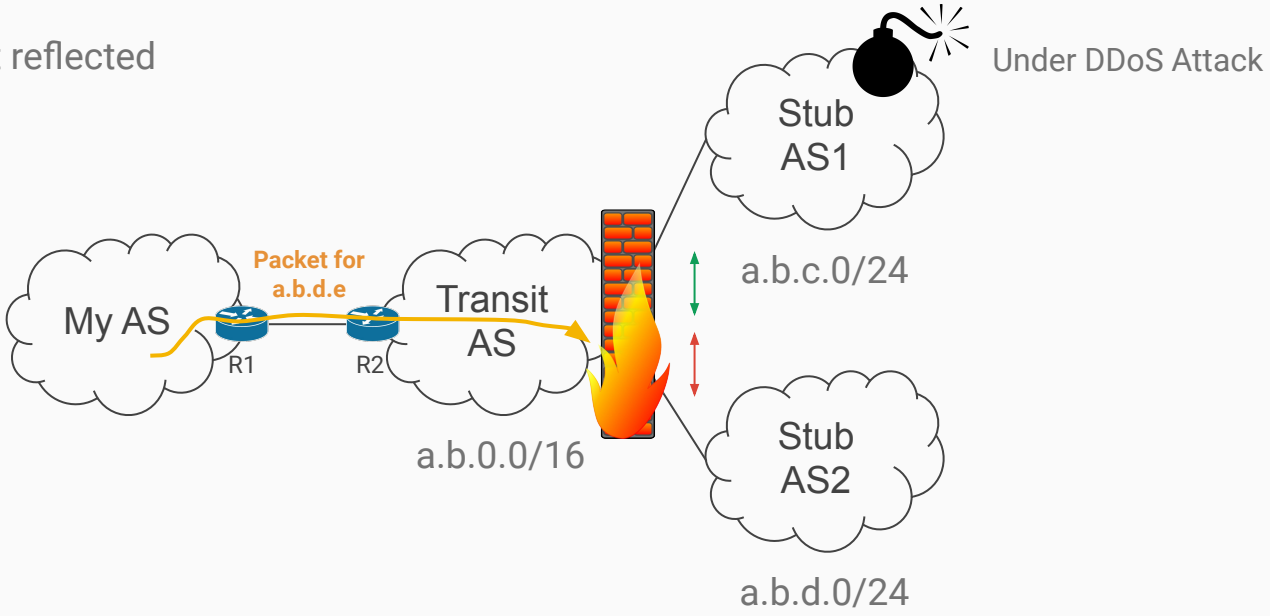
The lack of security mechanism in BGP



IP filter misconfigured !

The lack of security mechanism in BGP

The IP filter is not reflected
the control-plane



IP filter misconfigured !

Requirements to validate BGP paths

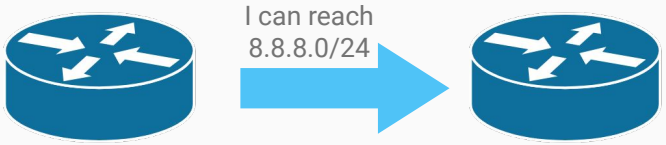
To be secure, the solution requires :

1. A new RPKI object
   - To find out which device is responsible for the secure handshake
2. TLS certificates
   - To authenticate the secure handshake
3. Modifications to BGP to support the validation extension
4. A service to answer to the secure ping

Requirements to validate BGP paths

1. A new RPKI object

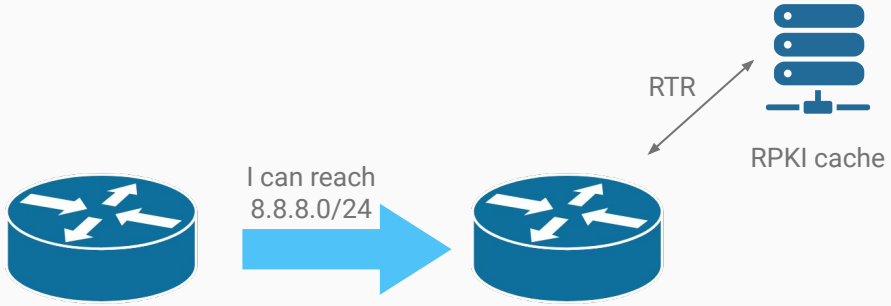
   To find out which device is responsible for the secure handshake.



Requirements to validate BGP paths

1. A new RPKI object

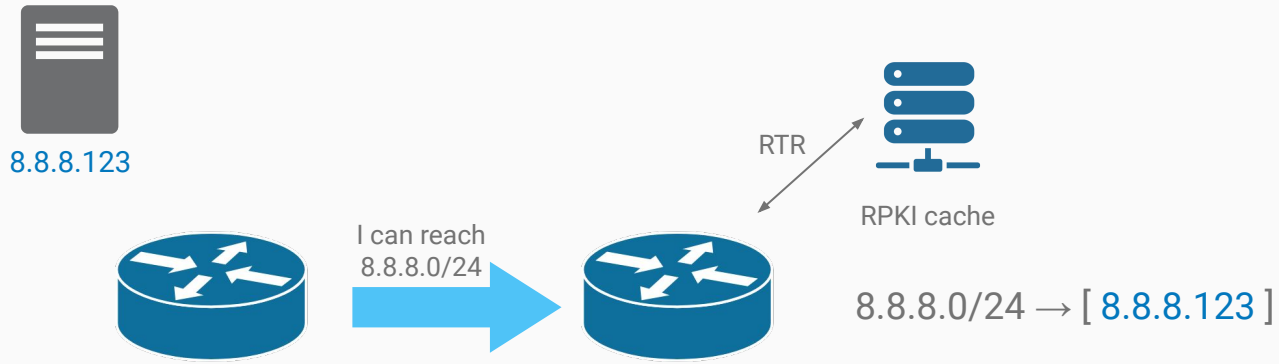
   To find out which device is responsible for the secure handshake.



Requirements to validate BGP paths

1. A new RPKI object

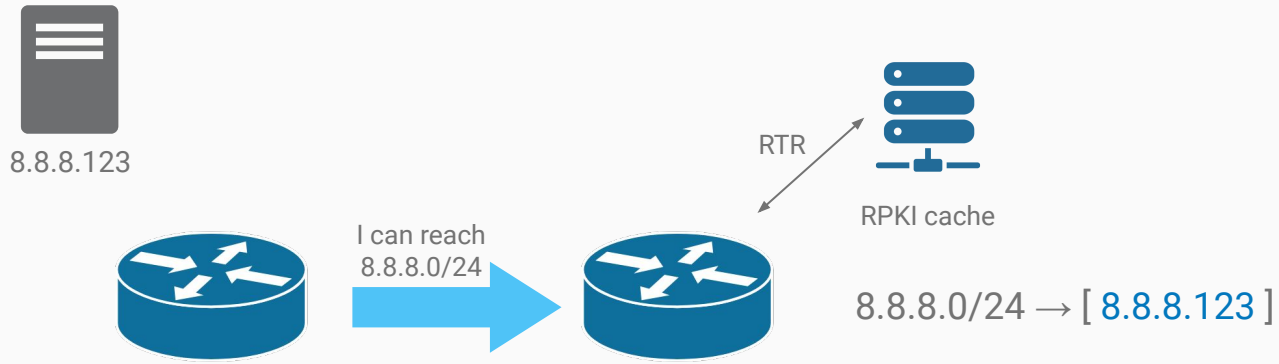
   To find out which device is responsible for the secure handshake.



Requirements to validate BGP paths

2. TLS Certificates

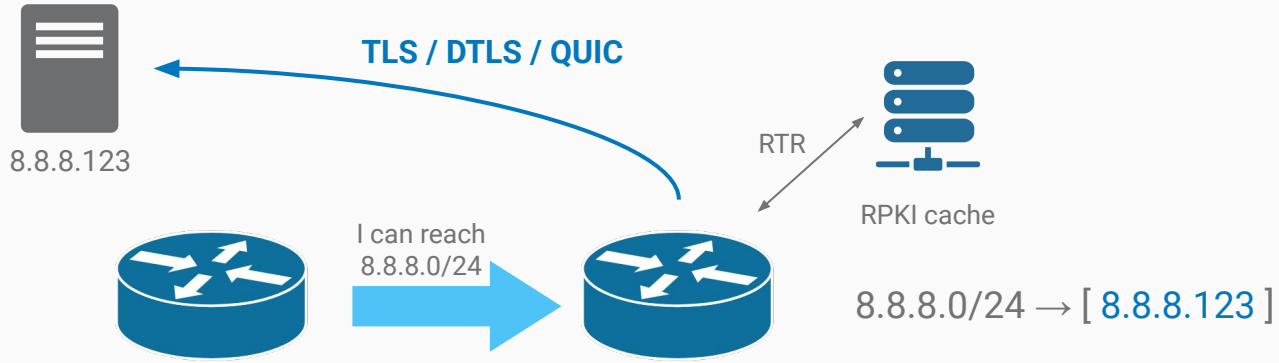
   To authenticate the secure handshake.



Requirements to validate BGP paths

2. TLS Certificates

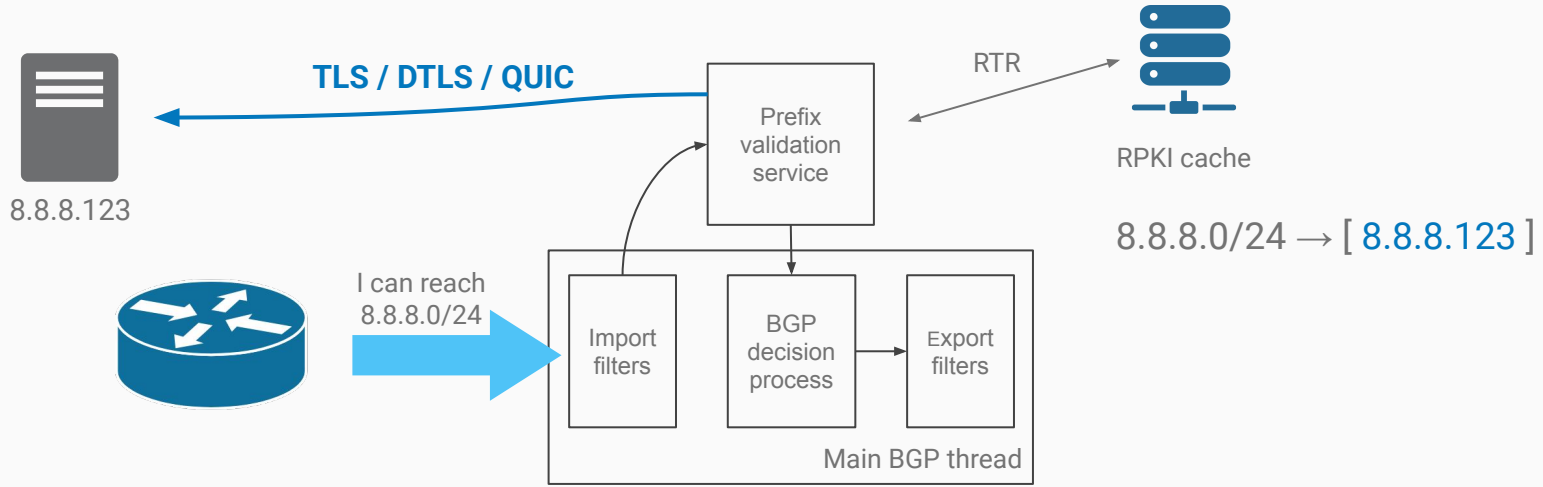
   To authenticate the secure handshake.



Requirements to validate BGP paths

3. Modification to BGP

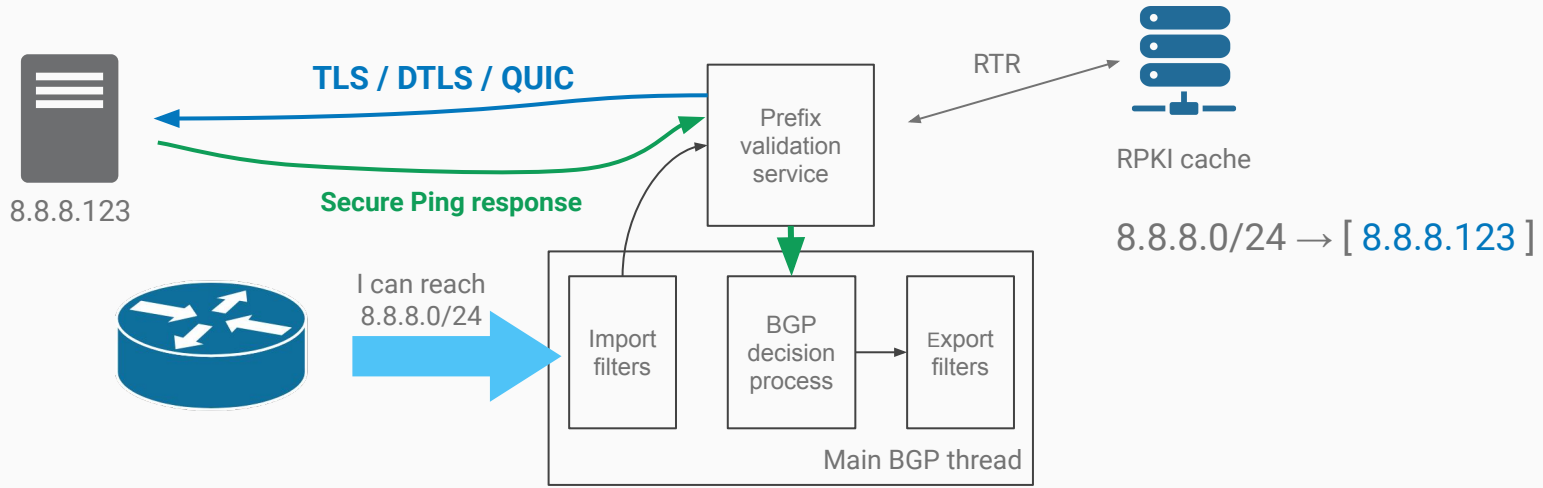
   Before importing it, the route must be validated



Requirements to validate BGP paths

3. Modification to BGP

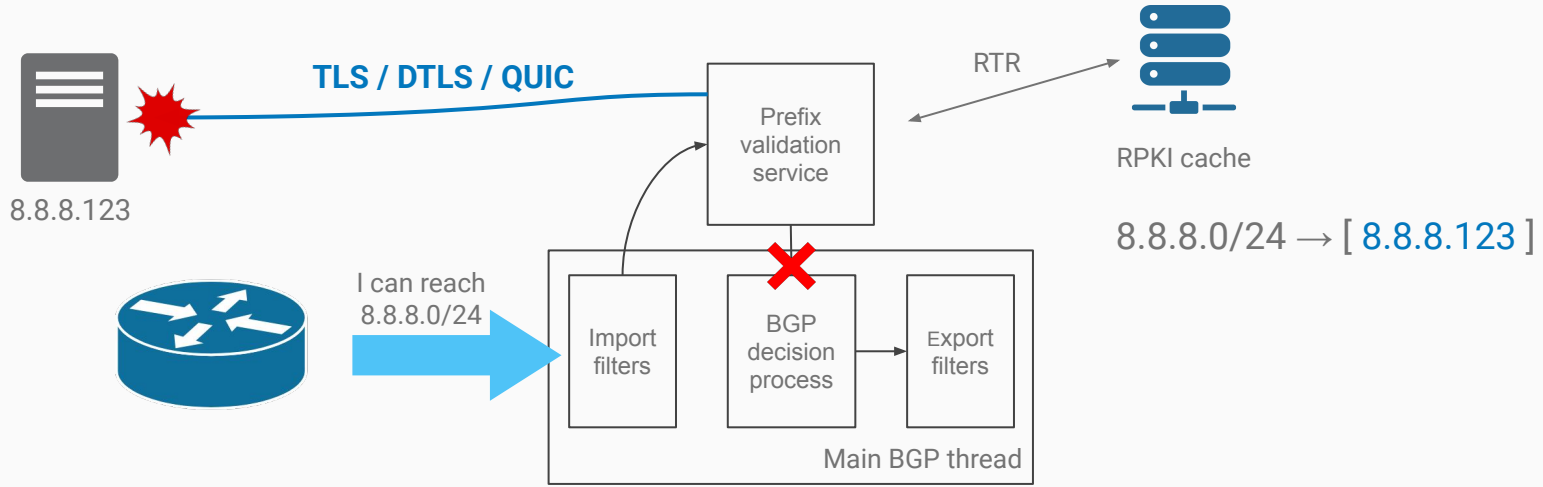
   Before importing it, the route must be validated



Requirements to validate BGP paths

3. Modification to BGP

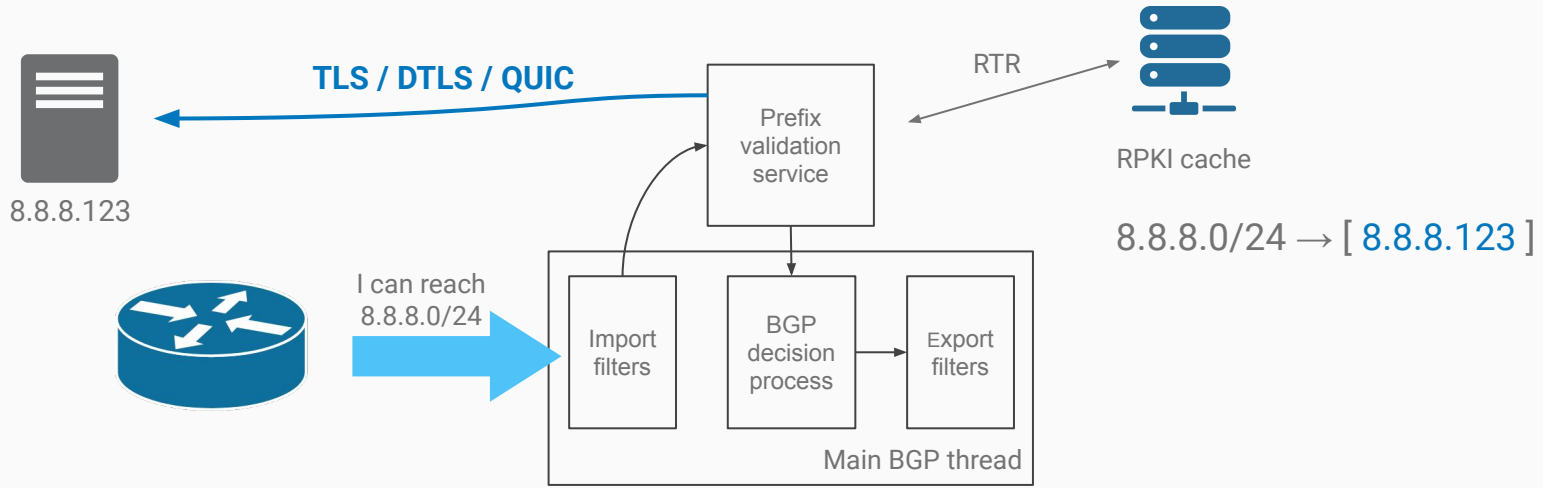
   Before importing it, the route must be validated



Requirements to validate BGP paths

4. The prefix validation service can be any device

   Either the router or an external device can be used



A first prototype

The first prototype is implemented with ~1.1k LoC in FRRouting v8.2

The validation system:

- Is implemented in BGP directly
- Supports ICMP Pings and TLS
- Uses community to tag route to be validated

https://github.com/twirtgen/frr/tree/stable/8.2-dataplane

Configuring path validation is done through CLI

The network operator can choose what to do with the path validation.

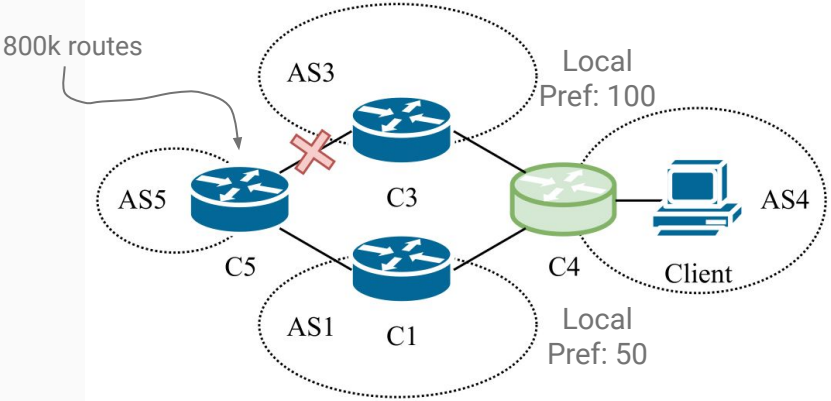
The CLI is flexible.

```
route-map path_validation permit 10
 match path-validation notrequested
!
route-map path_validation permit 20
 match path-validation pending
 set community additive no-export
!
route-map path_validation permit 30
 match path-validation valid
 set community additive 65021:6
!
route-map path_validation deny 40
```

Early Evaluation

800k routes originated from C5

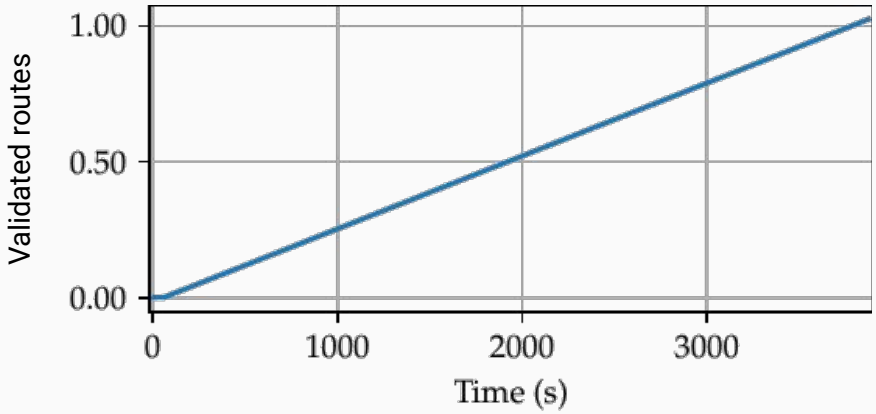
2% of the routes are tagged for validation check

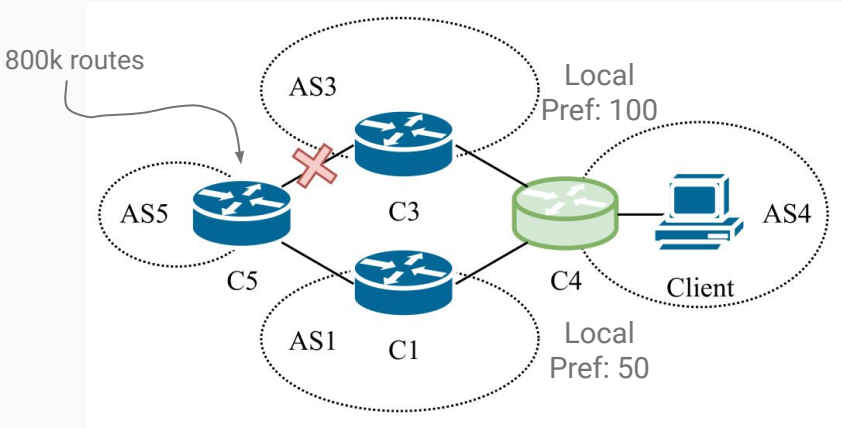


Early Evaluation

800k routes originated from C5

2% of the routes are tagged for validation check

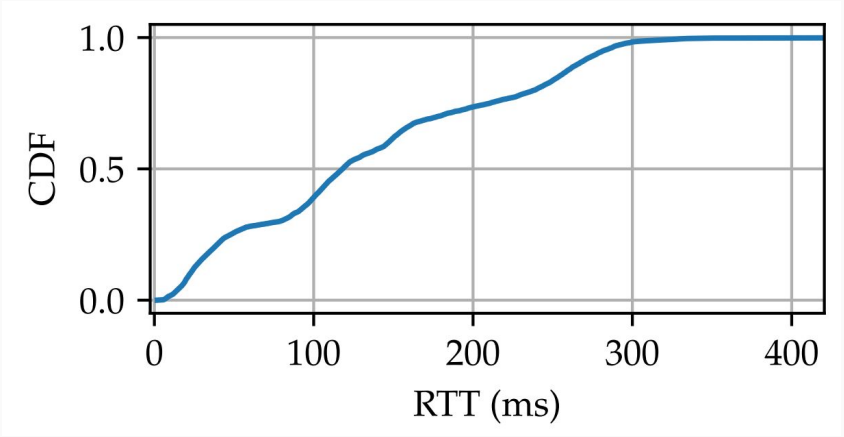




Early Evaluation (cont.)

Performing path validation takes time!

Even with a faster prototype, we are limited by the network!



RTT of 7k IPv4 destinations evenly distributed over the Internet

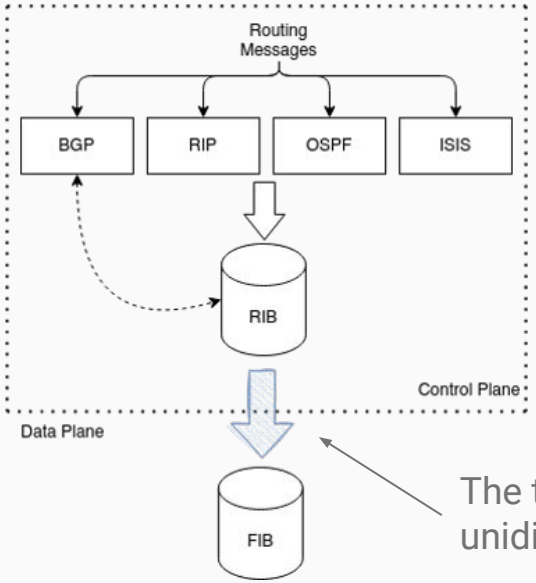
Improving BGP Path Validation

BGP Path Validation is still a WIP !

There is still a long way to go to achieve full validation in the data plane:

- Currently, the prototype **only checks** the path reachability.
- We are not sure that the path followed by packets is the one advertised by BGP
- There could be IP-tunnels between two malicious ASes (cf. wormhole attack)
- etc.

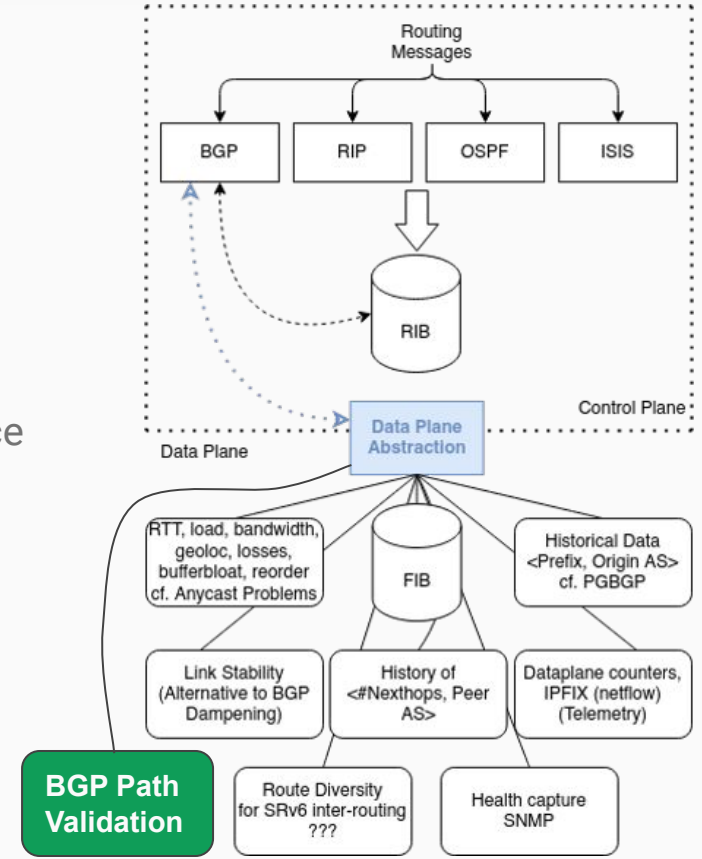
BGP Path Validation is the first step to merge control & data plane



Augment routing decision with dataplane intelligence

The traditional flow is unidirectional

Why not making it “bidirectional” ?



Conclusion: BGP Path Validation

thomas.wirtgen@uclouvain.be

BGP Path Validation complements the RPKI ROA validation

Querying the dataplane brings a lot of useful information to BGP

Make the control plane more aware of its environment

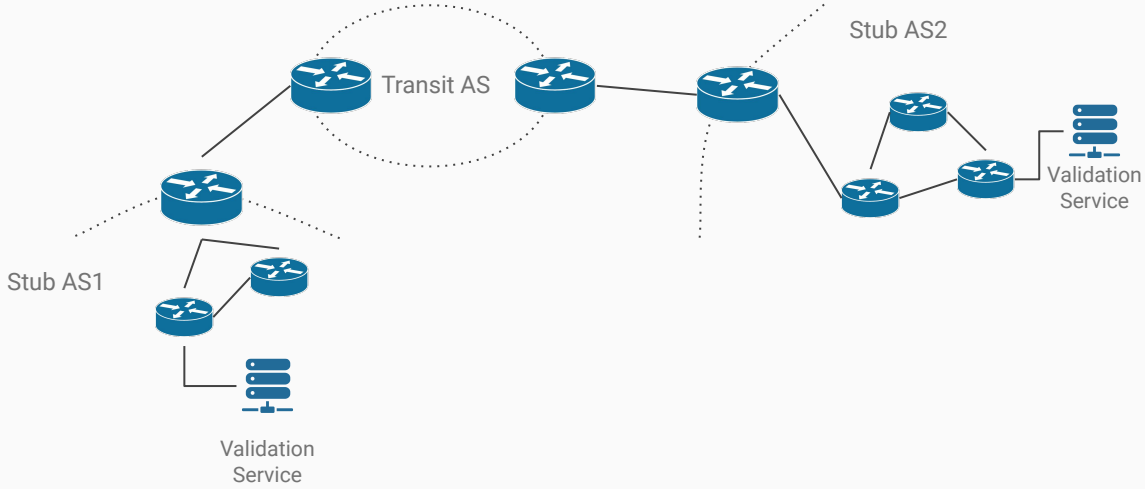
Future direction:

- Deploy and Experiment in a real environment
- Augmenting the BGP Decision process with dataplane intelligence
- Make BGP aware of the dataplane

Requirements to validate BGP paths

4. A service to answer to the secure ping

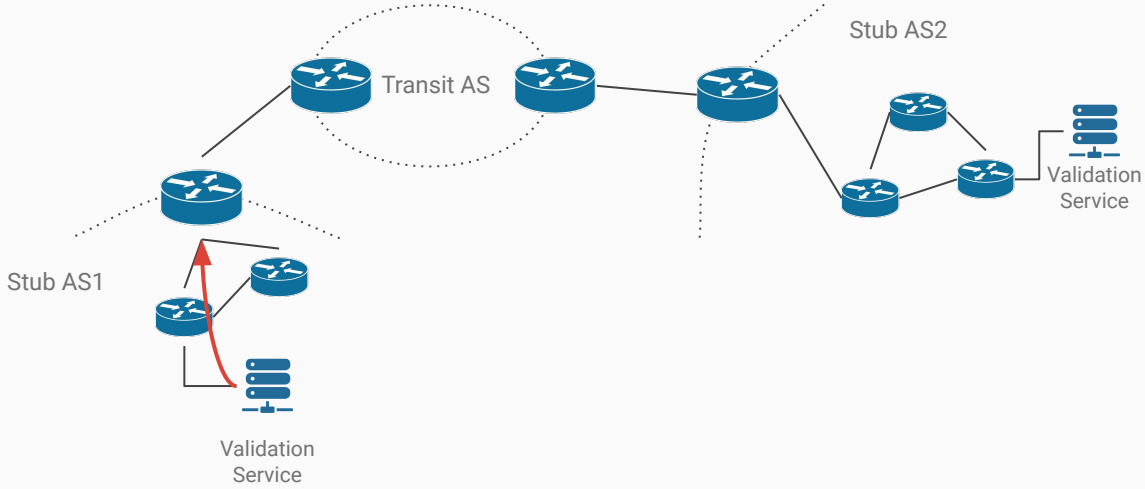
   The validation service can be either the router or an external device



Requirements to validate BGP paths

4. A service to answer to the secure ping

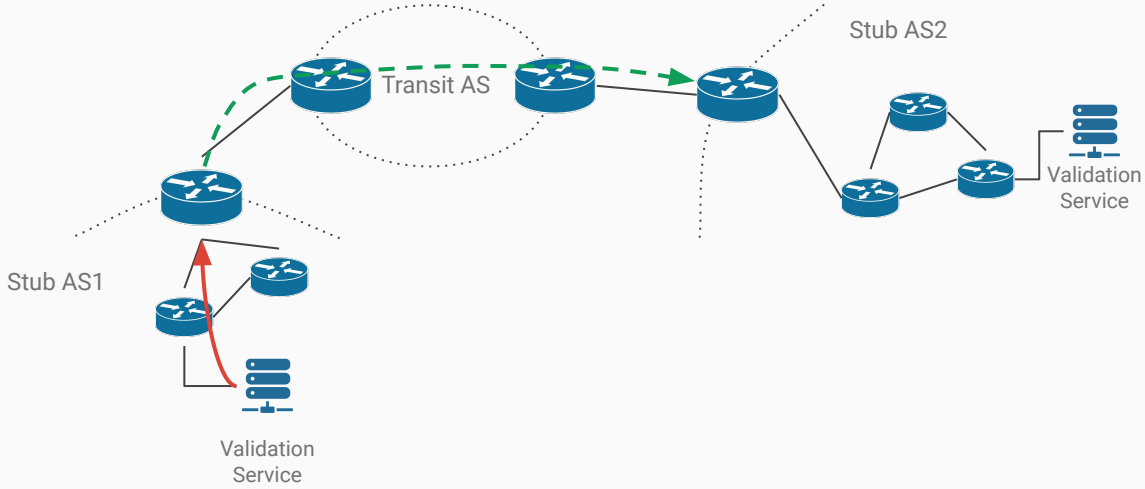
   The validation service can be either the router or an external device



Requirements to validate BGP paths

4. A service to answer to the secure ping

   The validation service can be either the router or an external device



Requirements to validate BGP paths

4. A service to answer to the secure ping

   The validation service can be either the router or an external device