Microsoft RPKI Deployment Experience – NANOG 67

JR Mayberry

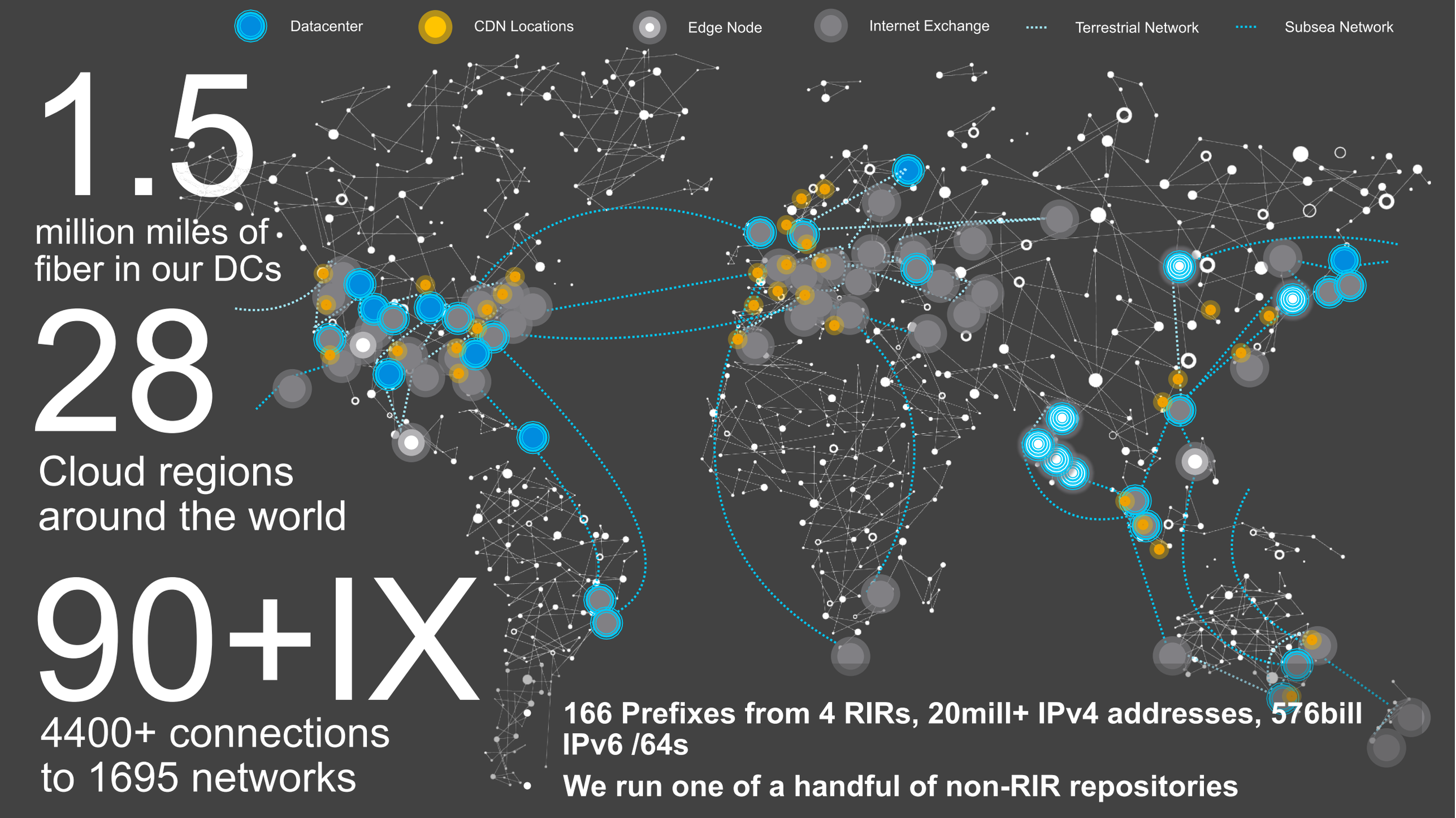
Cloud Network Security

Microsoft Azure/Networking

rimayber@microsoft.com, @mayberry0404

Purpose/Agenda

- Why Microsoft cares about RPKI
  - We are passionate about availability and security
  - Prefix hijacks compromise both
  - Only detective solutions are “effective” right now
- What is our goal?
  - RPKI adoption can be “scary” – the implications are unknown to most
    - Will I break routing?
    - Will I black hole my organization?
    - Will I de-preference my routes?
  - Demystify technology so there is wider adoption
  - We need clearer path to more effective risk mitigation of route hijacks – TODAY
- Agenda
  - Walk pragmatically through an implementation
  - Cover tips to help navigate decisions


Datacenter
CDN Locations
Edge Node
Internet Exchange
Terrestrial Network
Subsea Network
1.5
million miles of fiber in our DCs
28
Cloud regions around the world
90+IX
4400+ connections to 1695 networks
166 Prefixes from 4 RIRs, 20mill+ IPv4 addresses, 576bill IPv6 /64s
We run one of a handful of non-RIR repositories

RPKI in 10 Steps

1. Inventory “resources” – RIR, Prefixes, max length, origin ASN
2. Decide to run in Hosted vs. Delegated model
3. Understand basics of RPKI – and ROA validation states
4. Pilot RPKI and validate your pilot ROA
5. Read concerns about RPKI, RIR indemnification
6. Review lessons learned from other operators
7. Plan implementation/HA/Scale model – perfect cloud app
8. Install and secure RPKI
9. Monitor RPKI, ROAs and industry RPKI status
10. Plan recovery from breach/catastrophic failure

Decide Hosted vs. Delegated

- Questions to ask yourself
  - Will I ever have a downstream customer that I assign IP space to want to create ROAs or run their own RPKI?
  - Who are my RIRs? Does my predominant RIR support one model and not the other?
  - How do I feel about managing more infrastructure/software, etc?
  - How do I feel about securing more infrastructure/software, etc?
  - How do I feel about someone else's ability to run "critical infrastructure" on my behalf?
  - Am I okay with having multiple business processes if I have space from multiple RIRs?
  - Is my business changing that changes any of these answers in the future?
- Hosted – service run by RIRs in member portal
  - Could support an HSM
  - Infrastructure is someone else's management
- Delegated - RPKI.net tools or other
  - Perfect "cloud" solution
  - As of 2015, only ARIN had production support
  - Technically "one business process" – one stop shopping

Lessons Learned

- New development fork is coming…
- In the context of a delegated model/RPKI.net
  - Documentation is pretty decent – terms are new, can be confusing at first
  - Support was/is? best effort – helpful to an extent, DHS funding has been an issue
  - Mailing list volume is low to non-existent, marginally helpful – a thread a month
  - RPKI.net software can be “finicky” – breaks randomly, hard to troubleshoot, difficult to migrate
  - Community of experienced operators is difficult to find – MSFT one of a few operating a repository
  - Trial and error is how you’re going to learn however…
    - If you misconfigure something, have a down infrastructure, “people” will find you
    - These “people” are concerned about sensitivity to robustness of RPKI
  - RPKI is still viewed as a “science project” – minimal short term value, questioned long term
  - HSM support is not present – uses OpenSSL libs, tried integration, didn’t work
  - You need to ensure IP Address management processes incorporate RPKI processes – this includes ADD and DELETE of prefixes - the RPKI infrastructure is probably best operated by your IP address management team – make sure monitoring changes included in processes
  - Hard to tell “why” failing – manifests, caching, refresh
  - As an operator, you have no idea who is enforcing policy, and how, as a result of INVALID ROAs

Monitor RPKI

- Commercial monitoring services exist – like BGPMon
- Monitoring needs to be engrained in ops culture
- Almost 10% of global v4 ROAs are invalid right now
- Useful resources
  - RPKI repository monitoring - valuable for delegated model
  - RIPE prefix validator