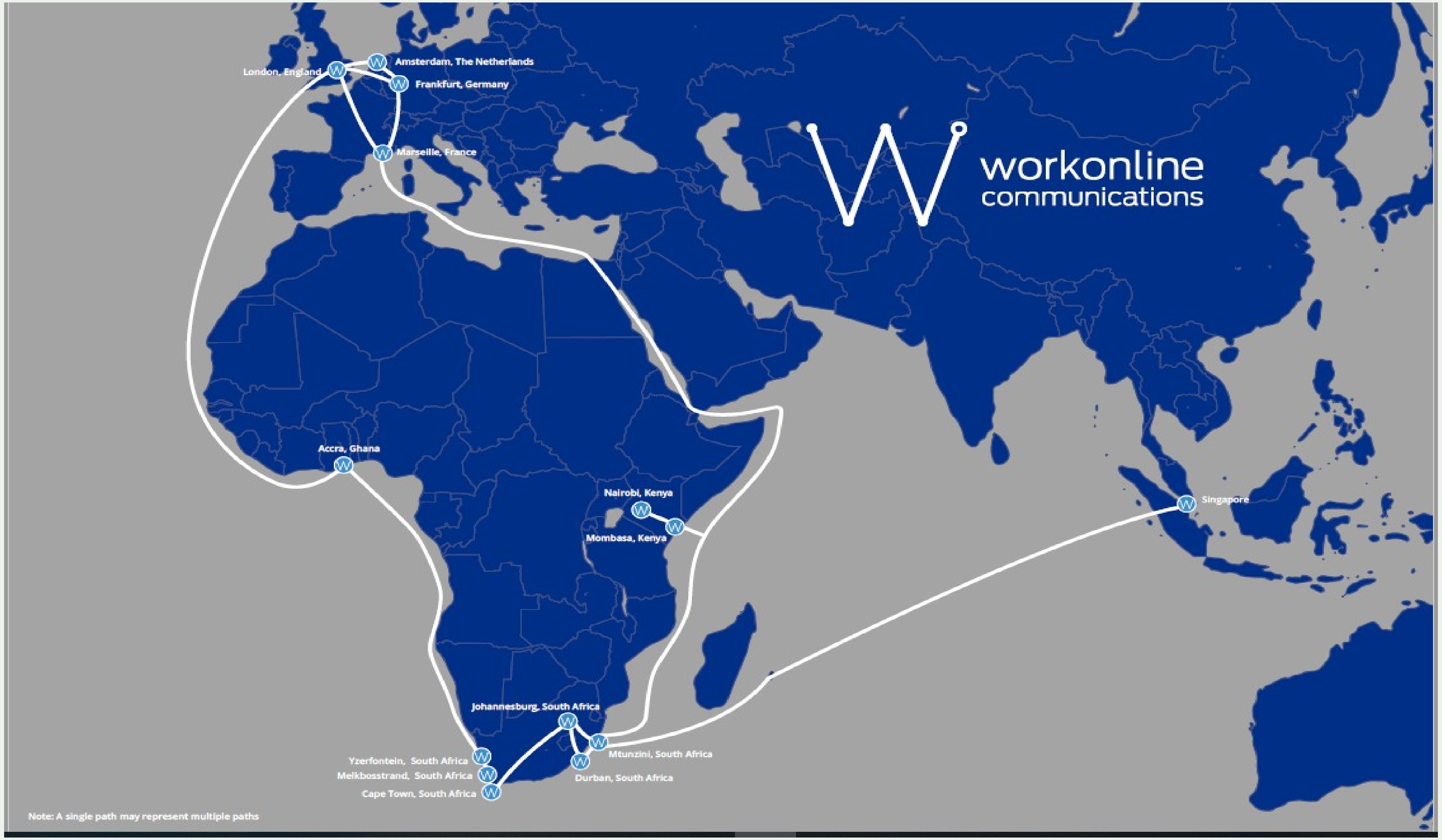
Workonline Communications

MICHELLE OPIYO
UGNOG 2020
14th October 2020

OUR NETWORK



Note: A single path may represent multiple paths

What are we talking about today?

- HOW NETWORK OPERATORS CAN CONTRIBUTE TO SECURING THE GLOBAL ROUTING SYSTEM

The Problem

A Routing Security Overview

The Basics: How Routing Works

There are ~69,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Routing Incidents are Increasing

In September 2020, 1'310 Routing Incidents were detected in data collected in the MANRS Observatory.

These incidents led to a range of problems including stolen data, lost revenue, reputational damage, and more.

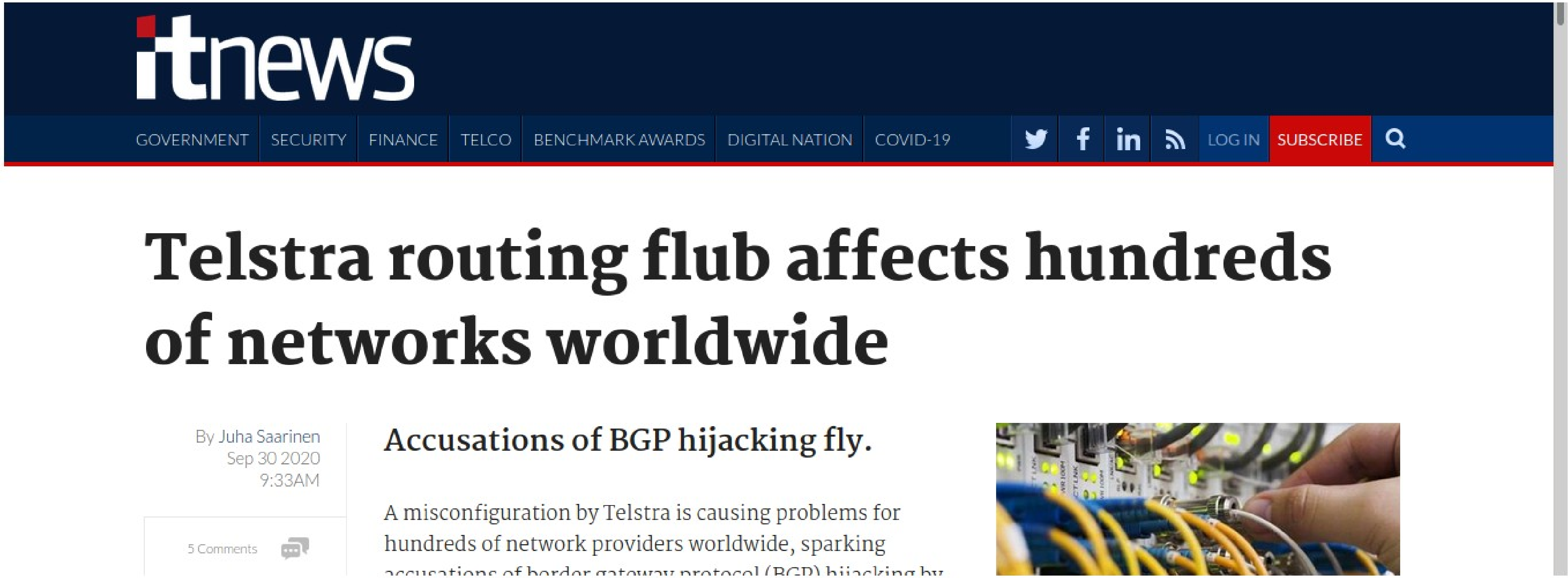
Some of these hijacks lasted for many hours

Incidents are global in scale, with one operator’s routing problems cascading to impact others.

Routing Incidents Cause Real World Problems

- Unsecure routing is one of the most common problem for malicious threats.
- Attacks can take anywhere from hours to months to even being identified.
- Inadvertent errors can take entire countries offline, while attackers can steal an individual’s data or hold an organization’s network hostage.

Recent Events



Telstra routing flub affects hundreds of networks worldwide

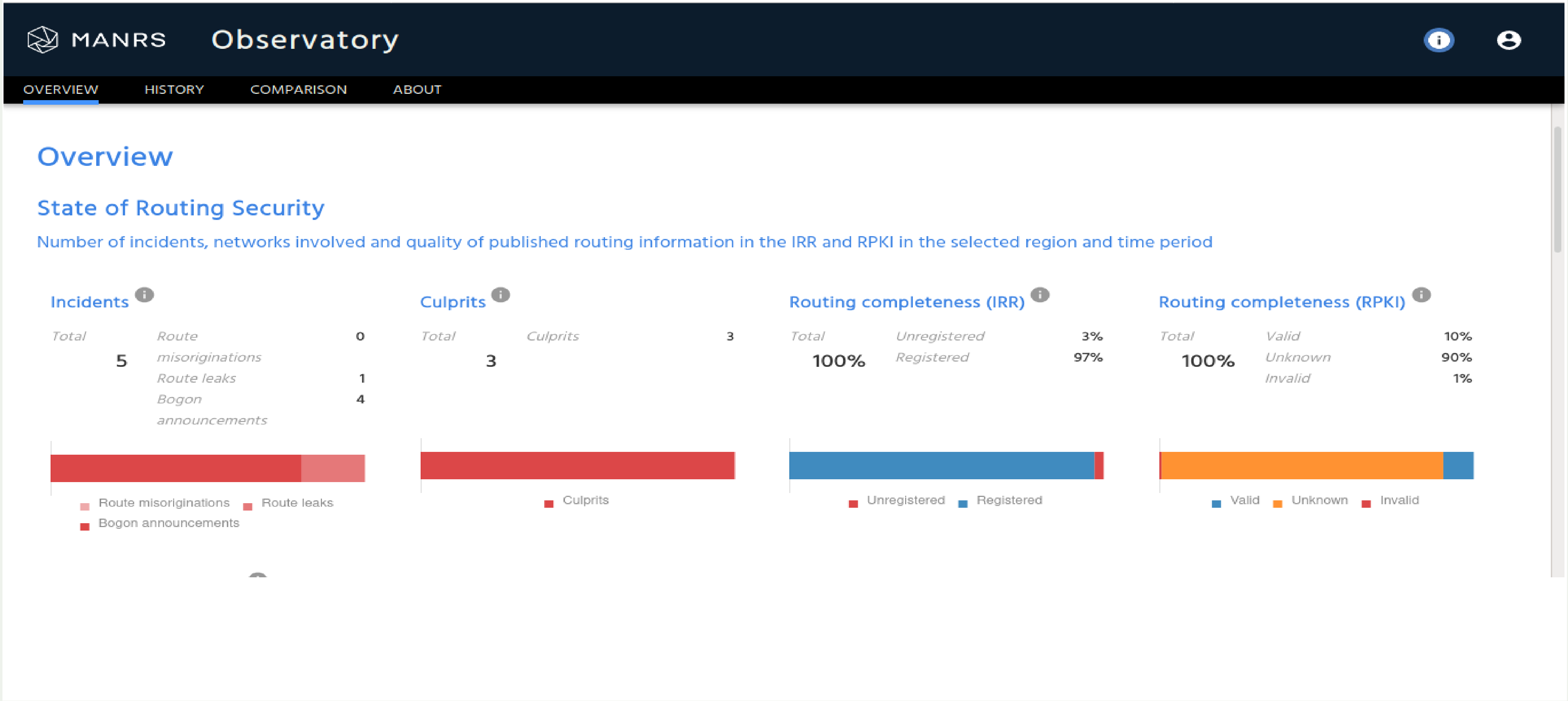
By Juha Saarinen
Sep 30 2020
9:33AM

5 Comments

Accusations of BGP hijacking fly.

A misconfiguration by Telstra is causing problems for hundreds of network providers worldwide, sparking accusations of border gateway protocol (BGP) hijacking by

Routing Incidences in Uganda–September 2020



Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
5	Route misoriginations	0
	Route leaks	1
	Bogon announcements	4

Culprits

Total		
3	Culprits	3

Routing completeness (IRR)

Total		
100%	Unregistered	3%
	Registered	97%

Routing completeness (RPKI)

Total		
100%	Valid	10%
	Unknown	90%
	Invalid	1%

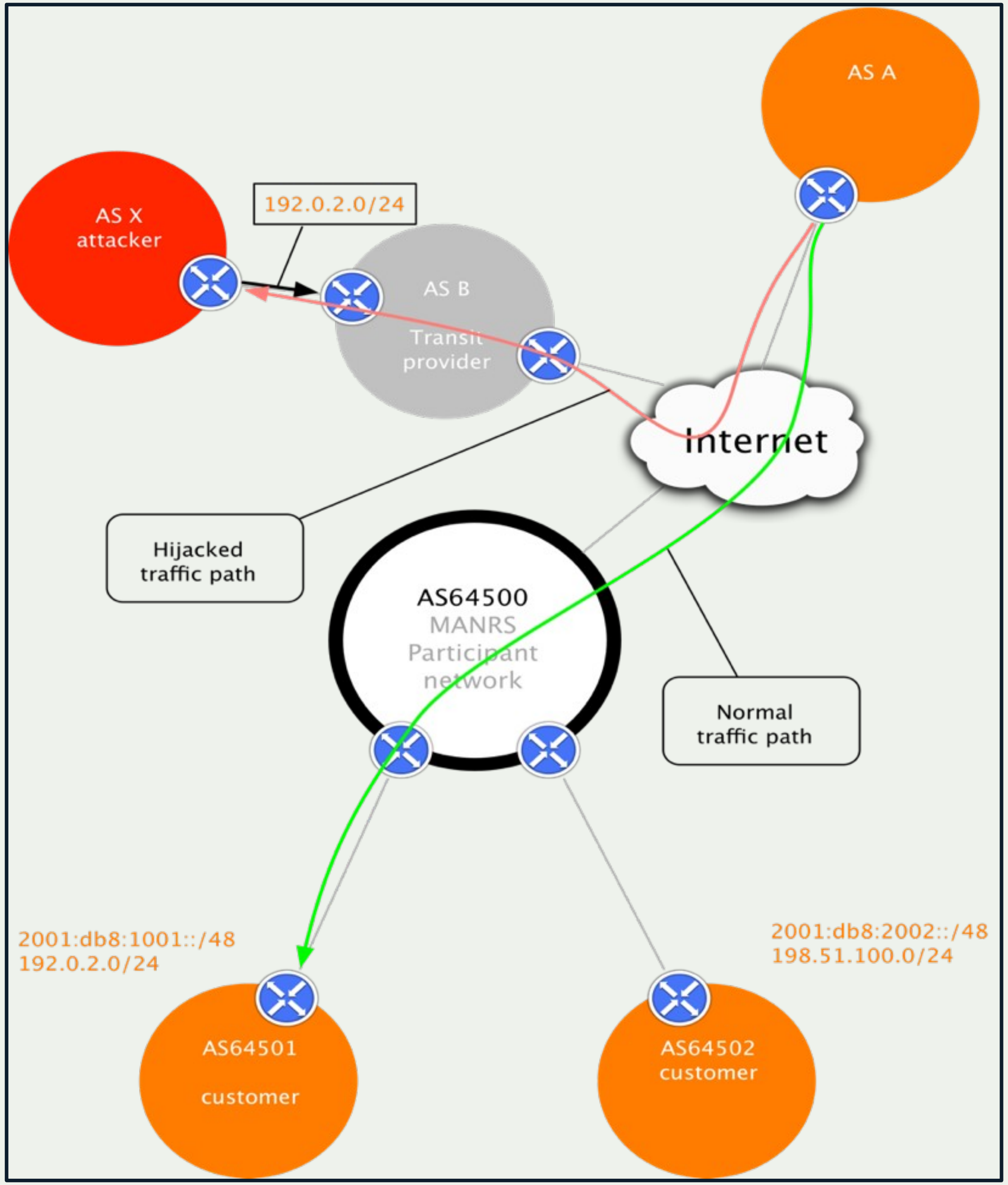
The Threats: What’s Happening?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

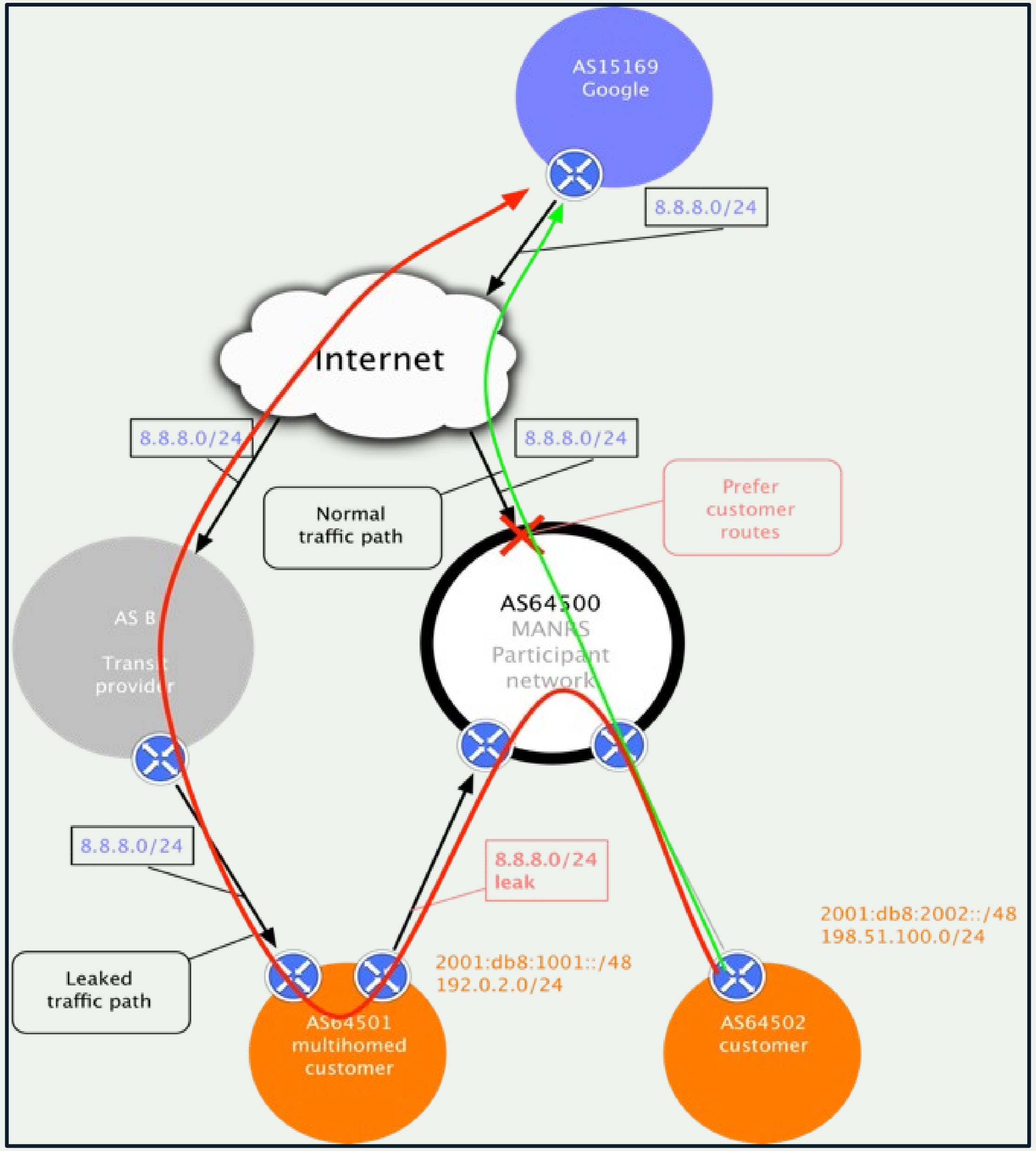
Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.



Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

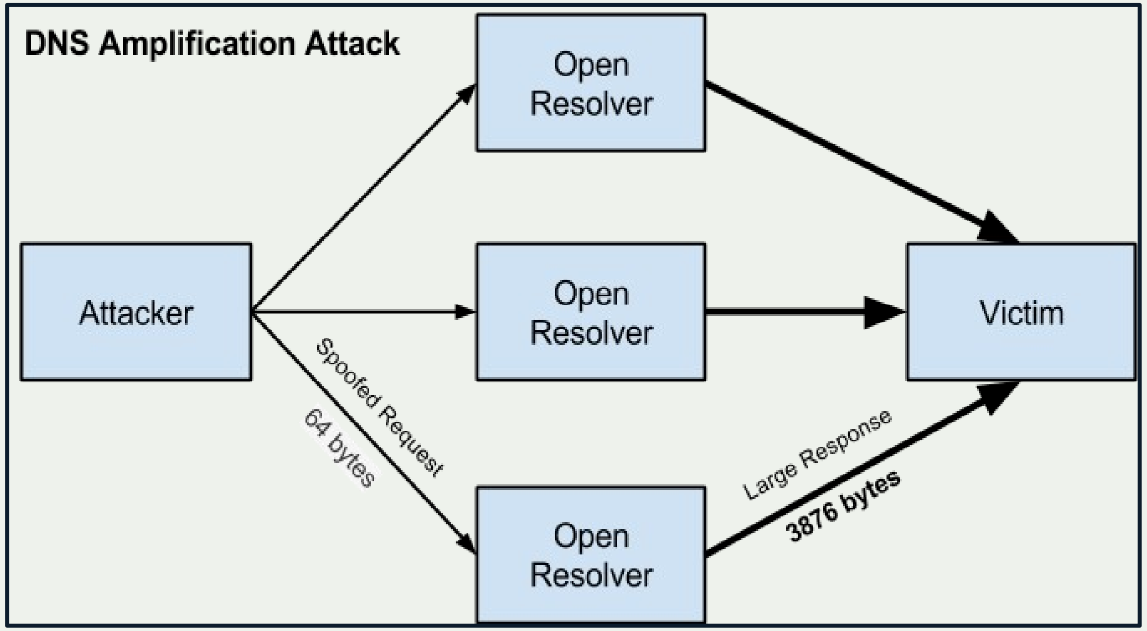
Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3’s networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.



IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.



Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).

Tools to Help

- Prefix and AS-PATH filtering
- RPKI, IRR toolset, IRRPT, BGPQ3/Q4
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

MANRS

MANRS Actions - Network operators

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

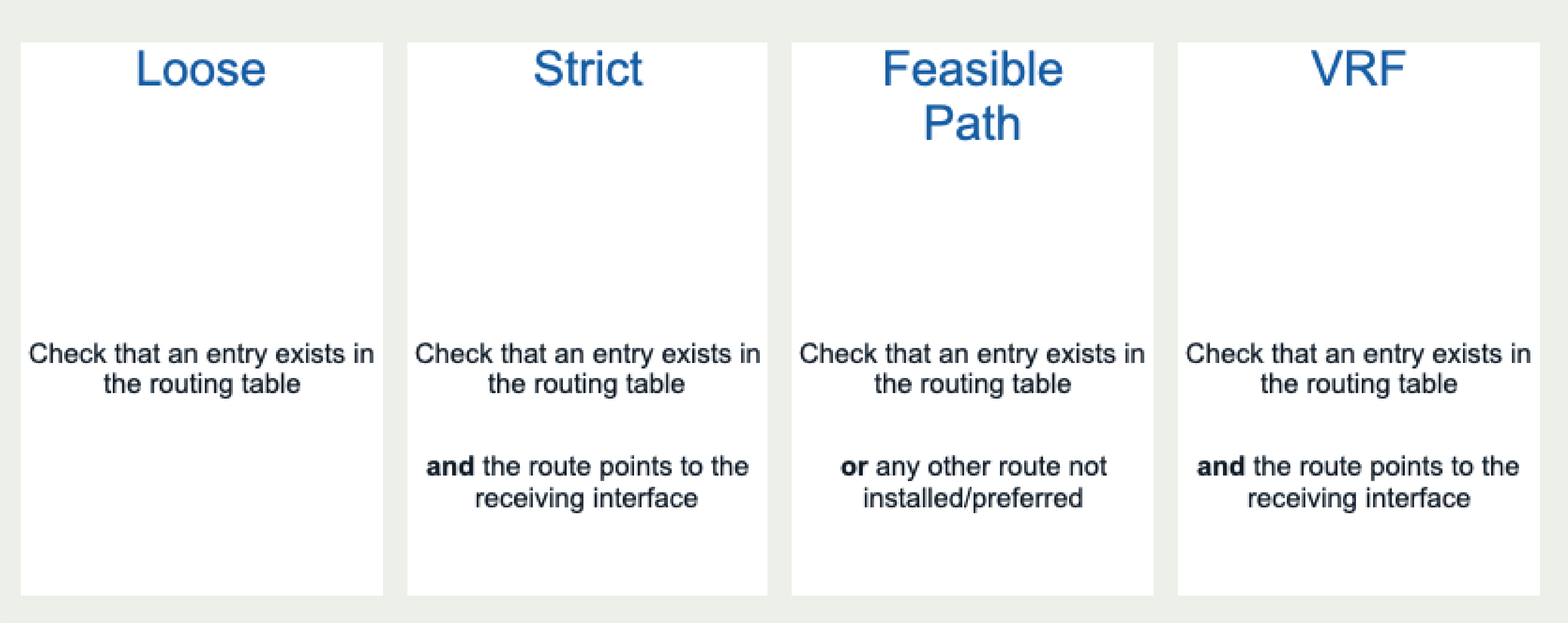
Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Source Address Validation



Loose	Strict	Feasible Path	VRF
Check that an entry exists in the routing table	Check that an entry exists in the routing table	Check that an entry exists in the routing table	Check that an entry exists in the routing table
	and the route points to the receiving interface	**or** any other route not installed/preferred	**and** the route points to the receiving interface

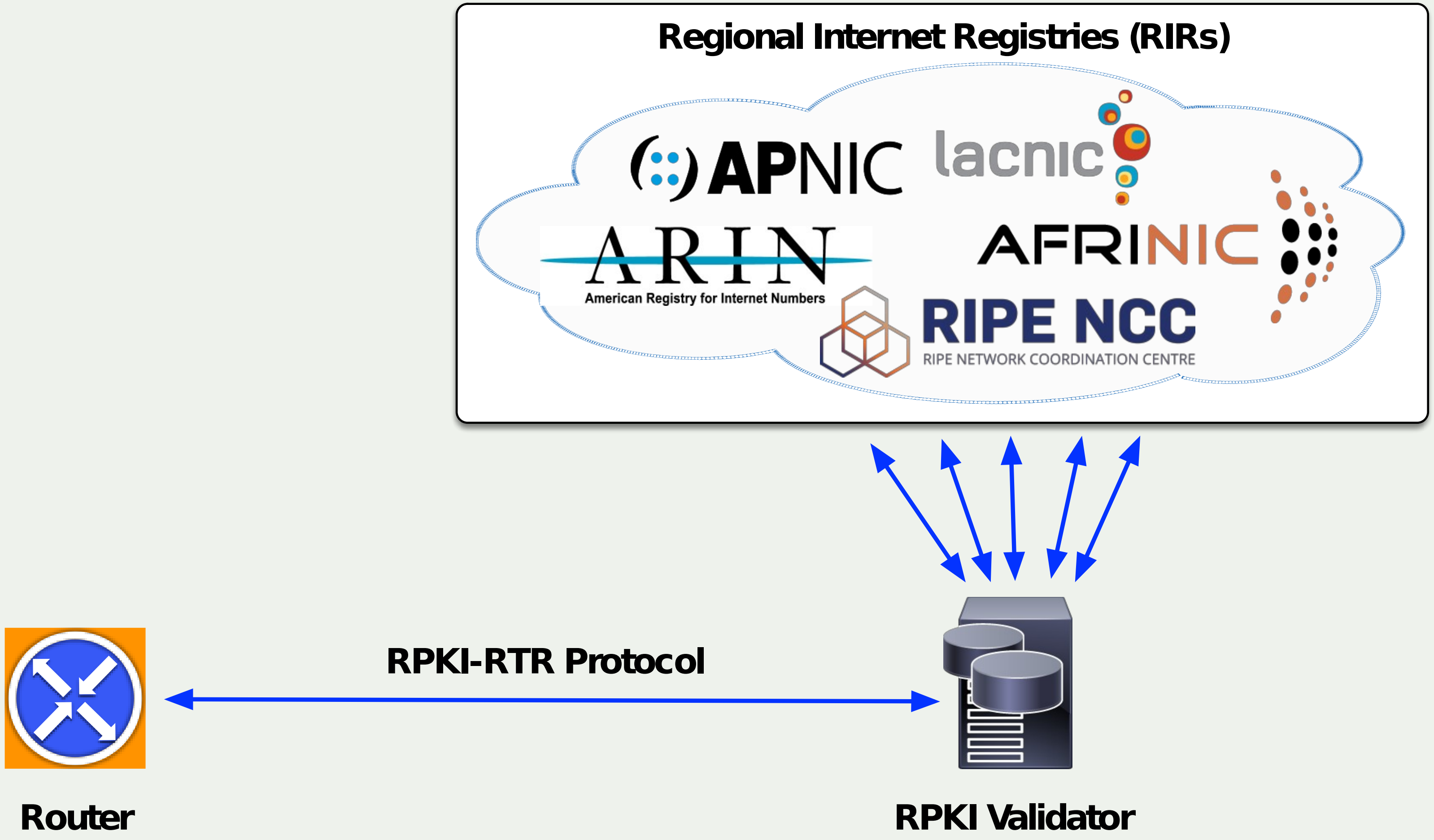
Global Validation

Routing information should be made available on a global scale to facilitate validation, which includes routing policy, ASNs and prefixes that are intended to be advertised to third parties. Since the extent of the internet is global, information should be made public and published in a well known place using a common format.

Object	**Source**	Description
aut-num	IRR	Policy documentation
route/route6	IRR	NLRI/origin
as-set	IRR	Customer cone
ROA	RPKI	NLRI/origin

Global Validation

Providing information through the RPKI system


Regional Internet Registries (RIRs)
APNIC
lacnic
ARIN
American Registry for Internet Numbers
AFRINIC
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
RPKI-RTR Protocol
Router
RPKI Validator

Why join MANRS?

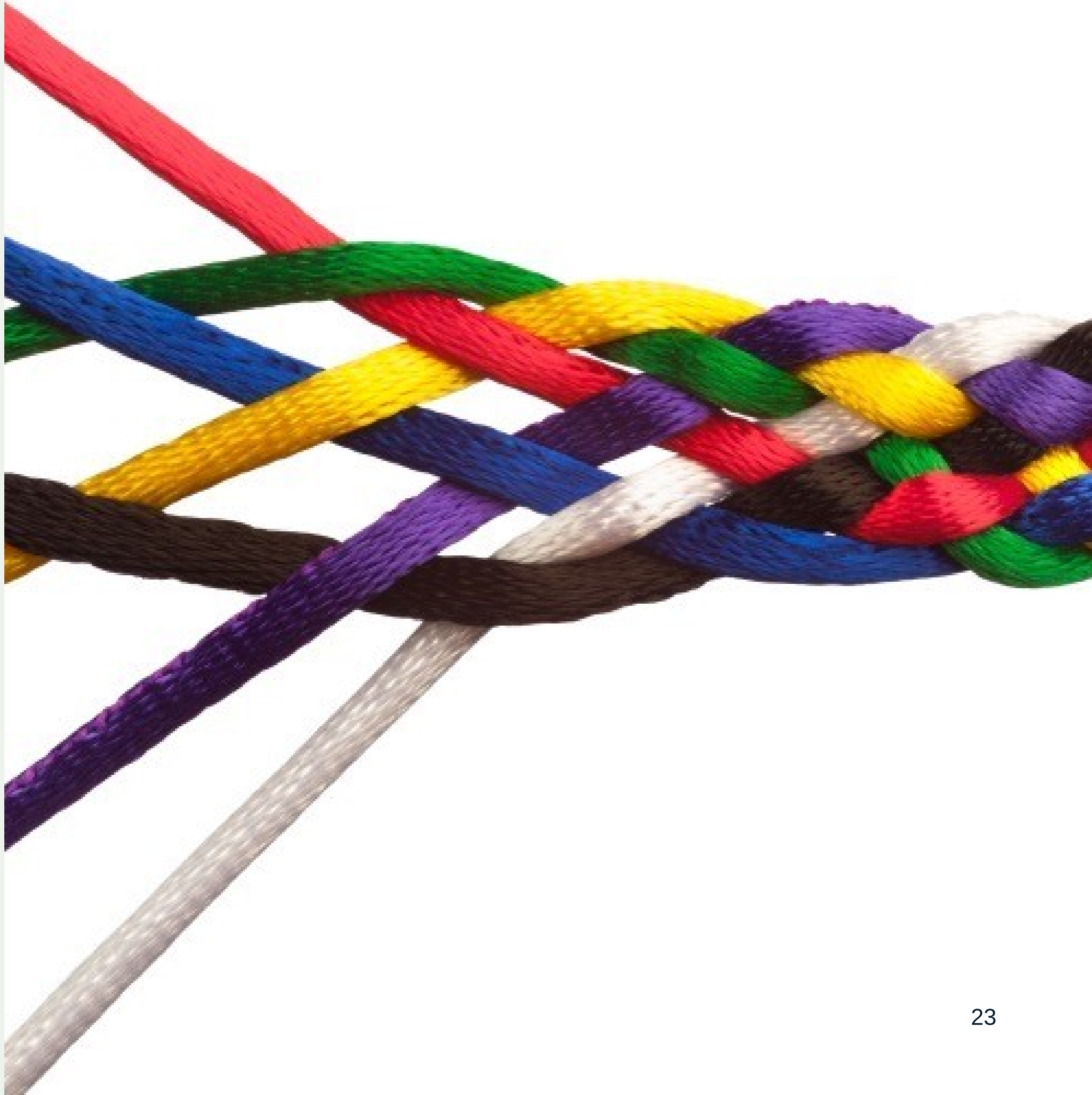
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

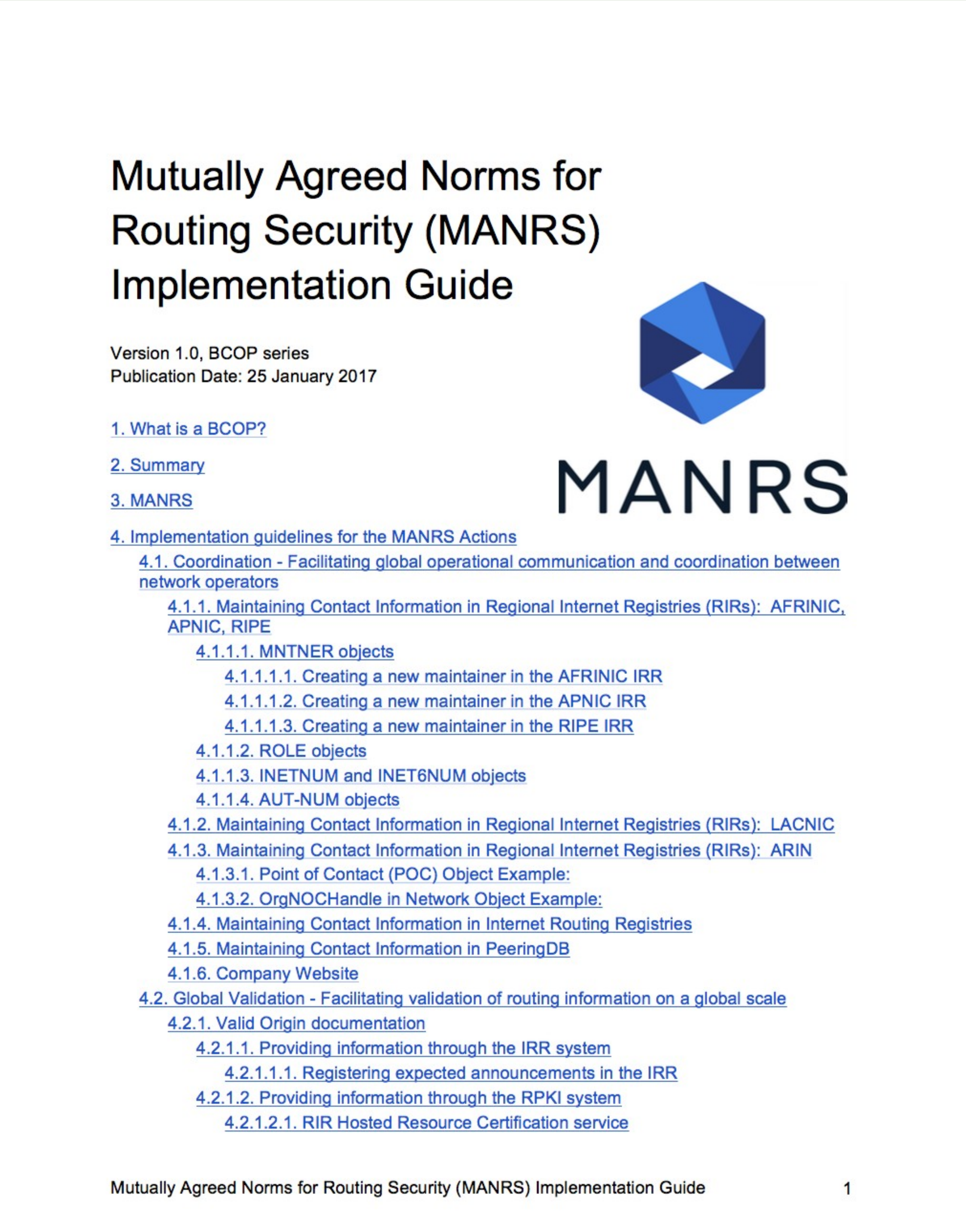
- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives



MANRS Implementation Guide

If you’re not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series
Publication Date: 25 January 2017

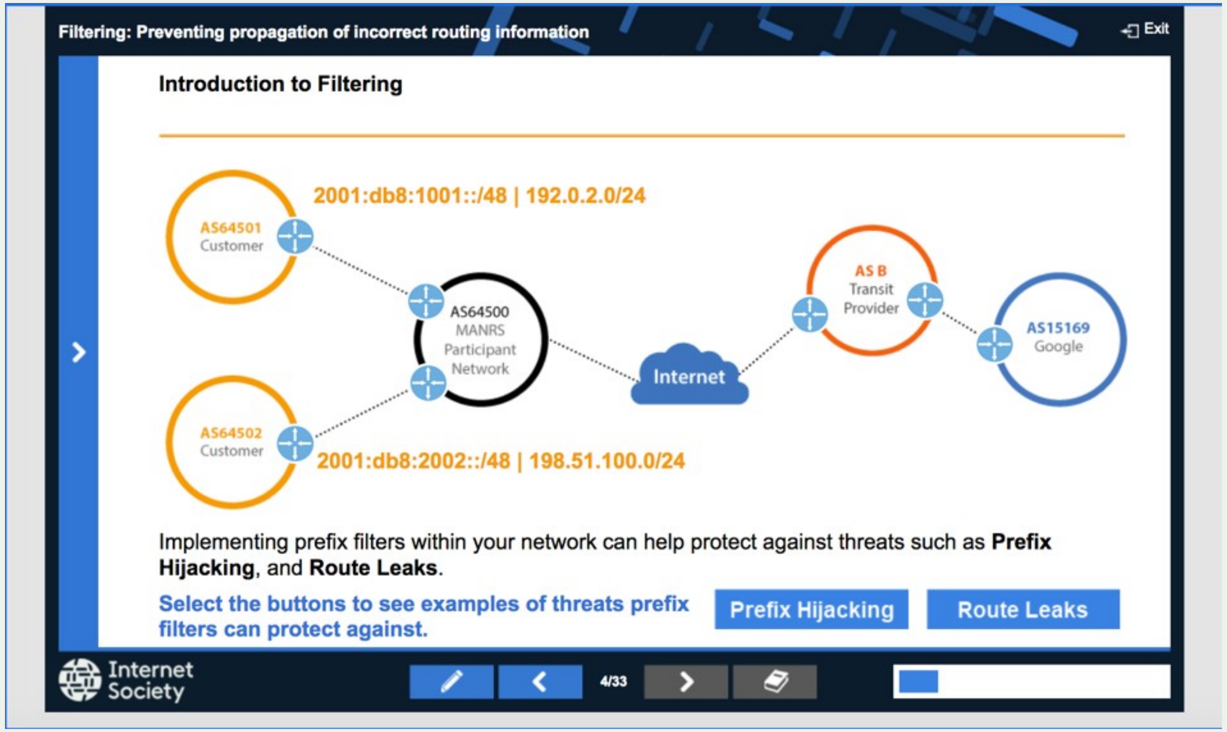
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://academy.apnic.net/en/course/manrs/



Filtering: Preventing propagation of incorrect routing information

Introduction to Filtering

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

Select the buttons to see examples of threats prefix filters can protect against.

hanks to APNIC for hosting MANRS Tutorial

LEARN MORE:

https://www.manrs.org

Thank you.

manrs.org