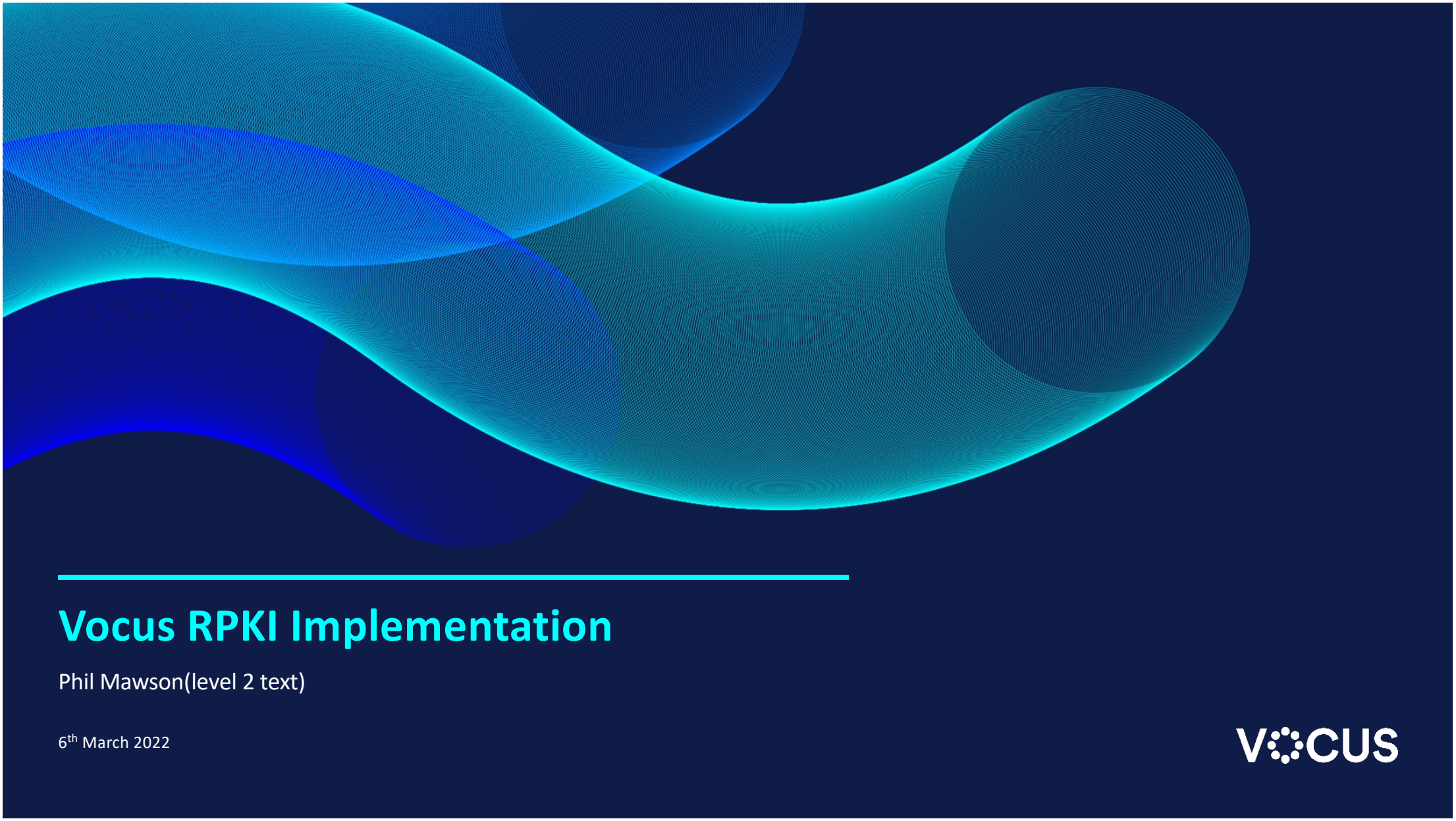


# Vocus RPKI Implementation

Phil Mawson(level 2 text)

6th March 2022

VOCUS

# Design Decision

Multivendor (Cisco, Juniper, Arista, Nokia)

International (Australia, NZ, US & Asia)

Security Concerns

Centralised Management & Monitoring

What validator software to use

| | IOS | XR | JUNOS |
|---|---|---|---|
| SSH | NO | YES | NO |
| TLS | NO | NO | NO |
| TCP | YES | YES | YES |
| TCP-MD5 | NO | NO | NO |
| TCP-AO | NO | NO | NO |
| IPsec | NO | NO | NO |

# Validator Software

NLNet Labs Routinator – Very community focussed

Join their RPKI Discord Server

RIPE RPKI Validator – EOL mid July 2021

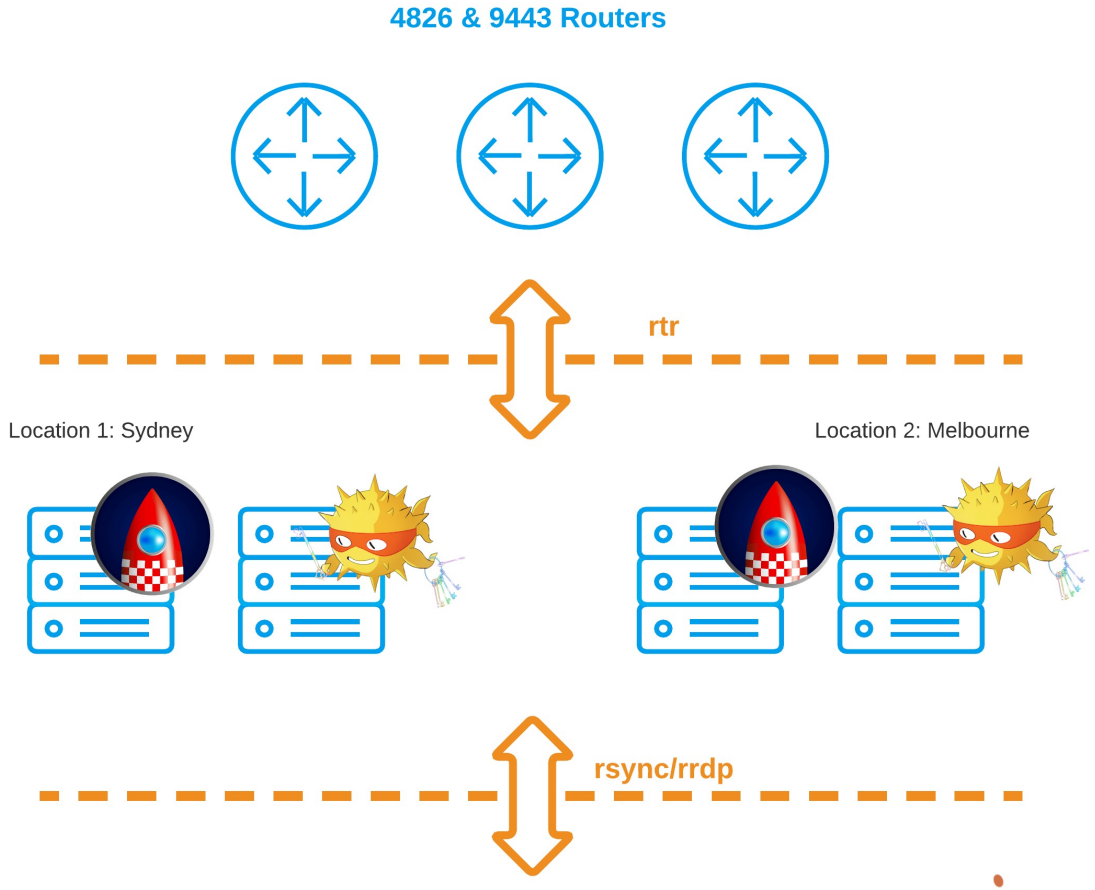
Fort

OctoRPKI

BSDs open-rpki with GoRTR (now StayRTR)



VOCUS




RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ARIN
American Registry for Internet Numbers

AFRINIC

lacnic

APNIC

VOCUS

# Timeline

**Feb 2020**
(Apricot Melbourne)
Initial “kick in the butt”

**April – June 2020**
All Vocus group owned routes signed with valid ROAs via APNIC portal and announcements aggregated and cleaned

**April – July 2020**
Internal testing of validator software in our lab

**August 2020**
AS9443 & AS38285 blocking invalid routes

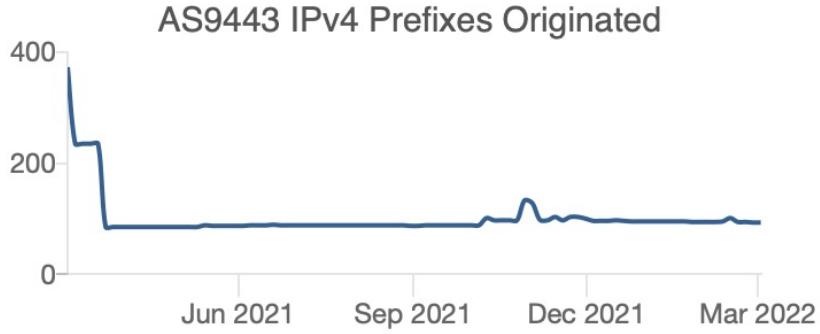
**16th March 2021**
AS4826 now blocking invalid ROAs

# Aggregation of routes and IRR Clean up

AS9443 routes were aggregated as highly as possible, we remove approx. 60% of the announced routes into global table.

Any Vocus Owned route now have their WHOIS object via APNIC and removed from many third party data sources (RADb, REACH, NNT, Level3). Single source of truth

Long term goal to remove all legacy entries in our RADb – Got any, irr@vocus.com.au



# Timeline

**Feb 2020**
(Apricot Melbourne)
Initial “kick in the butt”

**April – June 2020**
All Vocus group owned routes signed with valid ROAs via APNIC portal and announcements aggregated and cleaned

**April – July 2020**
Internal testing of validator software in our lab

**August 2020**
AS9443 & AS38285 blocking invalid routes

**16th March 2021**
AS4826 now blocking invalid ROAs

# Lessons Learnt

OpenSource software can be EOL'd very quickly
- RIPE Dropped their validator support end of 2020
- Louis left Cloudflare, leaving GoRTR un-maintained. This was later forked to StayRTR

Java Sucks (Who didn't know this already)
- RIPE Validator UI was built on Java, often would crash and require process restart

Clean your IRRs
- APNIC make it very easy to create those objects in their portal.
- Trust a RIR over RADb

Customer notifications
- Get this right, and get it done early.



VOCUS

# Limitations Learnt

Cisco

- Unable to set source address for validation session

  Bug CSCvg37740 and resolved in 6.7.1

- If session to validator server lost, cache may not be re-built locally

  Bug CSCvp82287 and resolved in a number of versions

Juniper

- Only support clear text (no SSH unlike Cisco)

  Not resolution for this yet, is a feature request



VOCUS

# Monitoring

**BGP Alerter** APP 15:35

**rpki**

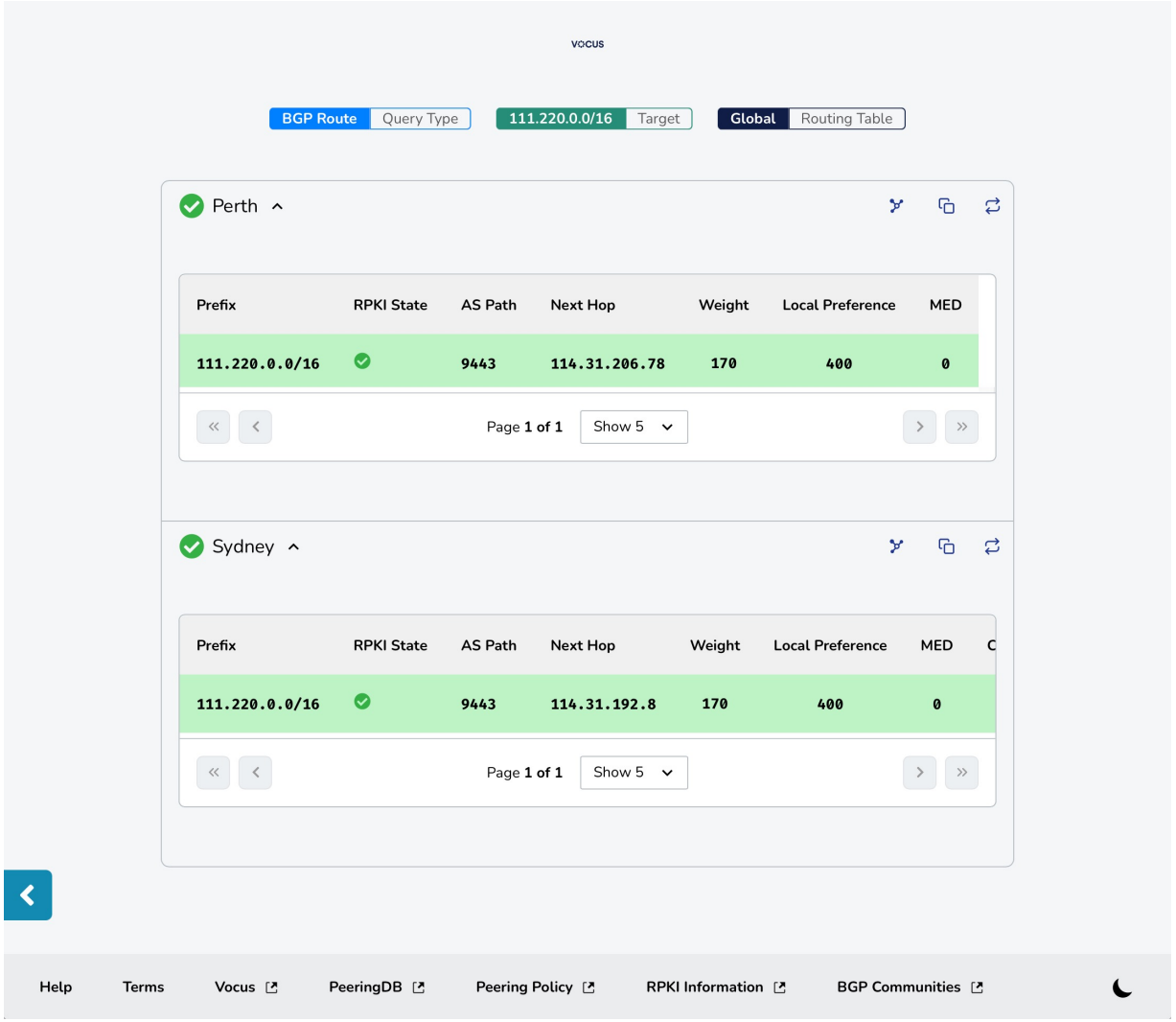
The route 202.43.86.0/24 announced by AS4826 is not RPKI valid. Valid ROAs: 202.43.86.0/24|AS45947|maxLength:24. Top 3 most used AS paths: [3356,4826], [8220,4826],[8758,6830,3257,4826].

**BGP Alerter** APP 15:57

**visibility**

The prefix 202.43.86.0/24 (CUSTOMER) has been withdrawn. It is no longer visible from 40 peers

# Updated Looking Glass – lg.vocus.network



# Special Shout Outs

Tashi Phuntsho & Dave Phelan @ APNIC

Mark Duffel & Scott Reed @ Telstra

Francis Nie & Jorg Dekker @ Telia

Job Snjiders @ NTT/Cloudflare/BSD

Handy resources

- NLNet Labs RPKI Discord channel
- bgp.he.net & rpki.cloudflare.com websites



VOCUS

VOCUS