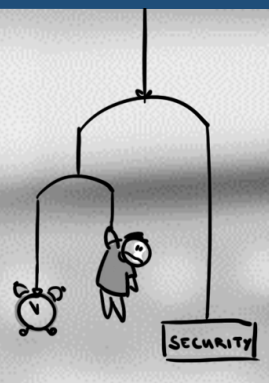
Revisiting BCP194



Picking the Worms Out of the Routing Can

Tobias Fiebig
Max-Planck Institut für Informatik

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Imagine a Perfect Internet

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Photo by: John Towner on Unsplash: https://unsplash.com/photos/people-on-top-of-hill-under-white-clouds-golden-hour-photography-CakC6u4d95g

Imagine a Perfect Internet

- Everyone filters in/out routes
- BGP speakers are secured
- There are no route leaks

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Imagine a Perfect Internet

- Everyone filters in/out routes
- BGP speakers are secured
- There are no route leaks
- (And only one AFI to worry about)

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

As we are not there, there is BCP194

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Photo by: John Towner on Unsplash: https://unsplash.com/photos/people-on-top-of-hill-under-white-clouds-golden-hour-photography-CakC6u4d95g

BCP194 / RFC7454: BGP Ops. & Security

- Published Feb 2015
- Recommendations for securing (e)BGP:
  - BGP Speaker
  - BGP Session
  - Route im/export and filters
- Common ground / BCP / 'your network your rules'
- Overall *very* reasonable recommendations
- But there are some issues…

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Some worms…

"[…] any IXP member SHOULD make sure it has a route for the IXP LAN prefix […] and that it announces the IXP LAN prefix […] to its downstreams."

"The easiest way to implement this is for the IXP itself to take care of the origination of its prefix and advertise it to all IXP members through a BGP peering."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Some worms…

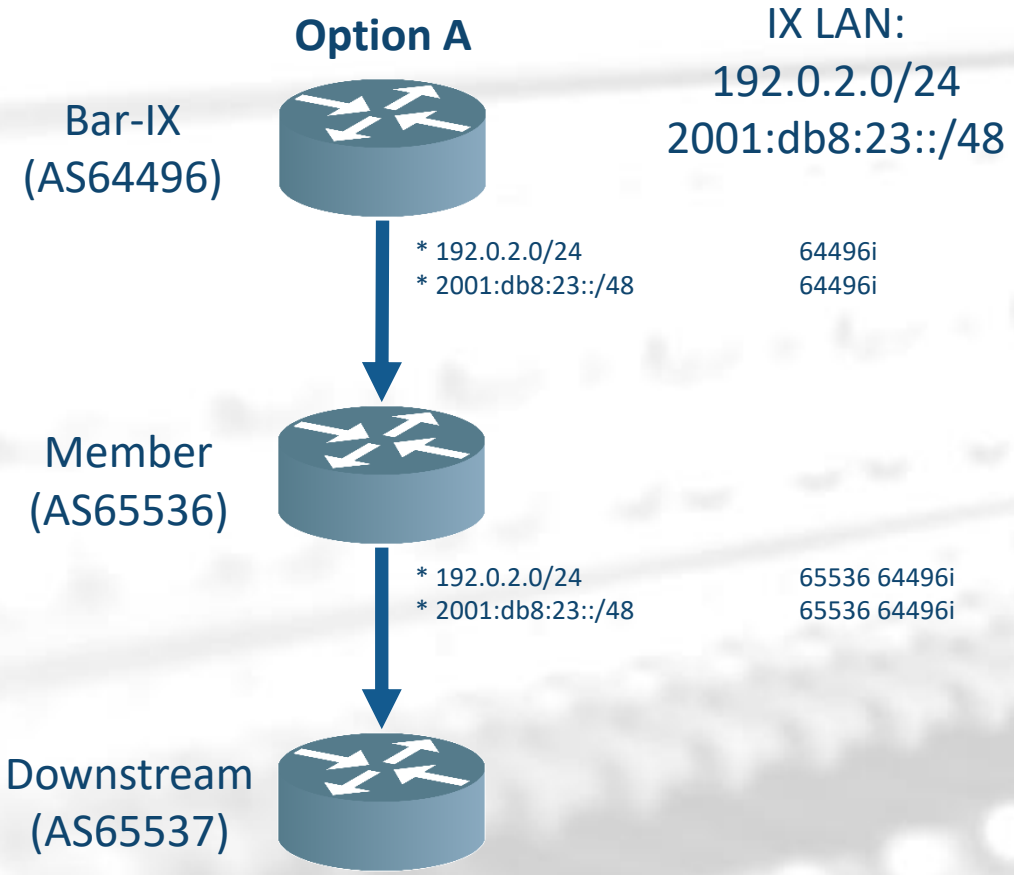
"[…] any IXP member SHOULD make sure it has a route for the IXP LAN prefix […] and that it announces the IXP LAN prefix […] to its downstreams."

"The easiest way to implement this is for the IXP itself to take care of the origination of its prefix and advertise it to all IXP members through a BGP peering."

" Tier 1 transit provider: an IP transit provider that can reach any network on the Internet without purchasing transit services."

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

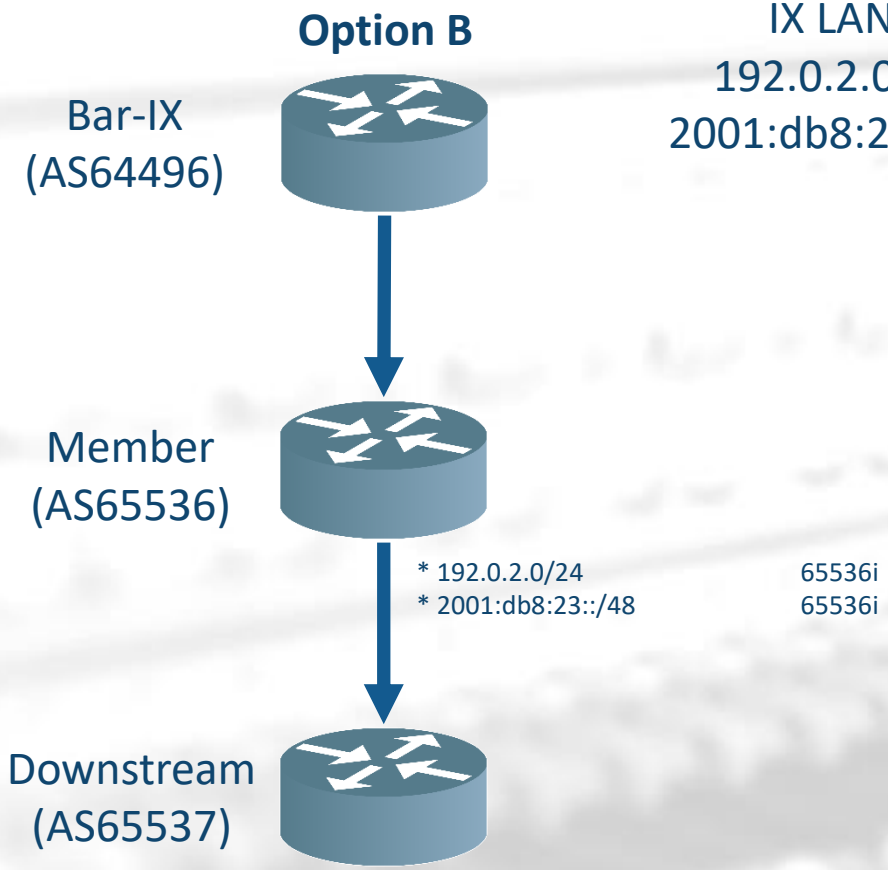
Implications (i)



- Implications
  - The IX will not do this if they do not want to

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

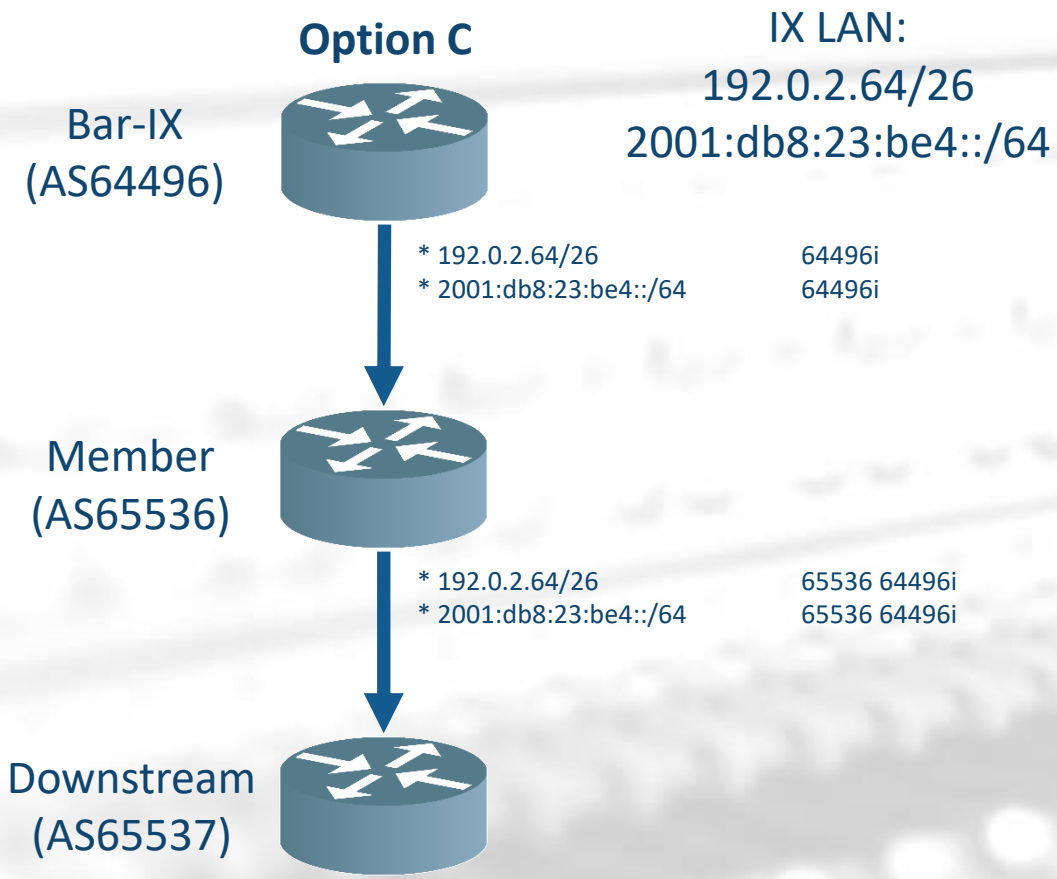
Implications (ii)



- Implications
  - The IX's NOC will probably have a 'small discussion' with AS65536

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

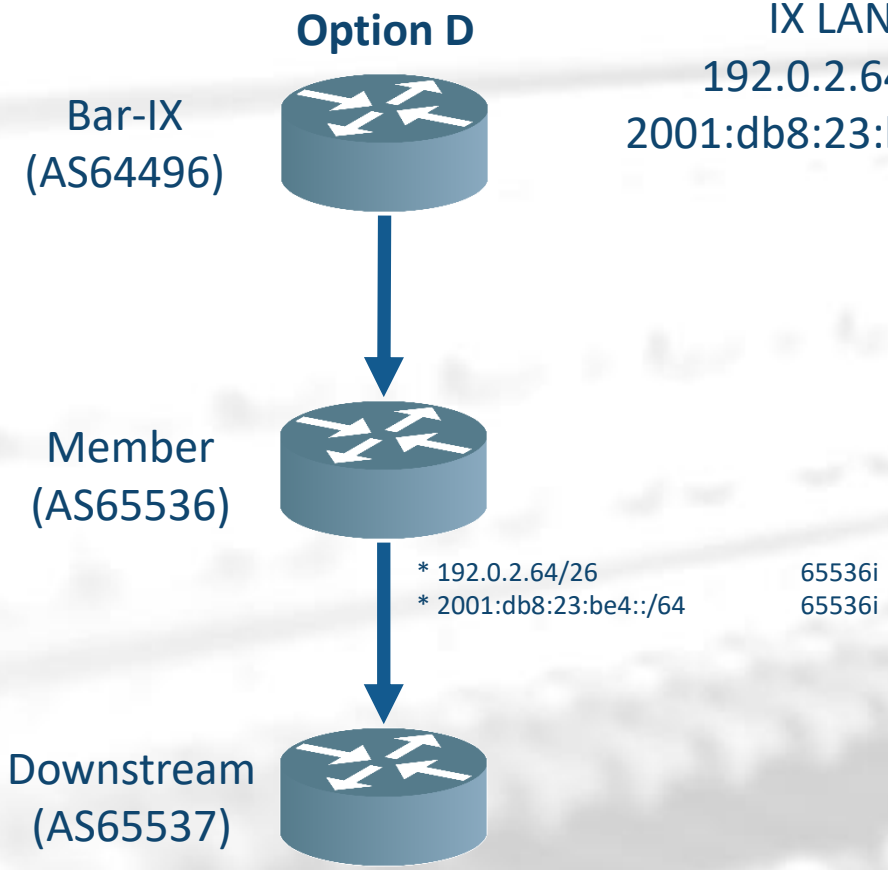
Implications (iii)



- Implications
  - The IX will not do this
  - AS65536 would have to have broken filters to import these routes

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Implications (iv)



IX LAN:
192.0.2.64/26
2001:db8:23:be4::/64

- Implications
  - The IX's NOC will probably have a 'small discussion' with AS65536
  - Best practice filters should catch this

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

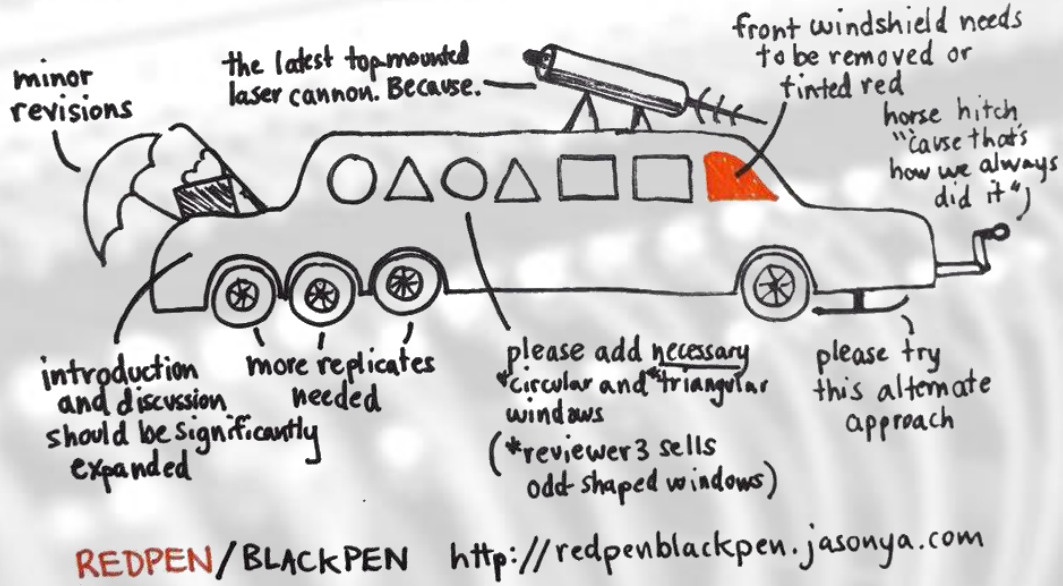
Some worms… that aren't really an issue.

- It was reasonable then, and operational practice shifted; Happens, things change, we can just ignore it
- IX operators can decide what *they* want
- While some creative interpretations can be difficult, nobody would try to force this, no? Like, by putting (not necessarily correct) assumptions on technology into laws and regulation.
- Still, it might be nice to update BCP194 to:
  - Be up-to-date with terms and technology
  - Iron out some of these smaller issues while we're at it

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

draft-ietf-grow-bgpopsecupd-01

- Collect a compendium of everything that is there
- Align terminology with what is currently going on
- Describe an ideal world best-practice
  - Yes, also prescribe honoring GSHUT & not setting higher LPREF on IXPs; This was probably THE most requested addition
- A 55 page draft
- Q: "What is in there?"
  A: "YES!"



Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Generally Well Received

"I read it last night, and I didn't hate it as much as I thought I would!"

- Anonymous IETF Attendee

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

On making laws and regulation: The FCC

> "*We therefore disagree with suggestions that testing should only occur within a provider's own network because providers do not always control the portion of the network reaching the nearest designated IXP.*", DA 18-710, FCC, 2018.

- Current discussions revolve around requiring test servers to be located directly on the IXP fabric
- Policy making is not made for ingesting long technical documents
- Long technical documents are—by definition—not made to be timeless

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

“I came here to drink milk …

- … and regulate the Internet; And I am all out of milk.”

- The FCC is currently looking at regulating BGP security:
  https://manrs.org/2024/05/fcc-bgp-regulation-recap/
  https://docs.fcc.gov/public/attachments/DOC-402609A1.pdf
- The FCC seems to have taken a rather informed approach this time around
- If the cool kids (here: FCC) have a fancy new toy^Wregulation, European regulators will want it, too
- Do you necessarily trust European regulators to always make technically well informed decisions?

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Things being regulated more strictly…

- National Security
  - Computer Security
  - Critical Infrastructure
  - Communication Services

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

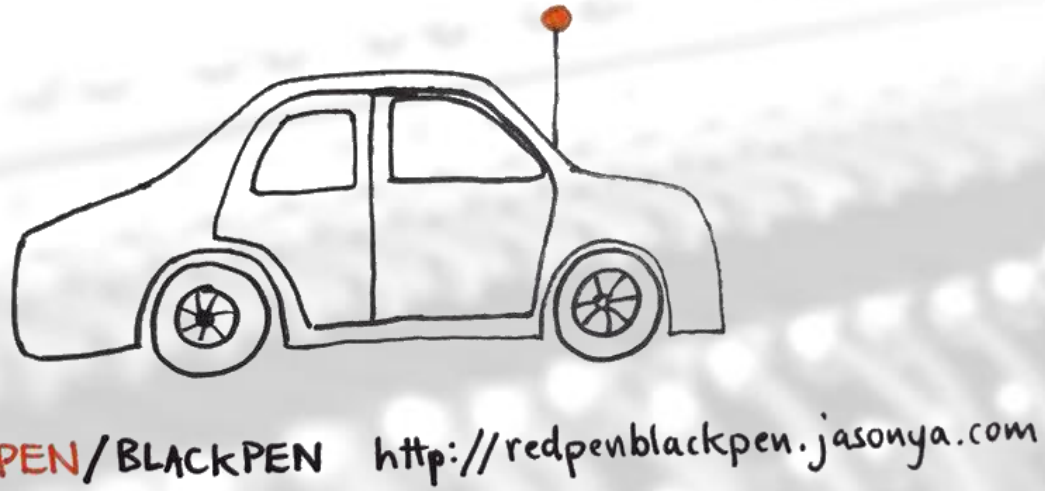
Things being regulated more strictly…

- National Security
  - Computer Security
  - Critical Infrastructure
  - Communication Services
- ISPs and IXPs are all of the above
- Policy makers need guidelines/documents to refer to
  - When is an entity 'doing good enough'?
  - What is the minimum to expect?
  - "At least follow best current practices!"

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

The BCP194 we need

- Short enough for policy makers to read and find actionable
- Testable enough to be referable in regulation
- Timeless (=technology agnostic) enough so it does not start falling on our feet without constant maintenance



Tobias Fiebig – tfiebig@mpi-inf.mpg.de

Towards draft-ietf-grow-bgpopsecupd-02

- Brief; Likely around 4 pages
  - Make sure no funny packets get to your BGP speakers
  - Make sure nobody meddles with your BGP sessions
  - Do not import anything you shouldn't
  - Do not export anything you shouldn't
  - Do not meddle with things not meant for you
- No specific technology or techniques
- No extensive terminology definitions
- Can be more authoritative due to higher-level guidelines

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

What got cut…

- There is extensive technical description and terminology documentation left over from -01
- Plan:
  - Create an *informational* 'available things and methods' draft
    - Easier to update
    - Not prescriptive -> Less arguments about what should (not) go in
    - Repository, not policy; Could have a best-before-date
  - Create an *informational* 'terms currently in use' draft
    - Will need constant updates anyway
    - Language differs per BGP application

Tobias Fiebig – tfiebig@mpi-inf.mpg.de

What to take away

- Please provide feedback on the current state of the draft: https://github.com/ichdasich/draft-ietf-grow-bgpopsecupd
- Talk to policy makers
  - They appreciate help contextualizing technical documents
  - The CONNECT WG is just right there ;-)
- Technical documents may get unexpected audiences

Draft Repo

Tobias Fiebig – tfiebig@mpi-inf.mpg.de