RIPE NCC
RIPE NETWORK COORDINATION CENTER

Ups and downs

BGP Security

Sweet memories (a short recap)

Original BGPv4

Late 1980s – early 1990s

The internet was still very small
Complete trust each other

The main goal is to turn the global network into a self-organizing one (no any security in mind)

The Internet was split into autonomous systems, and the open BGP protocol was born

Since then…

BGPv4 is still here

This technology proved to be a great success

This protocol is still in use today, 30 years after it was created

However, we can no longer trust just anyone on the internet

The protocol as it was originally created does not meet current security and operational standards

Issue statement

Some definitions for incidents

Prefix hijacks and route leaks

Prefix hijack

Originating an announcement by an unauthorized autonomous system

Route leaks

The propagation of BGP announcements beyond their intended scope

Other attributes modification

Real incidents

Stats and root causes

UNIQUE ROUTE LEAKER ASes	Q1, 2026	UNIQUE BGP HIJACKER ASes
1,823	January	9,432
1,960	February	6,294
1,955	March	7,130

Data from https://qrator.net/blog/details/Q1-2026-DDoS-bad-bots-and-BGP-incidents-statistics-and-overview/

Real incidents

Stats and root causes

In average, it is an incident every 4.5 minutes

And most of them happened due to the human mistakes

Data from https://qrator.net/blog/details/Q1-2026-DDoS-bad-bots-and-BGP-incidents-statistics-and-overview/

And now for something completely different

Money talks

But BGP's second main goal is to help operators make money

For 30 years, BGP has been refining ways to improve
our buying and selling traffic

BGP = “Money translated to the routers’ language”
You can't talk about inter-operator BGP without thinking about business

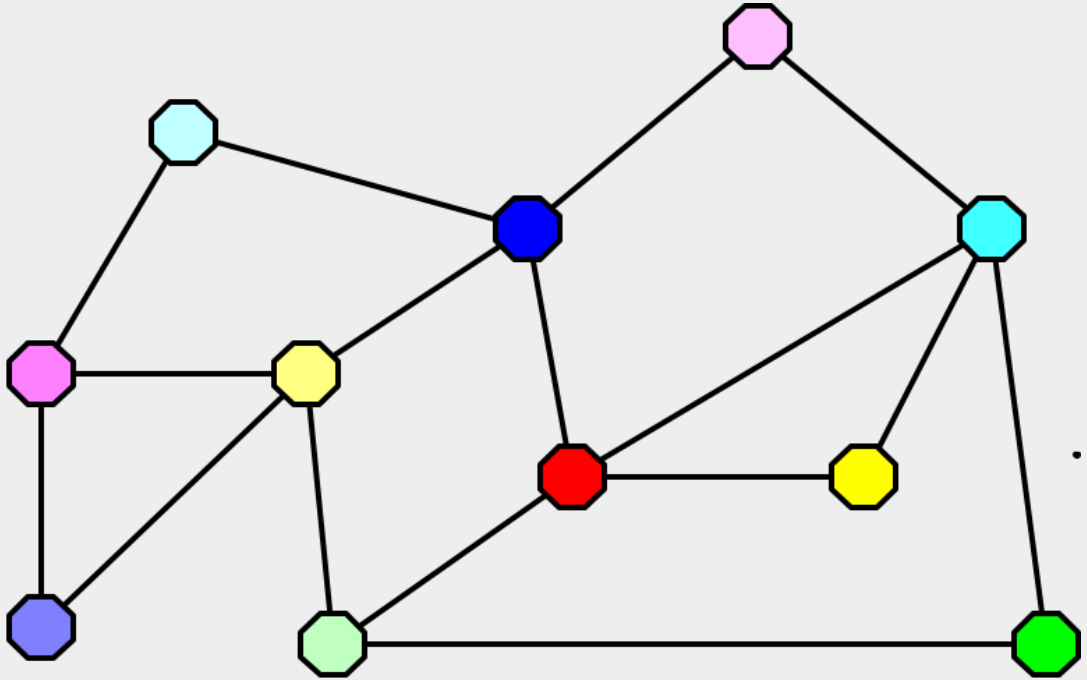
How did we start

Quite chaotic connections

Random traffic exchange

Complex interactions

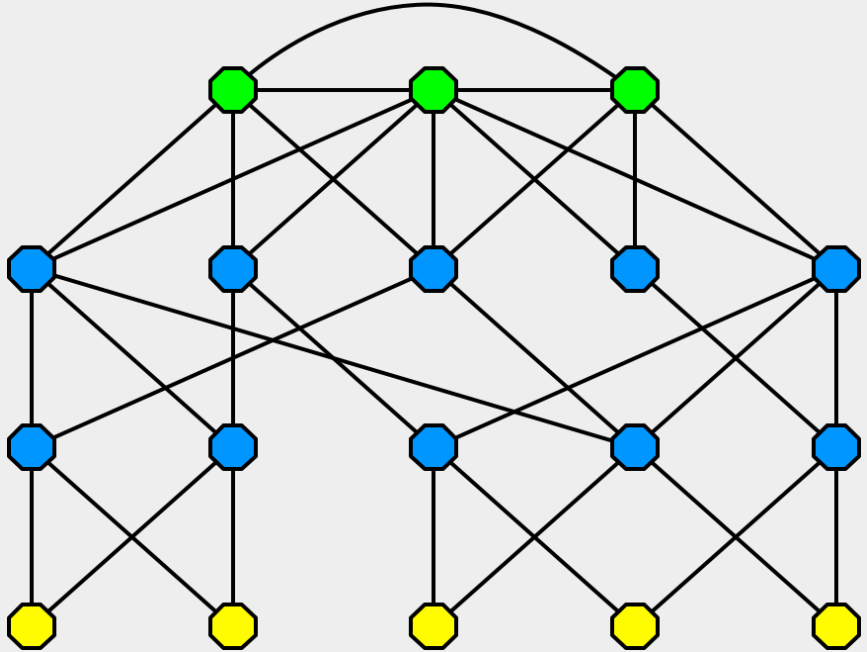
Often non-commercial



And where are we now?

The commercial hierarchy

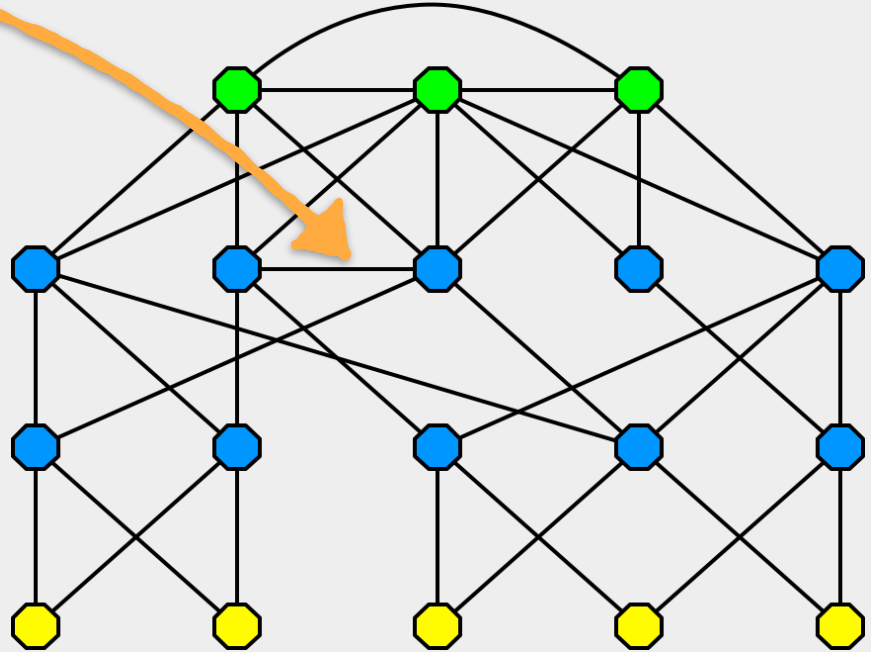
- **Operator tiers based on their business model**
  - **Tier 1: Do not pay anyone for traffic**
  - **Tier 2: Pay upstream providers and receive revenue from downstream operators**
  - **Tier 3: Pay upstream providers**



And where are we now?

Plus peering

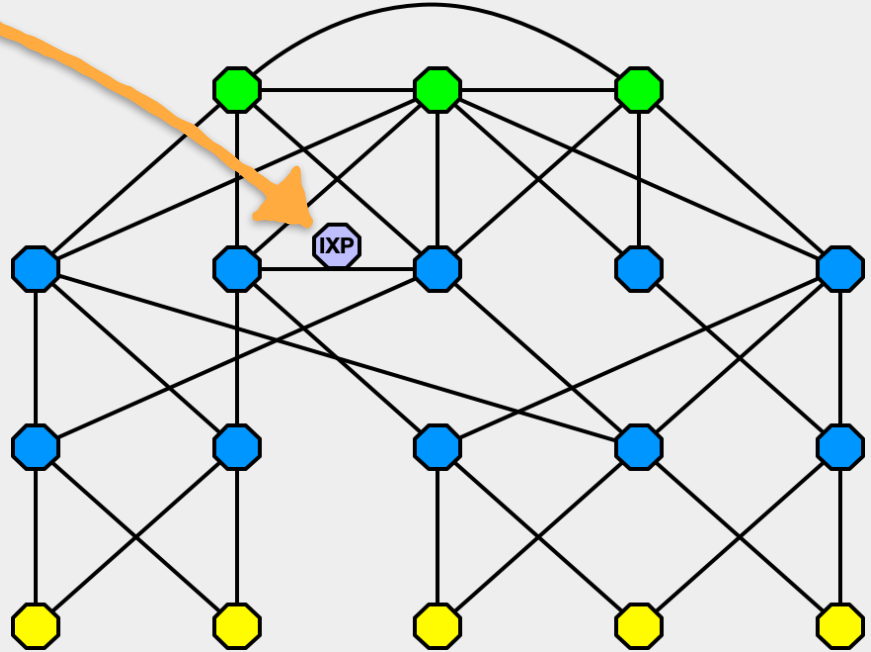
- **Peering: exchanging your own traffic and traffic from your clients cone**
- In fact, peering was already shown in this diagram
  - Between Tier 1 operators



And where are we now?

Plus IXP

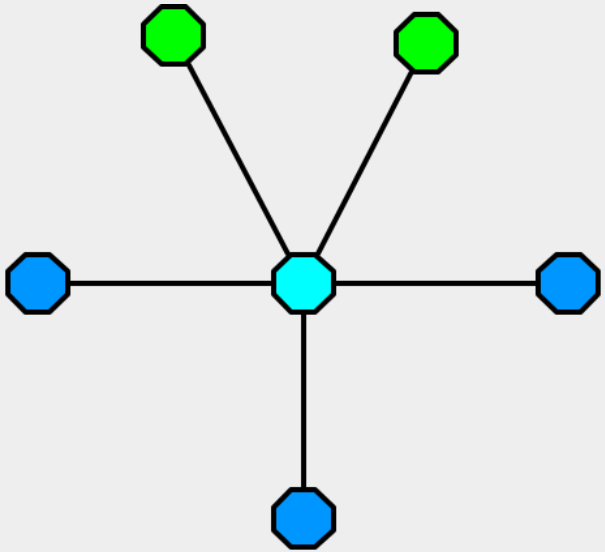
- Peering at scale: Internet Exchange Points (IXPs)
- Payment is typically not based on traffic volume
- IXPs have their own autonomous system, which is not visible in the AS PATH



Gao-Rexford World

How to propagate announcements?

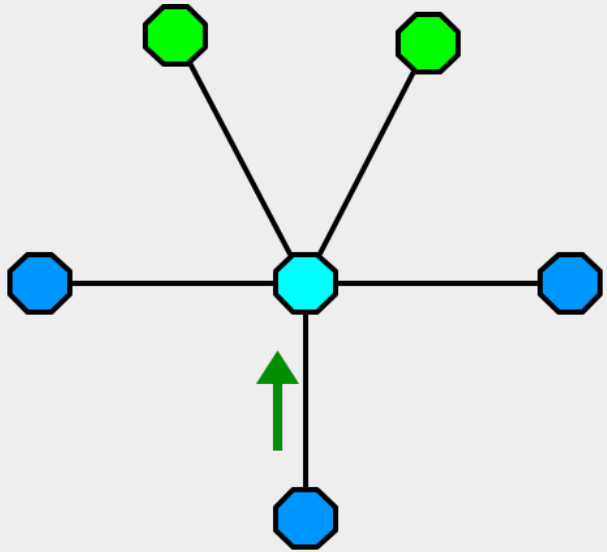
- We are in the center



Gao-Rexford World

From a downstream

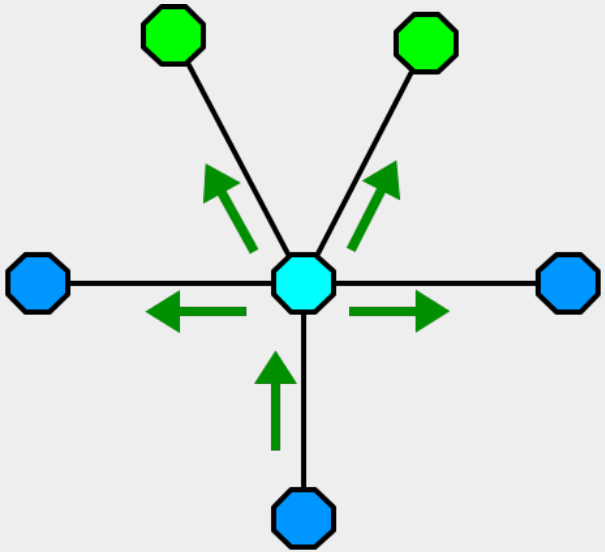
- **Announcement from our downstream (they pay us)**



Gao-Rexford World

From a downstream - to anyone else

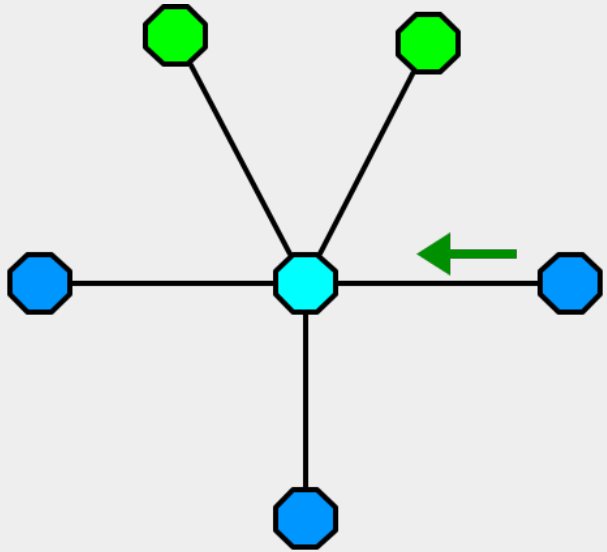
- **Announcement from our downstream (they pay us)**
- **Propagate it everywhere**



Gao-Rexford World

From a peer

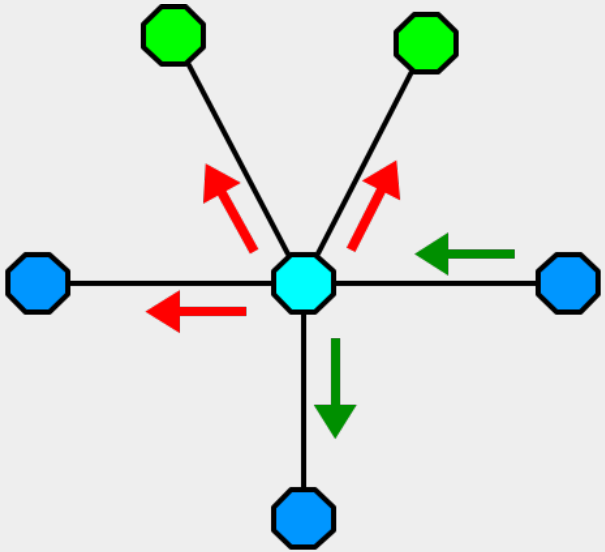
- **Announcement from our peer (they DON’T pay us)**



Gao-Rexford World

From a peer to downstreams only

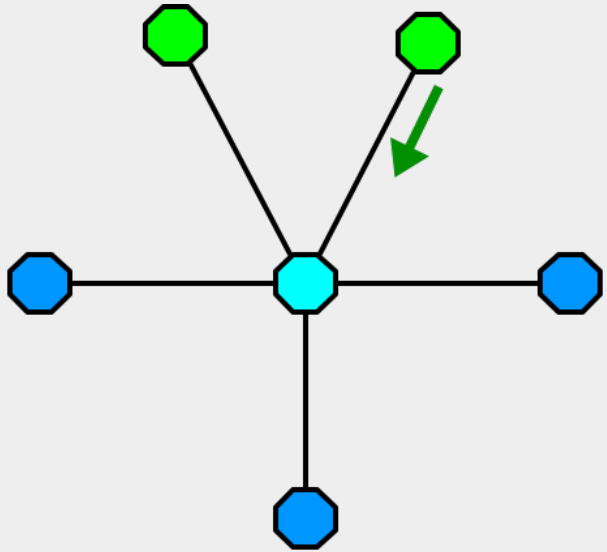
- **Announcement from our peer (they DON’T pay us)**
- **Propagate it only to our customers**



Gao-Rexford World

From an upstream

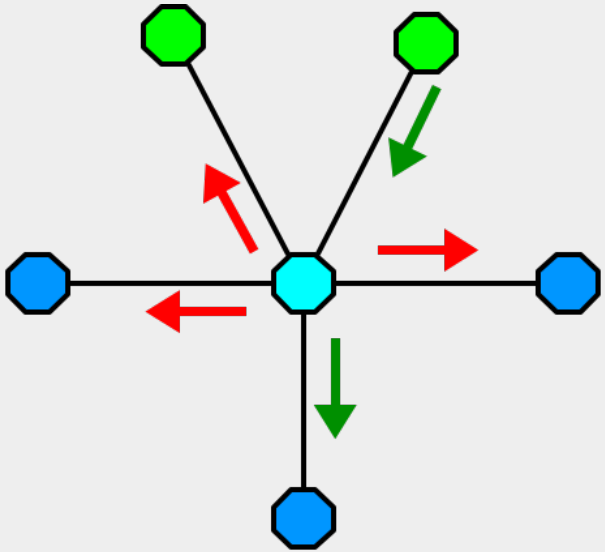
- **Announcement from our upstream (we pay them)**



Gao-Rexford World

From an upstream to downstreams only

- **Announcement from our upstream (we pay them)**
- **Propagate it only to our customers**



Gao-Rexford World

Long story short

Announcements coming from below are propagated everywhere

All other announcements are propagated only downward

But the original BGP had absolutely no concept of “up” or “down”

Are we doomed?

No, we are not

Technologies aren't set in stone

For decades, the industry has been developing solutions within the IETF

Many of them proved unsuccessful and remained on paper

But not all of them!

Ways to improve the situation

Principles to remember

Sources of trust external to BGP are required

Business relationships should be taken into account

Deployment will be gradual
Interoperability with old realisations is a must

A framework

Not a single mechanism, but
an *extensible* and *centralized* framework

New “bricks” can be added
Now we have two: ROA and ASPA

Completely external to BGP

No new attributes or NLRI types

Authorisation is built-in and cannot be bypassed

Resource Private Keys Infrastructure (RPKI)

Two sides of the same coin

Ties entities cryptographically
E.g., an IP prefix and it's originating ASN

Relies on chains of trust
With trust anchors in RIRs

So there are two parts
one side is responsible for creating signed "statements" (**signing**),
and the other is responsible for using them with BGP (**validating**)

BGP Roles

A tidy home comes first

BGP sessions are categorised *locally*
Setting up a local session type is a source of trust

The announcement from peers and upstreams should only go down

New BGP attribute (called OTC)

A silver bullet?

BGPsec_PATH instead of AS PATH

BGPsec Router Certificates (from RPKI repositories)

Chained signing in BGPsec_PATH

Unified verification for both Origin and Transit

(old good)
RPKI ROA

Route Origin Authorisation in RPKI (RPKI ROA)

Fighting prefix hijacks

A popular technology that has been widely adopted around the world

A cryptographic binding is created **between an IP prefix and the autonomous system** authorized to originate traffic from that prefix

This binding is called a ROA; once created, it is published in a public repository (**signing**)

Validating networks download all ROAs, filter out the faulty ones, and use remaining to match origins of incoming BGP announcements

Invalid announcements are discarded

Route Origin Authorisation in RPKI (RPKI ROA)

Where to find out more

Our training courses

- Deploying RPKI Webinar
- Introduction to RPKI Webinar
- BGP Routing Security Training Course (face-to-face, 1 day)

Self-paced learning: RIPE Academy

- Microlearning course: Why RPKI?
  https://academy.ripe.net/mod/scorm/player.php?a=110&currentorg=articulate_rise&scoid=220
- Microlearning course: What is RPKI?
  https://academy.ripe.net/mod/scorm/player.php?a=116&currentorg=articulate_rise&scoid=232
- Full e-Learning course: BGP Security
  https://academy.ripe.net/course/view.php?id=15

BGP Roles

BGP Roles

“Let's color this page”

- For each session we are specifying **the role from our side**:
  - customer
  - provider
  - peer
  - RS
  - RS-client

- Our role should **match the role of our neighbour**

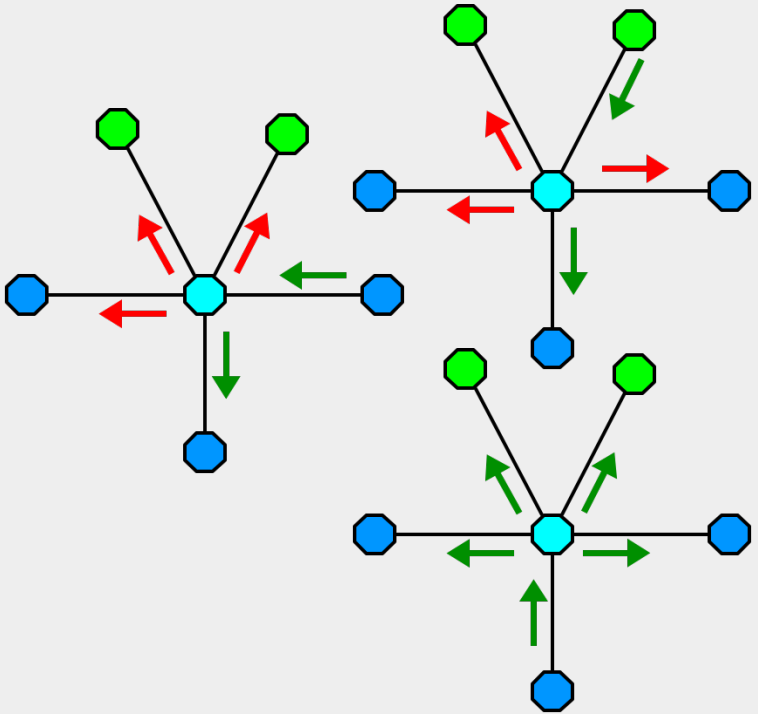
- When an announcement is first sent downward or to the side, the AS should add the **OTC (Only-To-Customer) attribute** with its ASN as the value
  - Transitive optional
  - Attribute Type Code 35

- An announcement not from customers (especially **with the OTC** attribute) can only be sent **via sessions with the local “provider” role**

BGP Roles

A familiar mountain landscape

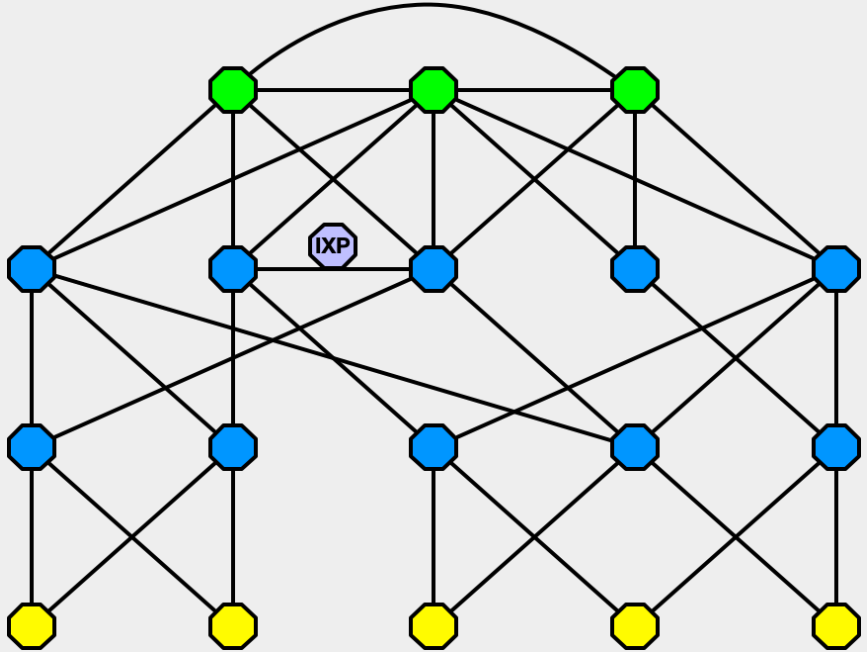
- **Without the OTC attribute**
  - **Each node just follows Gao-Rexford rules locally**



BGP Roles

A familiar mountain landscape

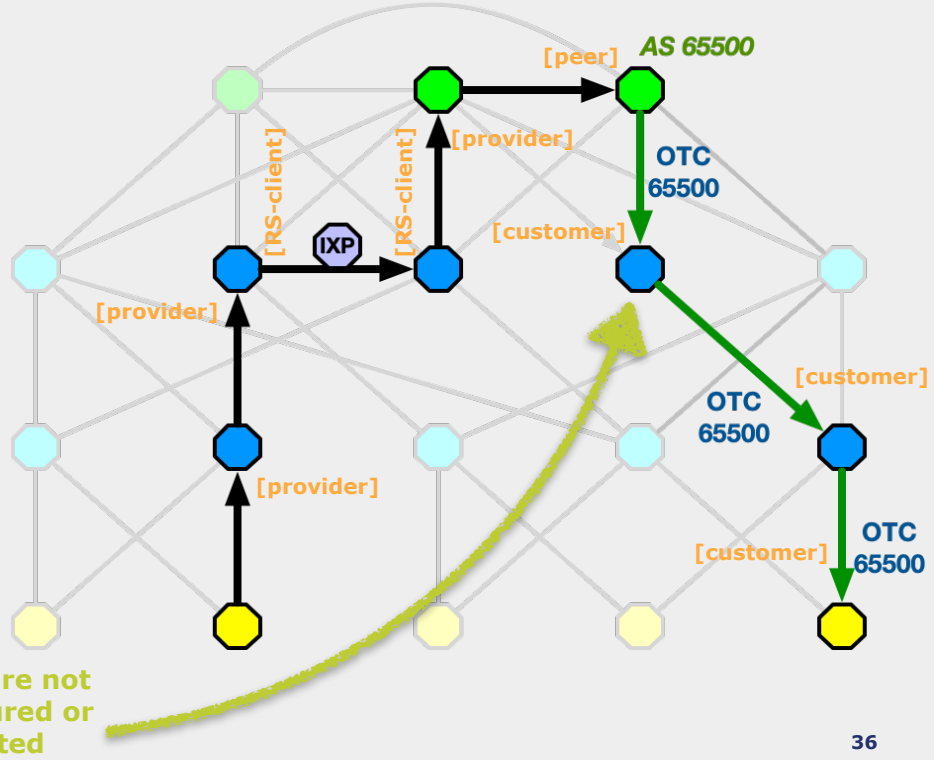
- **Using the OTC attribute**



BGP Roles

A familiar mountain landscape

- Using the OTC attribute
  - It doesn't matter how we climb
  - But we only make it down to the sessions with clients
  - It is transitive so if BGP Roles are not supported on some step, the logic can be restored after them



BGP Roles

Who is supporting?

Routing Software

BIRD
FRRouting
OpenBGPD
VyOS

Hardware

Juniper
Huawei
MikroTik (partially, no OTC support)

RFC 9234 - ask your manufacturer!

RPKI ASPA

Autonomous System Provider Authorization (RPKI ASPA)

General principles

A cryptographic binding **between this and upstreaming ASes:**
Each AS registers it's upstream ASNs in RPKI
Business relationships now are stored in the centralized way

This binding is called a **ASPA**; once created, it is published in a public repository (**signing part**)

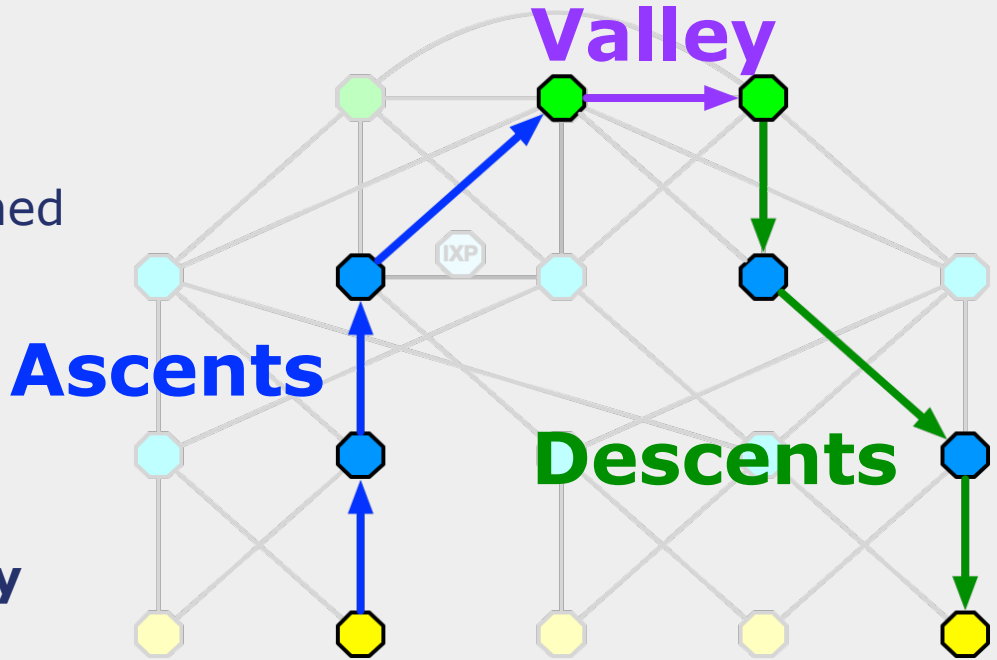
Validating networks download all ASPAs, filter out the faulty ones, and use remaining to match AS PATH in incoming BGP announcements

Autonomous System Provider Authorization (RPKI ASPA)

ASPA matching: no valleys in mountains of routing

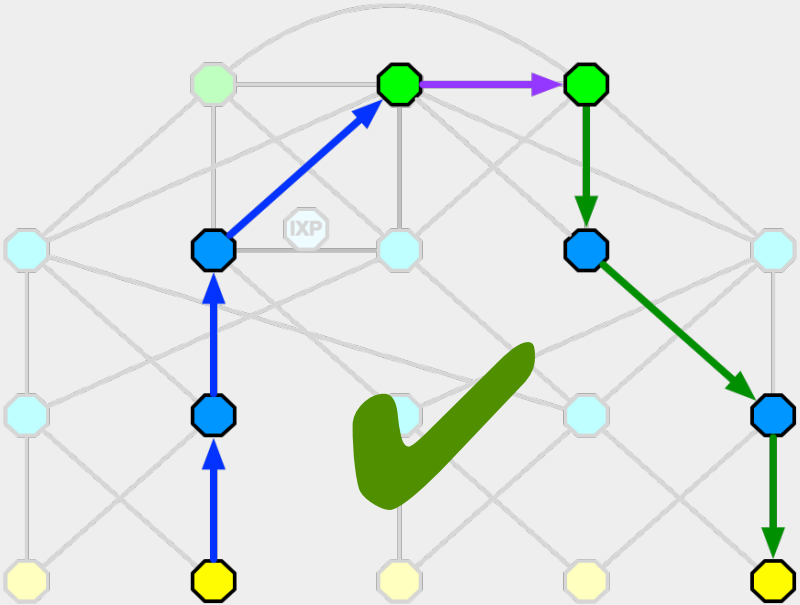
- **Ascent:** the **c ➤ p** segment
  Descent: the **p ➤ c** segment
  Valley: segment without defined relationship between ASes

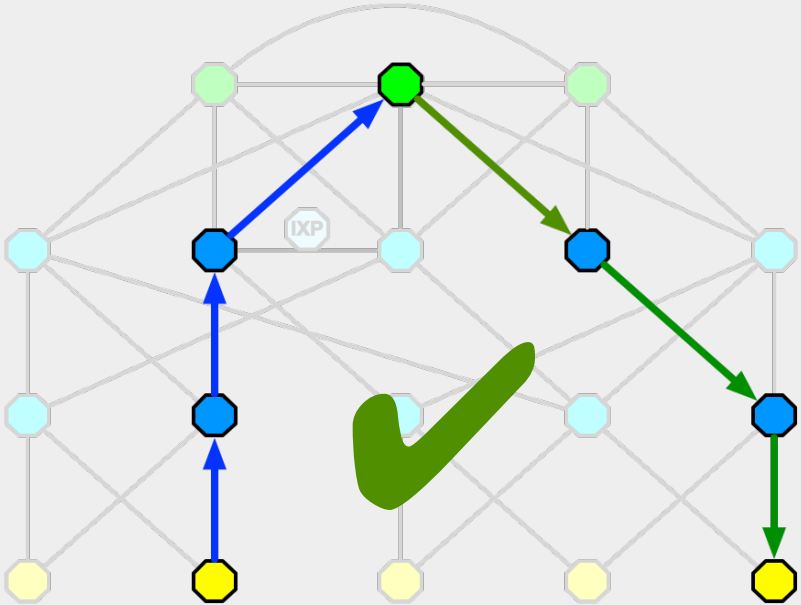
- **The AS PATH:**
  - **only ascents first**
  - **only descents after**
  - **not more than one valley in between**



Autonomous System Provider Authorization (RPKI ASPA)

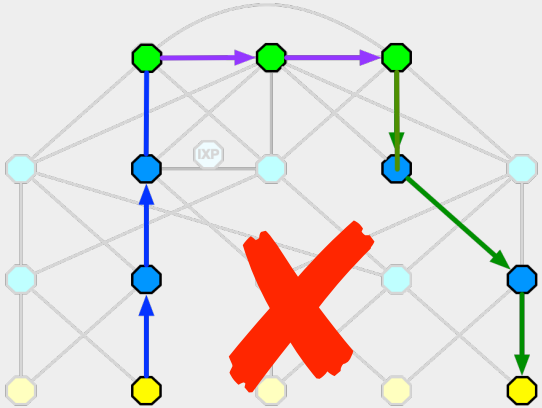
It’s easier to show: what is good

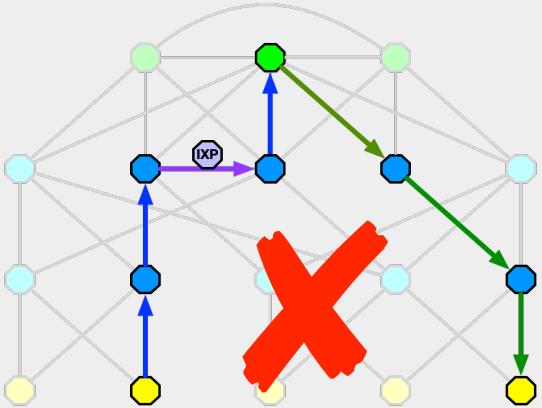


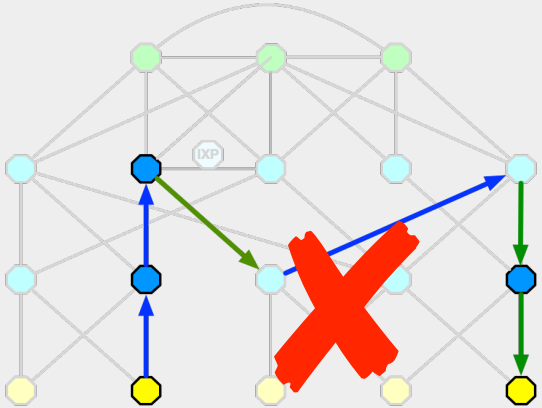


Autonomous System Provider Authorization (RPKI ASPA)

It’s easier to show: what is bad







Autonomous System Provider Authorization (RPKI ASPA)

Who is supporting?

RIR Repositories
Production: RIPE NCC, ARIN
Planned: APNIC, LACNIC, AfriNIC

Who validates it
RIPE NCC
Cloudflare
Probably Hurricane Electric
Maybe Cogent

Validators
Routinator
FORT Validator
rpki-client

Software routers
OpenBGPD
NIST BGP-SRx

Hardware routers
None at the moment

BGP Roles and ASPA: what can go wrong?

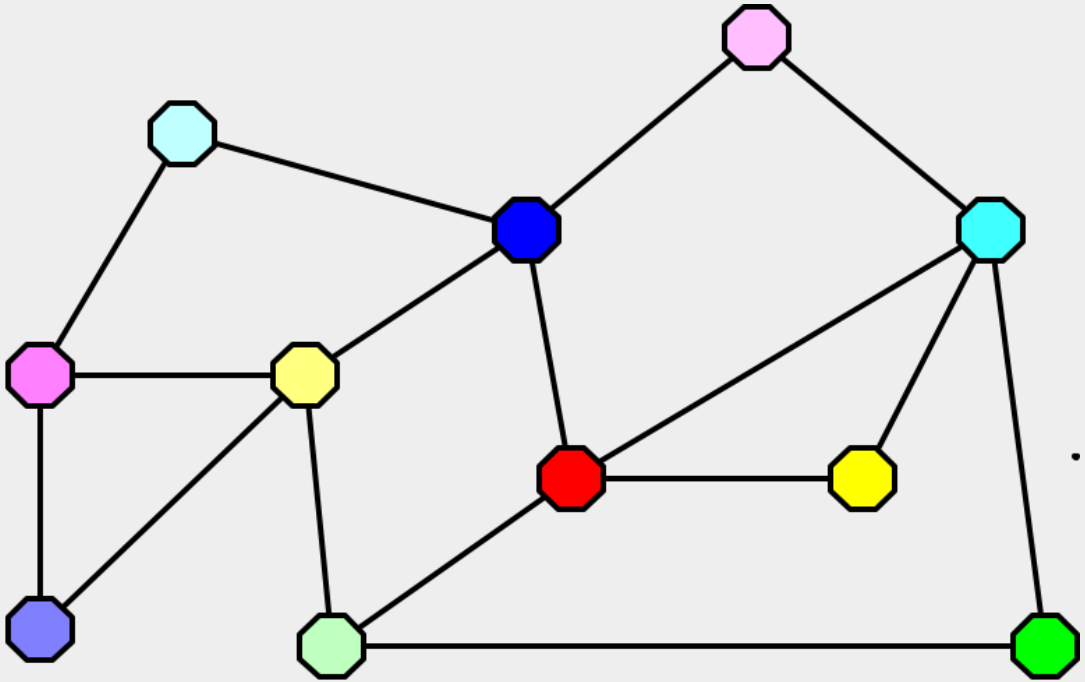
Partial control

BGP Roles
Control only over the descent

ASPA
It is difficult to judge the announcement
when only part of the AS path is covered
(“is a valley or a missing c ➤ p ASPA record?”)

Couple steps back (slides 9 and 10)

BGP = “Money translated to the routers’ language”



Complex scenarios

“You scratch my back, I'll scratch yours”?

Operators may have different roles:

- For different types of traffic
  (“you’re my upstream provider over IPv4, and I’m yours over IPv6”)
- For different regions
  (“I provide you with traffic in Asia, and you provide me with it in Europe”)

BGP Roles

- Can be solved with multiple BGP sessions

ASPA

- Everything is tougher, we need different ASNs and some additional BGP engineering

BGPSEC

BGPSEC

New attribute

AS_PATH is no longer mandatory: BGPsec_PATH is used instead
They cannot be used together

Either BGPsec_PATH or AS_PATH should present

BGPsec_PATH is not transitive
If a next peer does not support BGPsec_PATH,
it MUST be converted to AS_PATH

BGPsec_PATH consists of two chains
Secure_Path: equivalent to AS_PATH
Signature_Block: signature sequence for Secure_Path segments

Signing: blockchain technologies in the world of routing

Each routers signs the whole Secure_Path and the previous Signature_Block

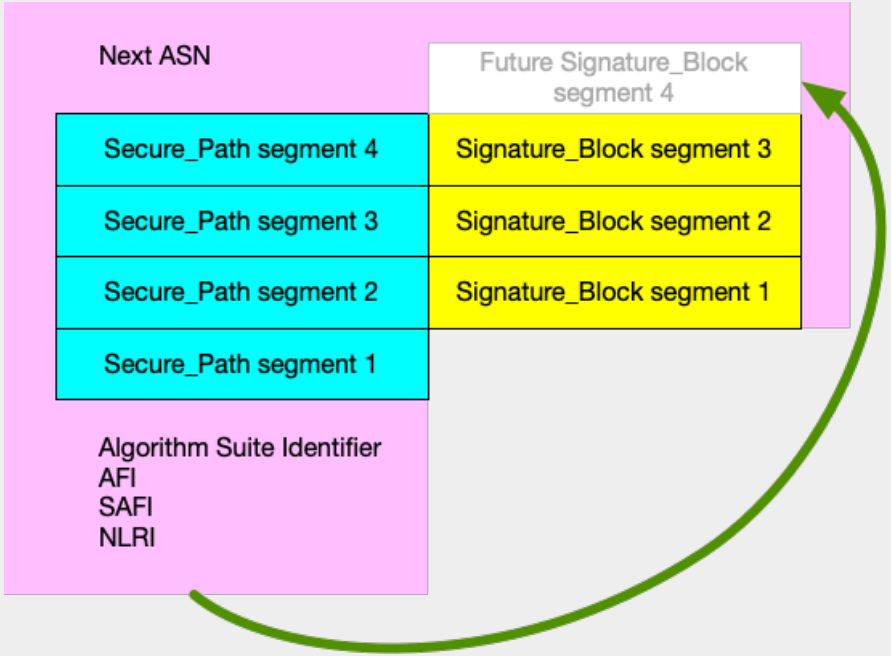
- use all signatures from the previous step in the new signature generation process

On the validation stage we check all signatures in the reverse order

BGPsec Router Certificates are used to verify signatures

- published RPKI repositories

Graphically



NLRI is used on each step

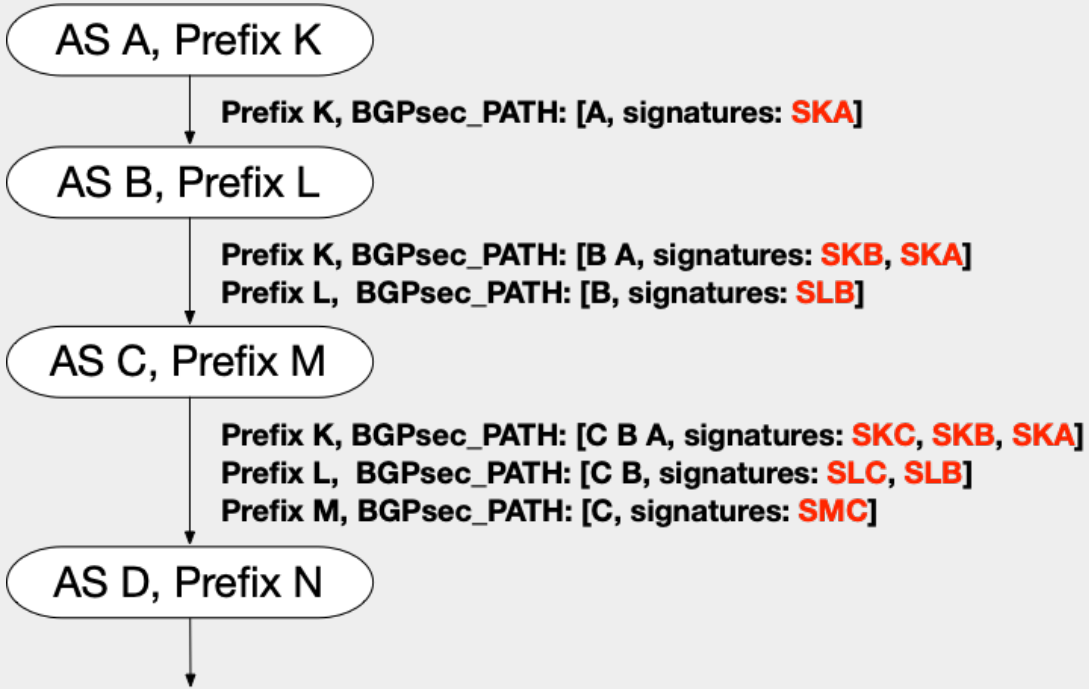
All previous signatures are used on each step

Not too much to cache

Cryptographic operations cannot be performed in advance

Validation

- All cryptographic checks must be performed **between** the receipt of the announcement and its processing
- As the network grows, the number of expensive operations increases **nonlinearly**



Surprise!

Have you seen how business relationships are described in BGPSEC?

Surprise!

Have you seen how business relationships are described in BGPSEC?

No, because they aren't described there at all

In its current form, it won't help with route leaks at all

Issues

A way too expensive computationally

For it to really work, 100% adoption is required

It doesn't solve every problem
Security is top-notch, but
operational errors (route leaks) aren't detected

Conclusions

Conslusions

There is no silver bullet

But there is a lot that can and should be done right now

You need to wash your hands, brush your teeth, and use routing security mechanisms

Don't accumulate technical debt

RIPE NCC
RIPE NETWORK COORDINATION CENTER

Questions?
Comments?
Applauses?

asemenyaka@ripe.net