How to use this template:

There are ~50 slides in this presentation, so you likely will not use them all (some are intentionally repetitive to provide options). This is the most up-to-date MANRS messaging, graphics, notes, etc. Take what you need, leave the rest!

1. Opening the POTX (PowerPoint template) creates a new document.

2. Cut out the slides irrelevant to your audience, and/or add new information as needed.

3. Please share your presentation with us. Send it to manrs@isoc.org naming it YYYYMMDD_EVENTNAME_MANRS.ppt.

4. If you find an error in the original slides, let the MANRS team know so they can fix it in the template for the next person. Write to us at contact@manrs.org.

MANRS

Mutually Agreed Norms for Routing Security

NAME

EMAIL

Why Does Routing Security Matter?

A Routing Overview

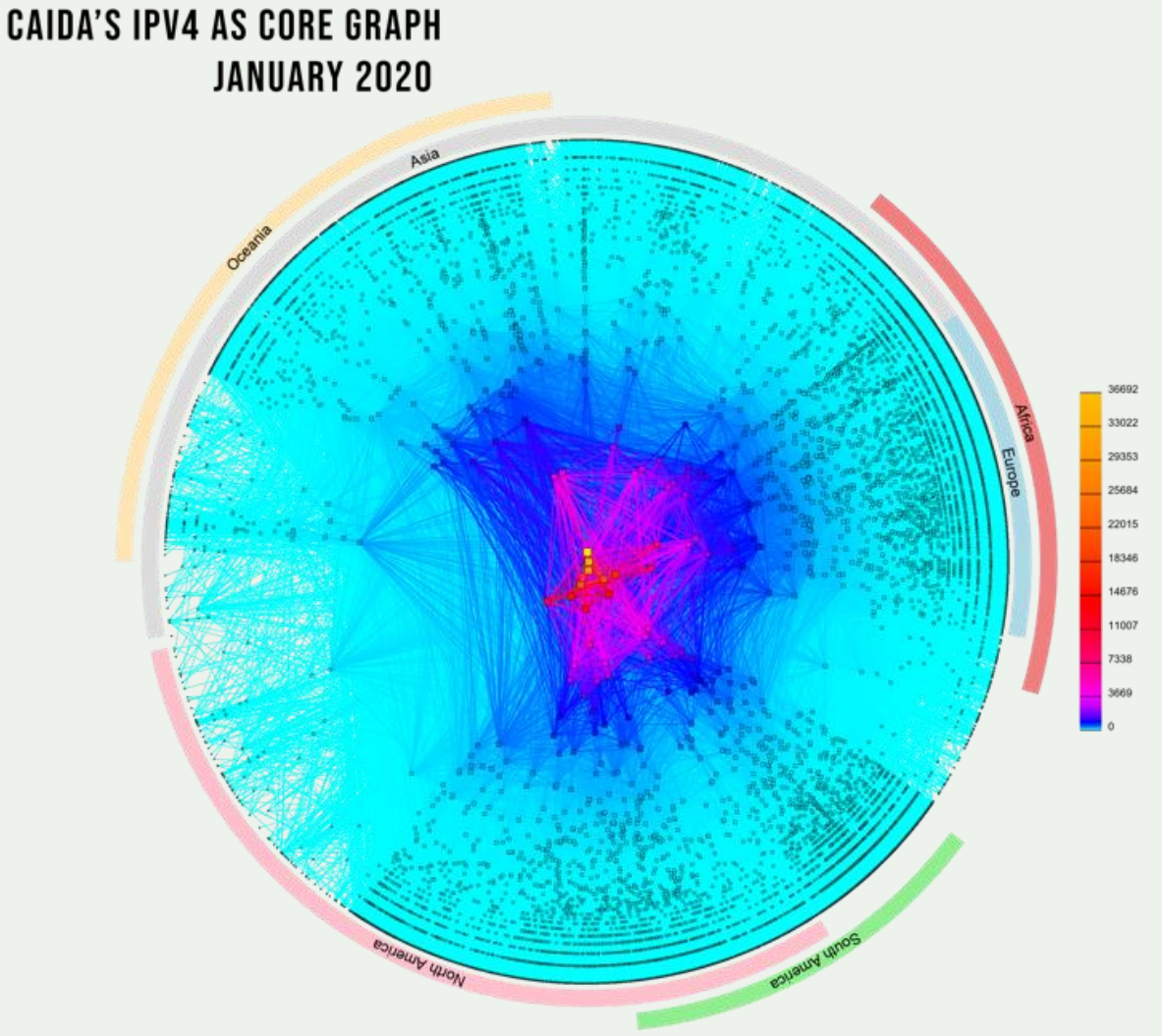
An Extremely Condensed Routing 101

There are ~74,000 independent networks that together make up the Internet.

Each network is identified by an **Autonomous System Number, or ASN**.

Each ASN makes its own decisions about how to move Internet traffic using a language called **Border Gateway Protocol, or BGP.**

BGP is a fundamental underpinning of the Internet.



The Problem with BGP

BGP was created in 1989, before Internet security was a concern.

BGP assumes all networks are trustworthy. Any network can announce it has a path to any other network, even if it does not.

There is no built-in security mechanism to check if traffic is legitimate or not.

On today's Internet, this is a problem.

BGP is vulnerable to both malicious attacks and human mistakes.

Routing Incidents Happen Across the Internet

In 2019 alone, over 10,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet were affected.

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

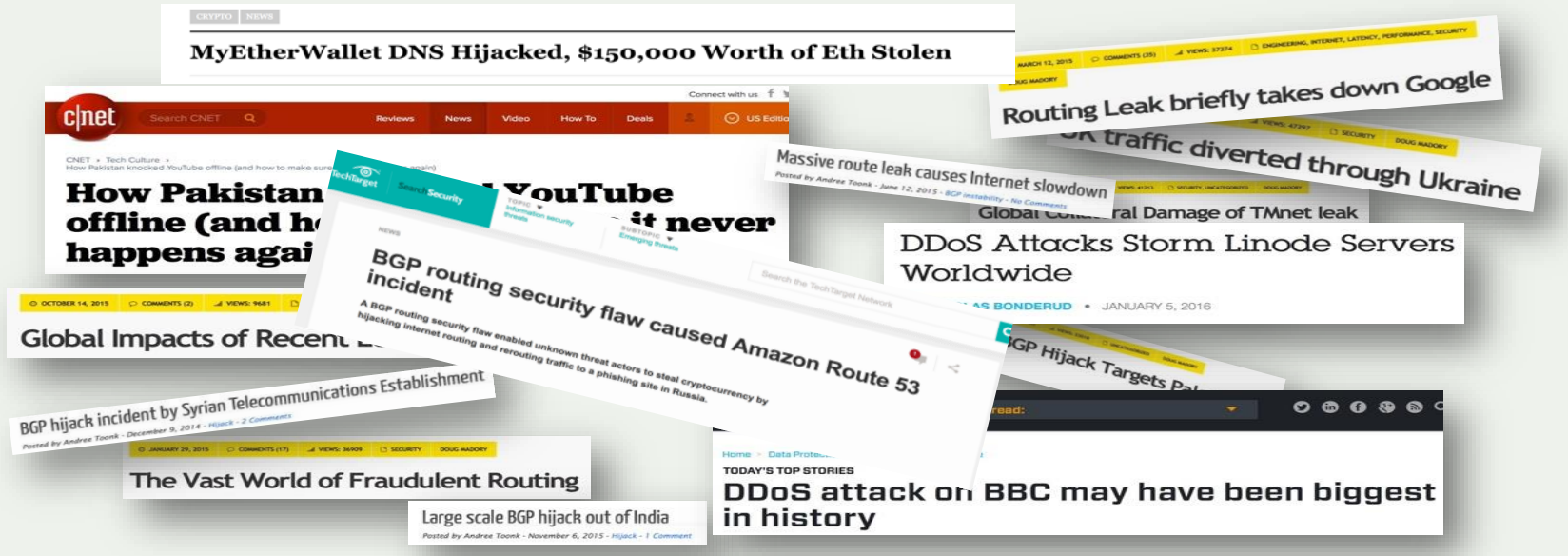
https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/

Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.



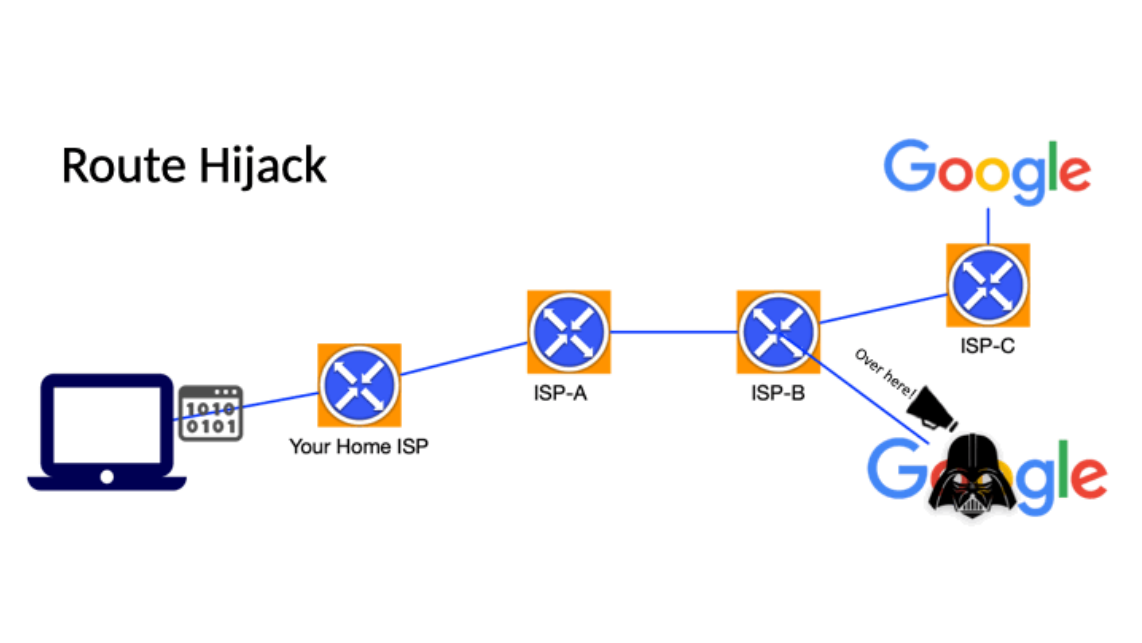
What are Routing Incidents?

A Routing Security Overview

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; this can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers announces (often due to accidental misconfiguration) 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

Problem: BGP Hijacks

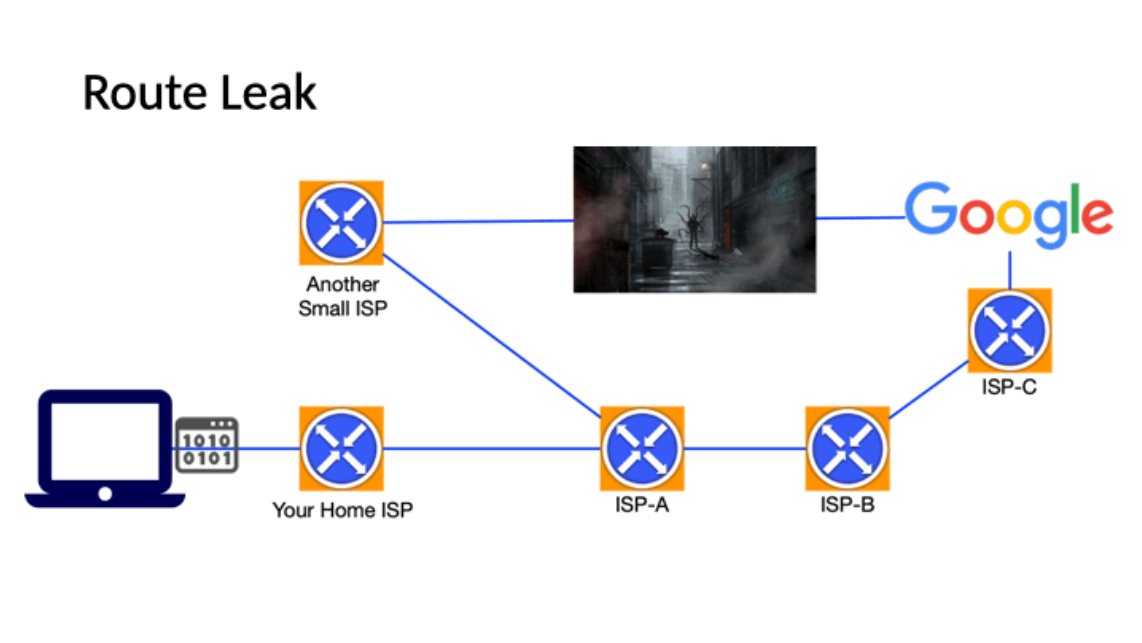


A network or attacker impersonates another network, pretending that a server or network is their client.

Result: Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.

Hijacks are usually intentional.

Problem: BGP Leak

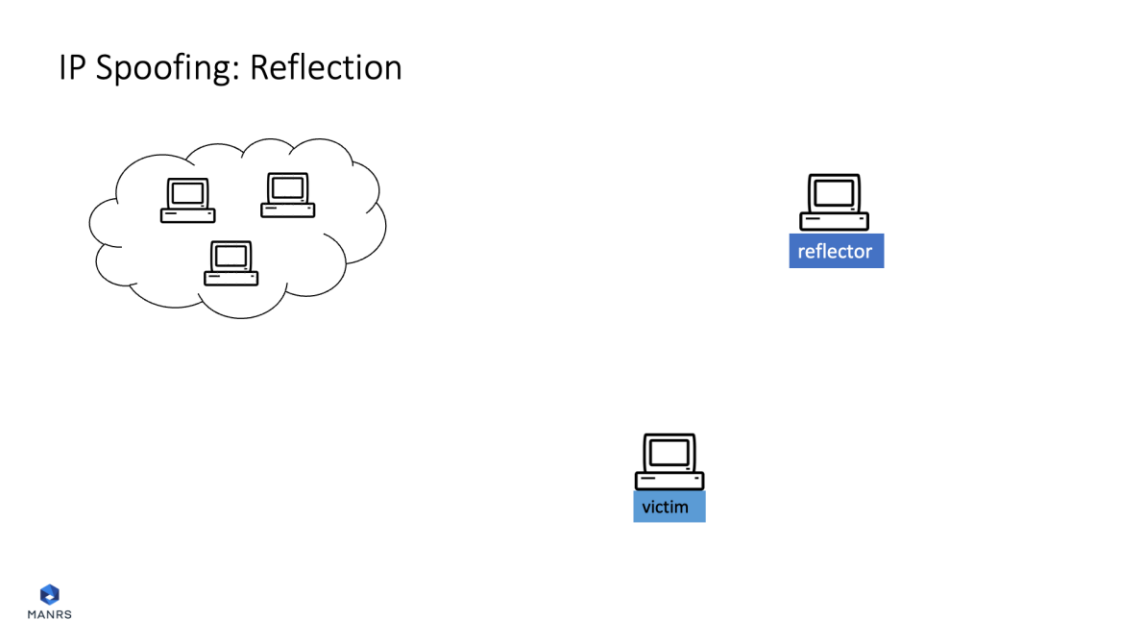


A network or attacker advertises illegitimate IP prefixes, which propagate across networks and lead to incorrect or suboptimal routing.

Result: Packets can be redirected through a path that could enable eavesdropping or traffic analysis.

Leaks can be malicious, but are often accidental misconfigurations.

Problem: IP Address Spoofing



Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another network.

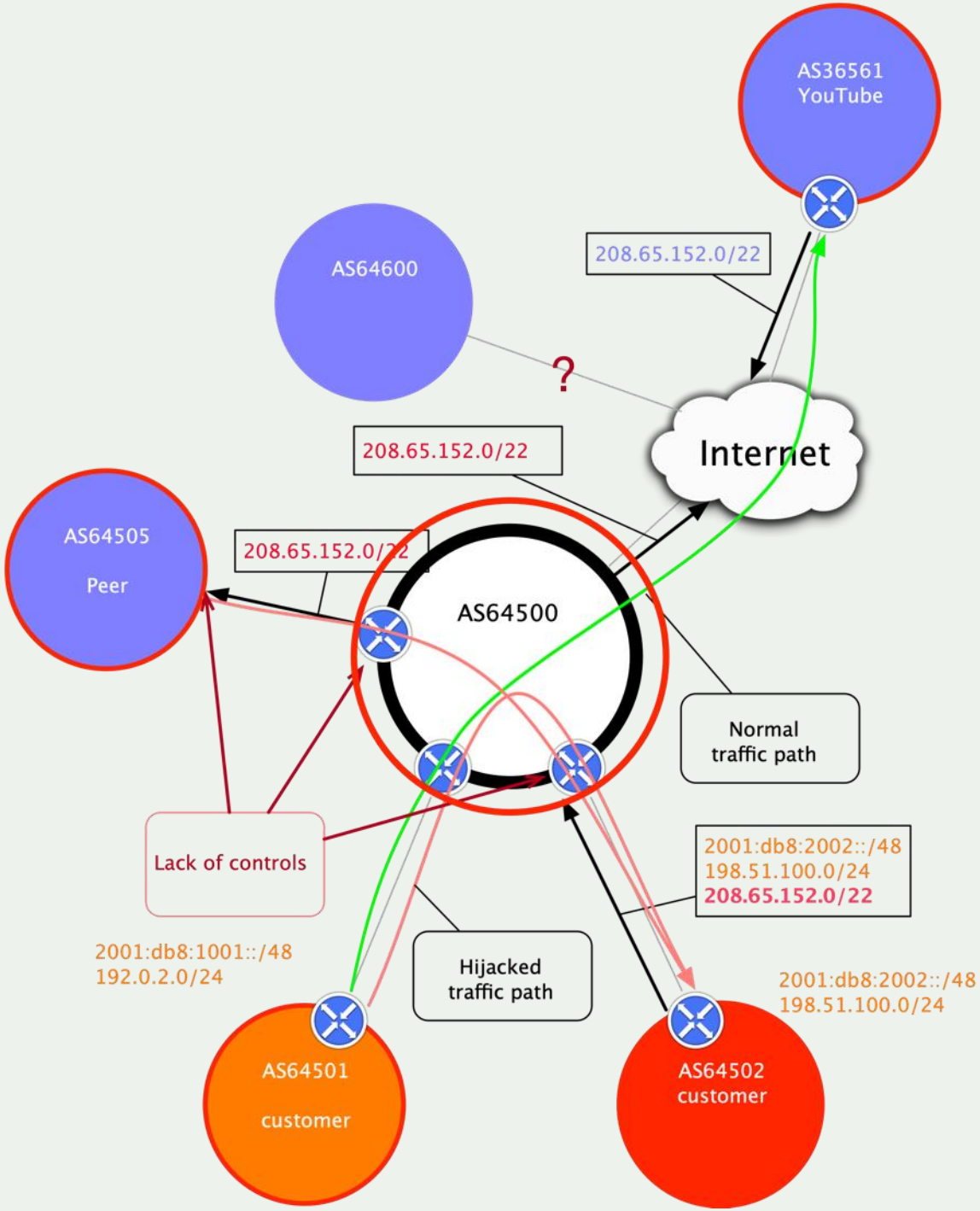
Result: Attackers magnify the amount of malicious traffic and obscure the sources of the attack traffic, causing a reflection DDoS attack.

Prefix/Route Hijacking

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

Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).

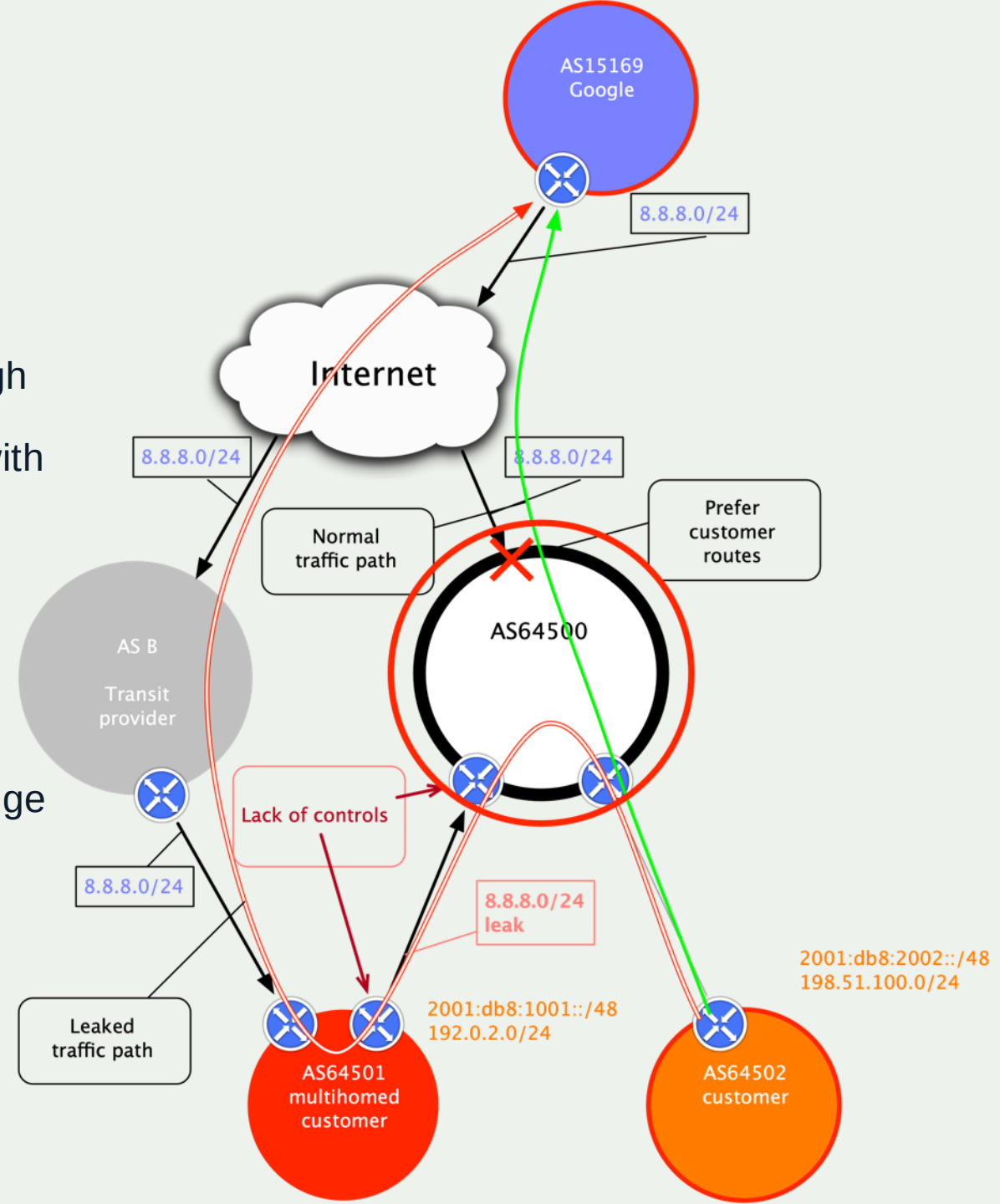


Route Leak

A route leak is where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is 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 through the network 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.

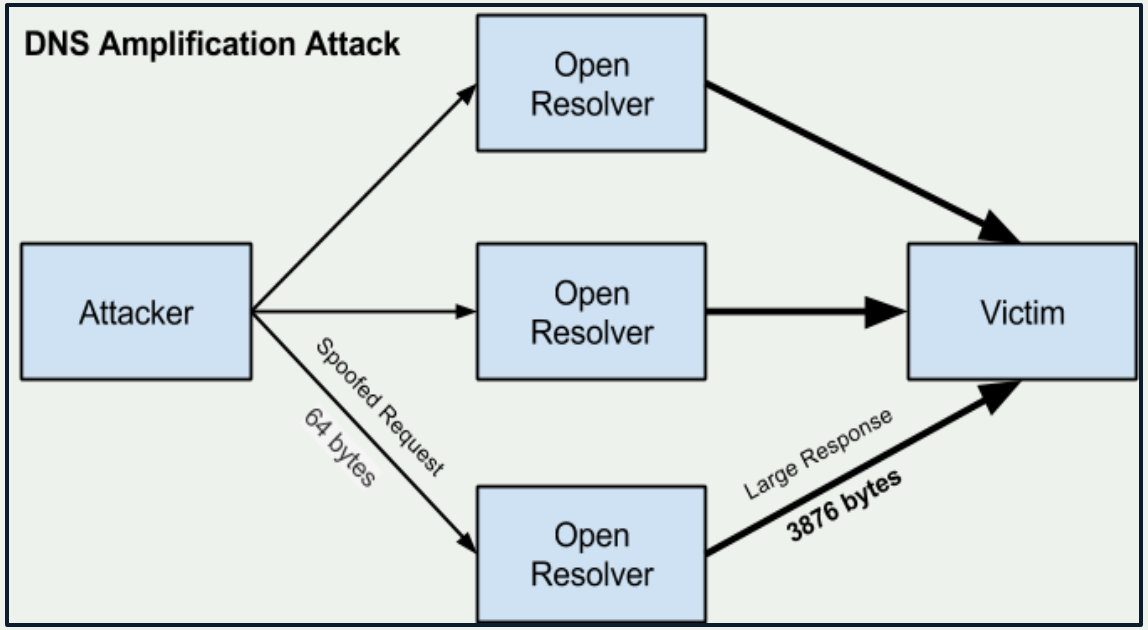
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).



IP Address Spoofing

IP address spoofing is used to hide the true identity of a 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 validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC

But…

- Not enough deployment
- Lack of reliable data

We need concerted action to improve routing security.

Why is Routing Security Hard?

Every network has a responsibility to implement basic routing security practices to mitigate threats.

But implementing best practices does not bring many immediate benefits. It costs time and money, and you probably can’t charge extra for it.

Even if you do everything right, your security is still in the hands of other networks.

This is a classic collective action problem.

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.

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

MANRS sets a new norm for routing security.

Mutually Agreed Norms for Routing Security (MANRS)

Industry-led initiative of 1000+ participating networks to implement best practices and collaborate toward a shared vision of a secure routing infrastructure.

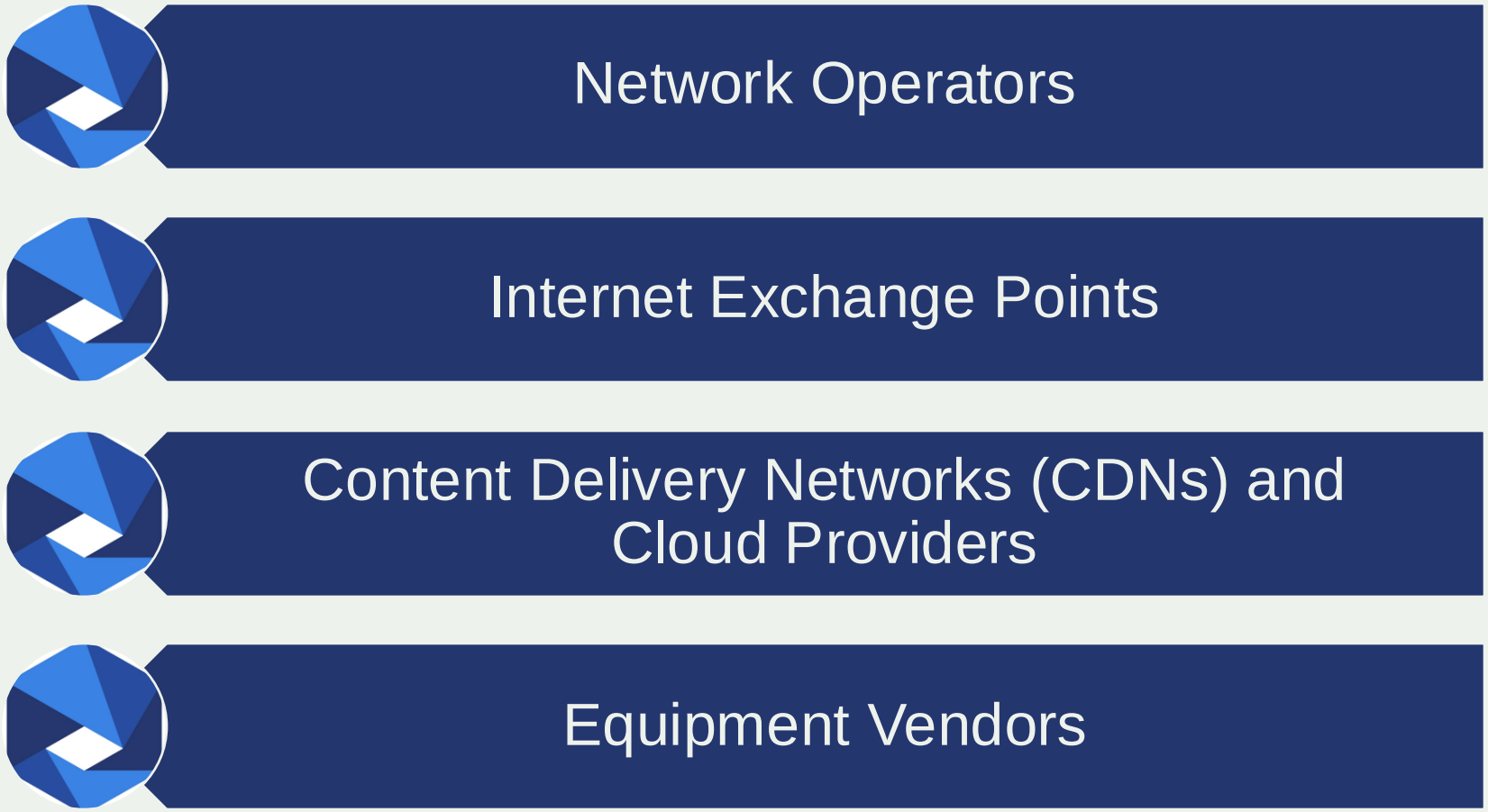
MANRS provides concrete actions for Network Operators, IXPs, CDN/Cloud Providers, and Equipment Vendors to reduce or eliminate the most common threats to routing.

There are no fees to join MANRS.

MANRS is supported by the Global Cyber Alliance.

MANRS

MANRS Programs



MANRS Actions

Filtering

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

Anti-spoofing

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

Coordination

Maintain globally accessible up-to-date contact information

Routing Information

Publish your information, so others can validate routing information on a global scale

Tools

Provide monitoring and debugging tools to help others

Promotion

Actively encourage MANRS adoption among peers, customers, and partners

MANRS Development Process

We are developing a formal process to guide how MANRS documents are developed, adopted, and maintained.

Objectives:

- Increase credibility, transparency and inclusiveness: a formal, documented mechanisms to develop and modify MANRS documentation (MANRS Actions, MANRS Charter…)
- Introduce a formal document series: this provides stable references and version control, making it easier to refer to it in external documents

The Business Case for MANRS and Routing Security

Implementing MANRS Actions

Signals an organization's security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

Reduces routing incidents, helping networks readily identify and address problems with customers or peers.

Improves network's operations by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Addresses many concerns of security-focused enterprises and other customers.

The Role of Routing in Supply Chain Security

85% of all ASes are origin-only networks. They fully depend on their connectivity provider for accessing their external digital assets and the Internet.

Despite being origin-only, most enterprise networks can contribute to a better routing security by:

- **Implementing routing security best practices** in their network infrastructure
- **Demanding proper routing security controls** from their connectivity and cloud providers

Is your connectivity or cloud provider the first line of defense… or your weakest link?

Everyone Benefits

Joining MANRS means joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

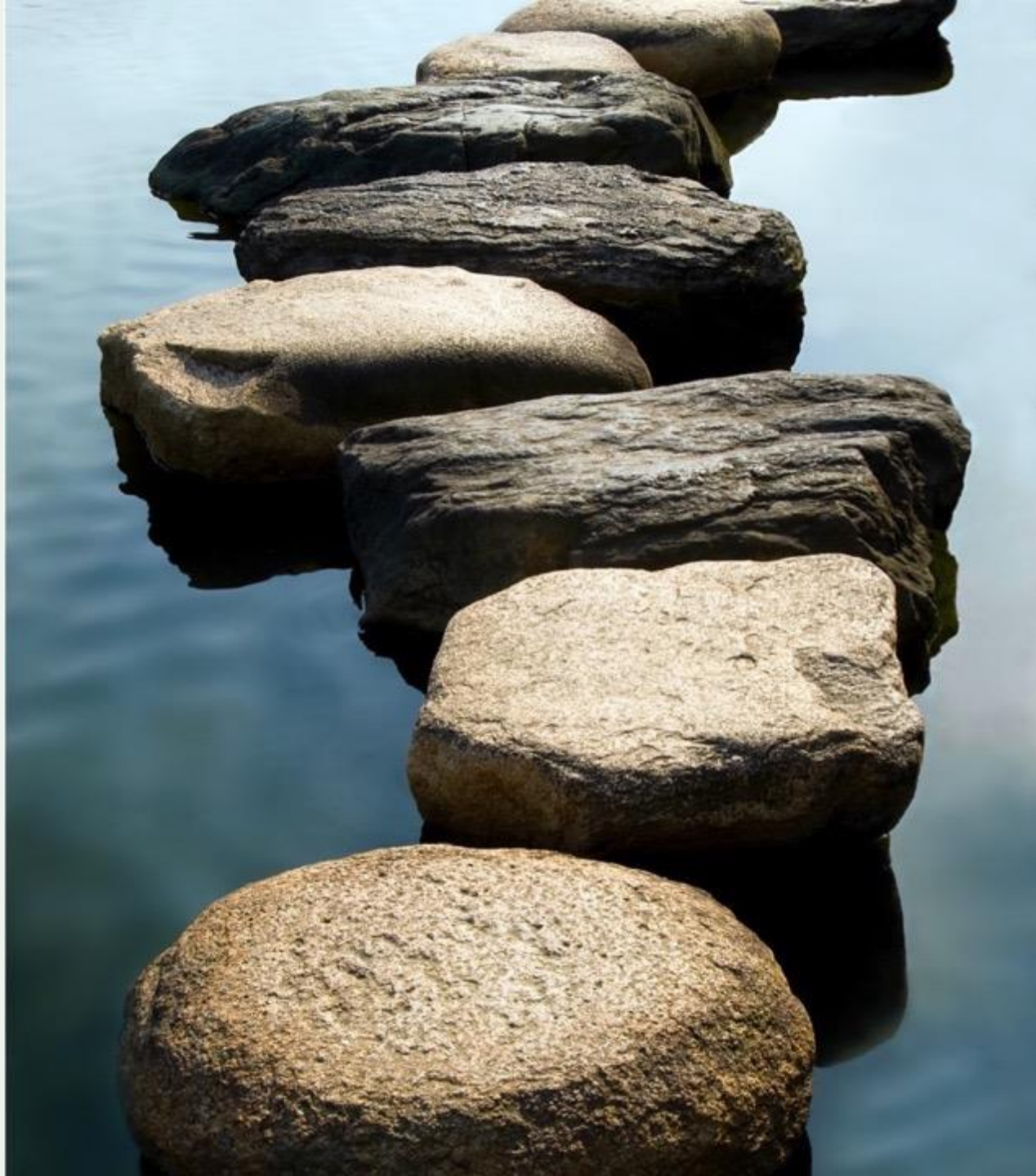
The more networks apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum a network should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure.



Why Service Providers Should Join MANRS

To help solve global network problems

- Lead by example to improve routing security and ensure a globally robust and secure routing infrastructure
- Strengthen enterprise security credentials

To add competitive value and differentiate in a flat, price-driven market

- Growing demand from enterprise customers for managed security services (info feeds)
- Signal security proficiency and commitment to your customers

To expand service portfolio - from a connectivity provider to a security partner

- Information feeds and other add-on services may increase revenue and reduce customer churn
- Enterprises indicate willingness to pay more for secure services

Why Enterprises Should Require MANRS

To improve your organizational security posture

- MANRS-ready infrastructure partners increase security and service reliability, while eliminating common outages or attacks
- Requiring MANRS adoption can help enterprises demonstrate due diligence and regulatory compliance

To prevent and address security incidents

- Preventing traffic hijacking, detouring, and malicious traffic helps prevent data loss, denial of service, reputational damage, and more
- Attacks and outages are resolved promptly by MANRS participants who are part of a broad network of security-minded operators

MANRS provides a foundation for value-added services

- Incident information sharing and information feeds can directly impact the bottom line
- Organizations can improve SLA compliance and address a host of routing deficiencies by simply seeking providers that adopt MANRS

Why Governments Should Promote MANRS

To drive the development or adoption of best practices across the country

- Encourage industry associations to develop or strengthen and promote existing voluntary codes of conduct for network operators.
- MANRS can serve as both a baseline set of best practices and as a foundation to complimentary voluntary codes of conduct.

To encourage the use of routing security as a competitive best practice

- Encourage local industry to better convey security to consumers and specify security during procurement practices.

To lead by example

- Improve infrastructure reliability and security by adopting best practices in their own networks.

Why Research & Education Networks Should Join MANRS

To show technical leadership and distinguish you from commercial ISPs

- Customers increasingly willing to pay more for secure services

To add competitive value and enhance operational effectiveness

- Growing demand from customers for managed security services

To show security proficiency and commitment to your customers

- Promote MANRS compliance to security-focused customers

To help solve global network problems

- NRENs are often early adopters of new developments. Lead by example and improve routing security for everyone
- Being part of the MANRS community can strengthen enterprise security credentials

MANRS Observatory

MANRS Observatory

Provides a factual state of security and resilience of the Internet routing system and tracks it over time

Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how

MANRS Observatory Access

Launched in 2019

Uses trusted, publicly available third-party data

Anyone may view aggregated data

Only MANRS Participants have access to detailed data about their own network(s)

Caveats:

- There are still some false positives
- Lack of security controls is not always visible

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH September 2019 RIR REGIONS APNIC

Overview

State of Routing Security

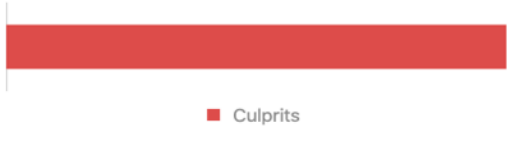
Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

Total		
398	*Route misoriginations*	68
	Route leaks	51
	Bogon announcements	279

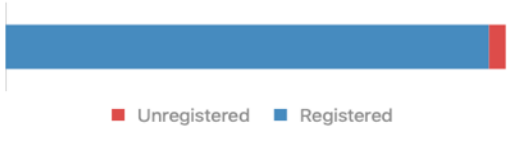
Culprits

Total		
180	*Culprits*	180



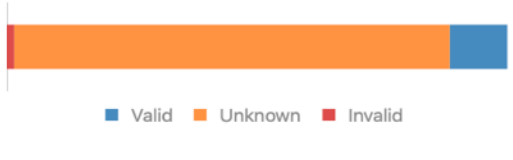
Routing completeness (IRR)

Total		
100%	*Unregistered*	3%
	Registered	97%



Routing completeness (RPKI)

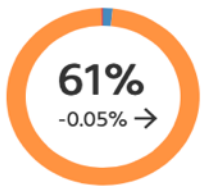
Total		
100%	*Valid*	12%
	Unknown	87%
	Invalid	1%



MANRS Readiness

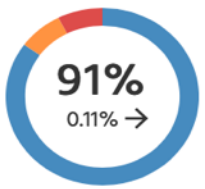
Filtering

Anti-spoofing



Coordination

Global Validation IRR



Global Validation RPKI

Ready Aspiring Lagging

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

Filtering

Anti-spoofing

Coordination

Global Validation IRR

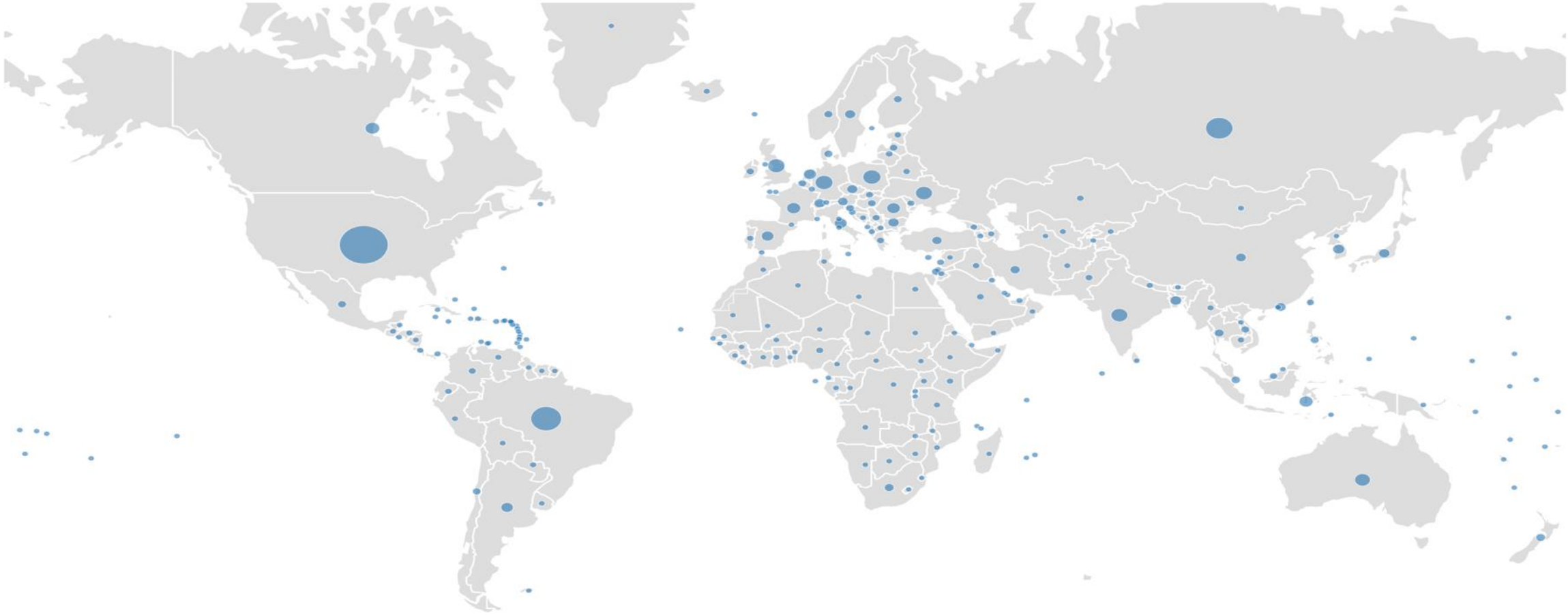
Global Validation RPKI

Ready Aspiring Lagging

Global view

Size: Count | Incidents | Culprits

Region: Country | UN Regions | UN Sub-Regions | RIR Regions



An Elevated Tier of MANRS Participation

MANRS has traditionally focused on peer-to-peer relationships between network operators, but we believe customer demand can be a driving force in increasing routing security.

If we can enhance the business case for MANRS, customers will demand better routing security of their network connectivity providers and providers will ensure they're complying with the MANRS Actions that mitigate routing security risks.

The **MANRS+ Working Group** explores the idea of creating a second, elevated tier of MANRS participation for organizations that comply with more stringent requirements and auditing. The working group is tasked with developing the requirements for MANRS+.

Meet MANRS+

A framework for routing security, an essential part of **supply chain security**

Focus on the demands of **enterprise customers** in various industry sectors

Extended set of requirements, covering a broader set of risks related to routing and traffic security

Conditioned to be included in / referenced from **common infosec frameworks**:

- ***Stronger and more detailed requirements*** enforcing best practices in traffic security
- ***High level of assurance of conformance***; this includes more profound technical audit and process audit

Developed in a transparent and inclusive manner using the MANRS Development Process (MDP)

The Control Matrix

What Should Enterprises Require from their Connectivity Provider?

Routing Security
7 Controls

DDoS Attack Mitigation
4 Controls

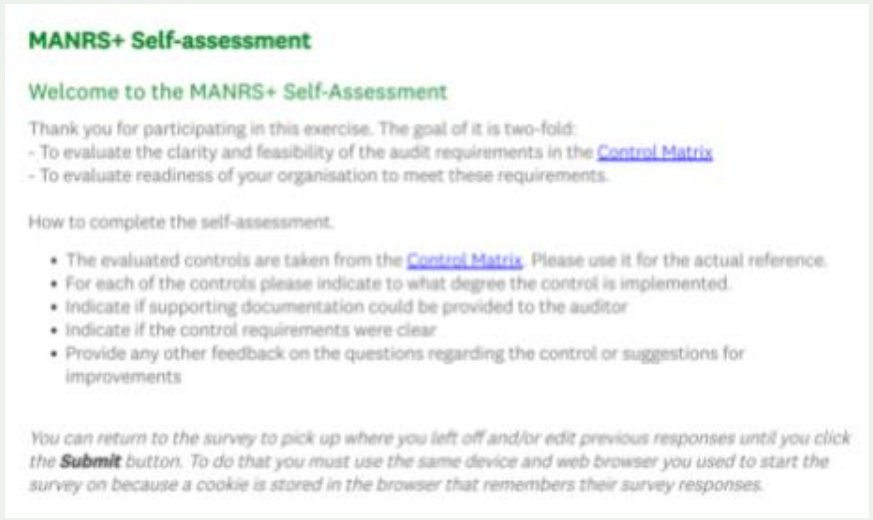
Anti-spoofing Protection
2 Controls

Maintaining Routing Info.
3 Controls

Global Communication
1 Control

Security Services
3 Controls

Self-Assessment Survey



MANRS+ Self-assessment

Welcome to the MANRS+ Self-Assessment

Thank you for participating in this exercise. The goal of it is two-fold:
- To evaluate the clarity and feasibility of the audit requirements in the Control Matrix
- To evaluate readiness of your organisation to meet these requirements.

How to complete the self-assessment.

- The evaluated controls are taken from the Control Matrix. Please use it for the actual reference.
- For each of the controls please indicate to what degree the control is implemented.
- Indicate if supporting documentation could be provided to the auditor
- Indicate if the control requirements were clear
- Provide any other feedback on the questions regarding the control or suggestions for improvements

*You can return to the survey to pick up where you left off and/or edit previous responses until you click the **Submit** button. To do that you must use the same device and web browser you used to start the survey on because a cookie is stored in the browser that remembers their survey responses.*

Objectives:

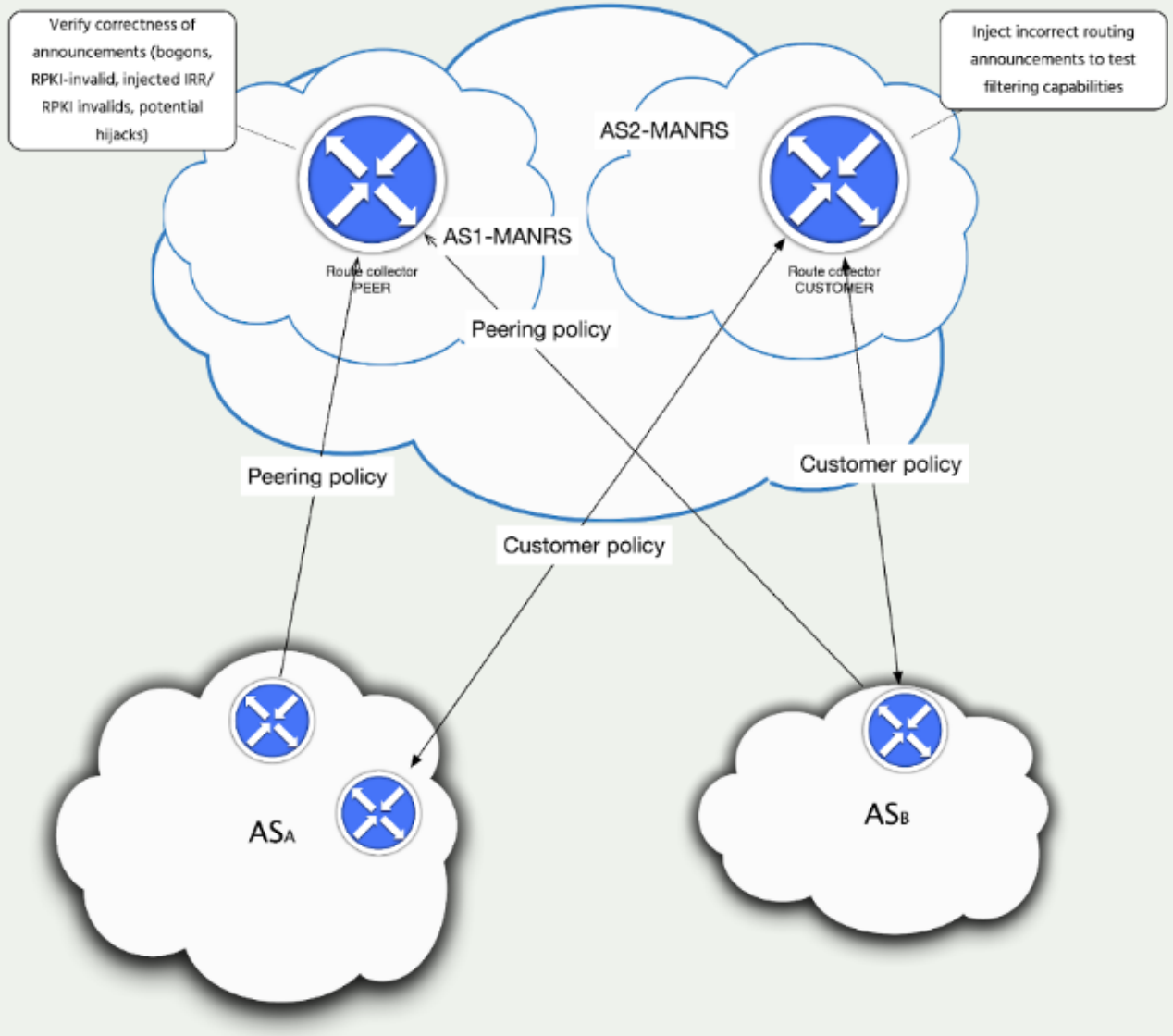
- To evaluate the clarity and feasibility of the audit requirements in the Control Matrix
- To evaluate readiness of your organization to meet these requirements
- Basis for the future application form
- The self-assessment survey is online:
- https://www.surveymonkey.com/r/86GGHC5

Future MANRS+ Work

Gather **interested organizations** among connectivity providers and enterprises

Develop a **prototype** and deploy the **enhanced measurement infrastructure**

Work on the **inclusion in common infosec frameworks** (eg.: M3AAWG Internet Routing Security Profile based on NIST CSF)

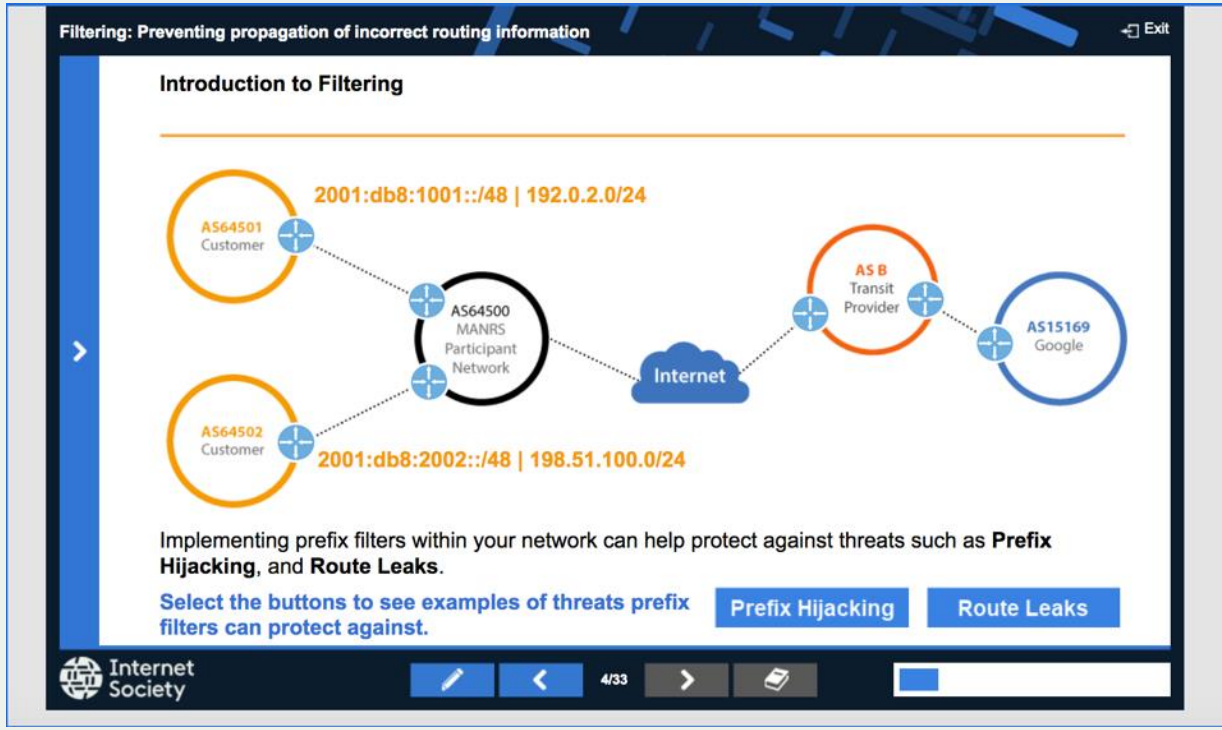


Learn More and Join Us

Help Is Available

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

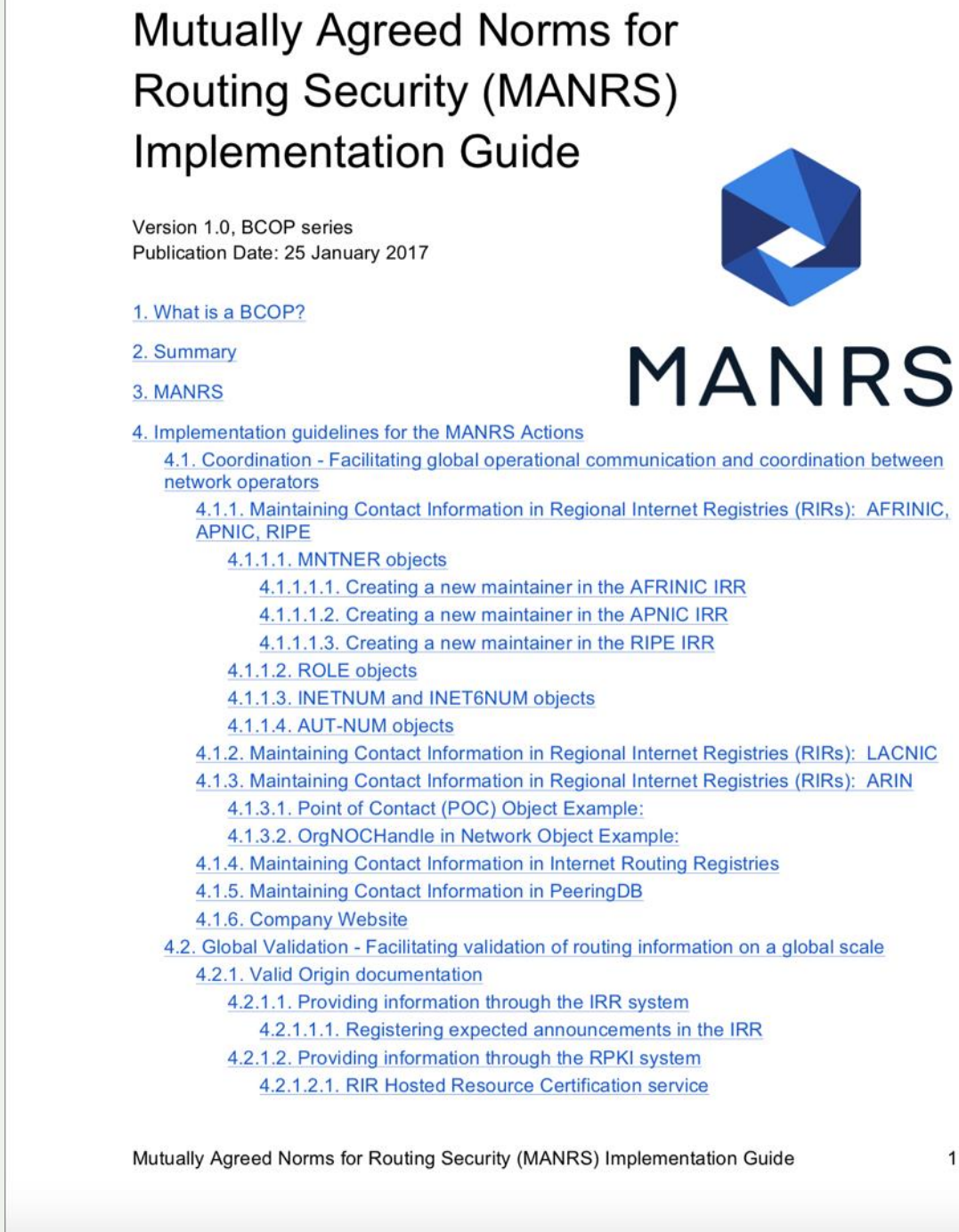
- **Implementation Guide** based on Best Current Operational Practices deployed by network operators around the world
- **Tutorial modules** based on information in the Implementation Guide.



MANRS Implementation Guide for Network Operators

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
- Recognition from the RIPE community by being published as RIPE-706
- 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

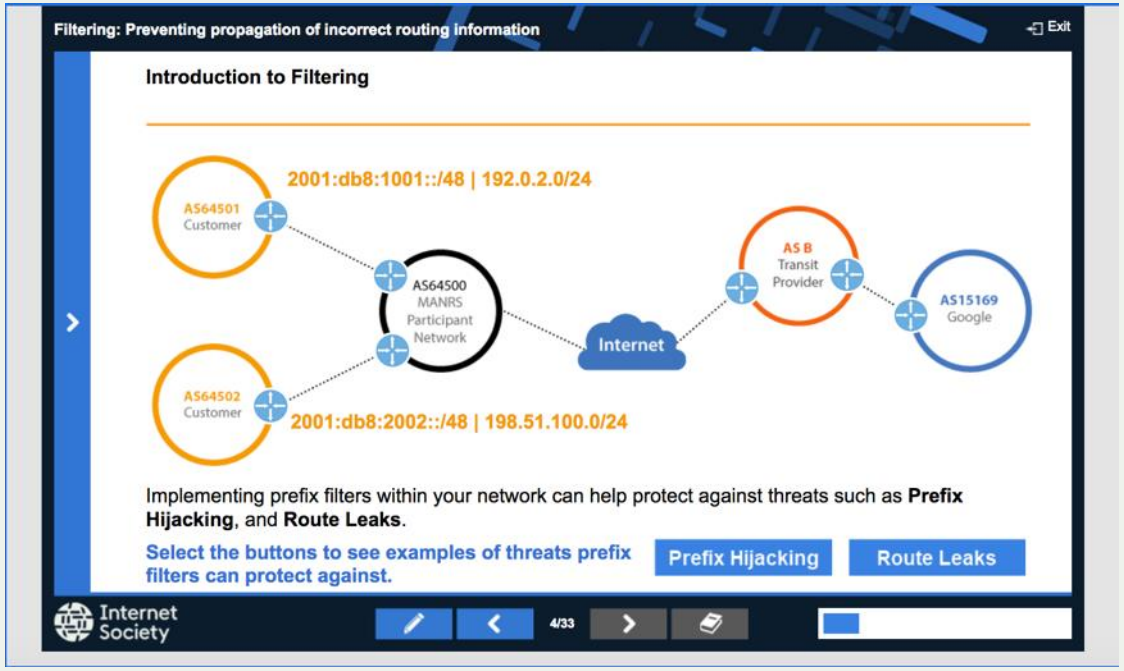
MANRS Tutorials

Tutorials 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://www.manrs.org/tutorials



MANRS

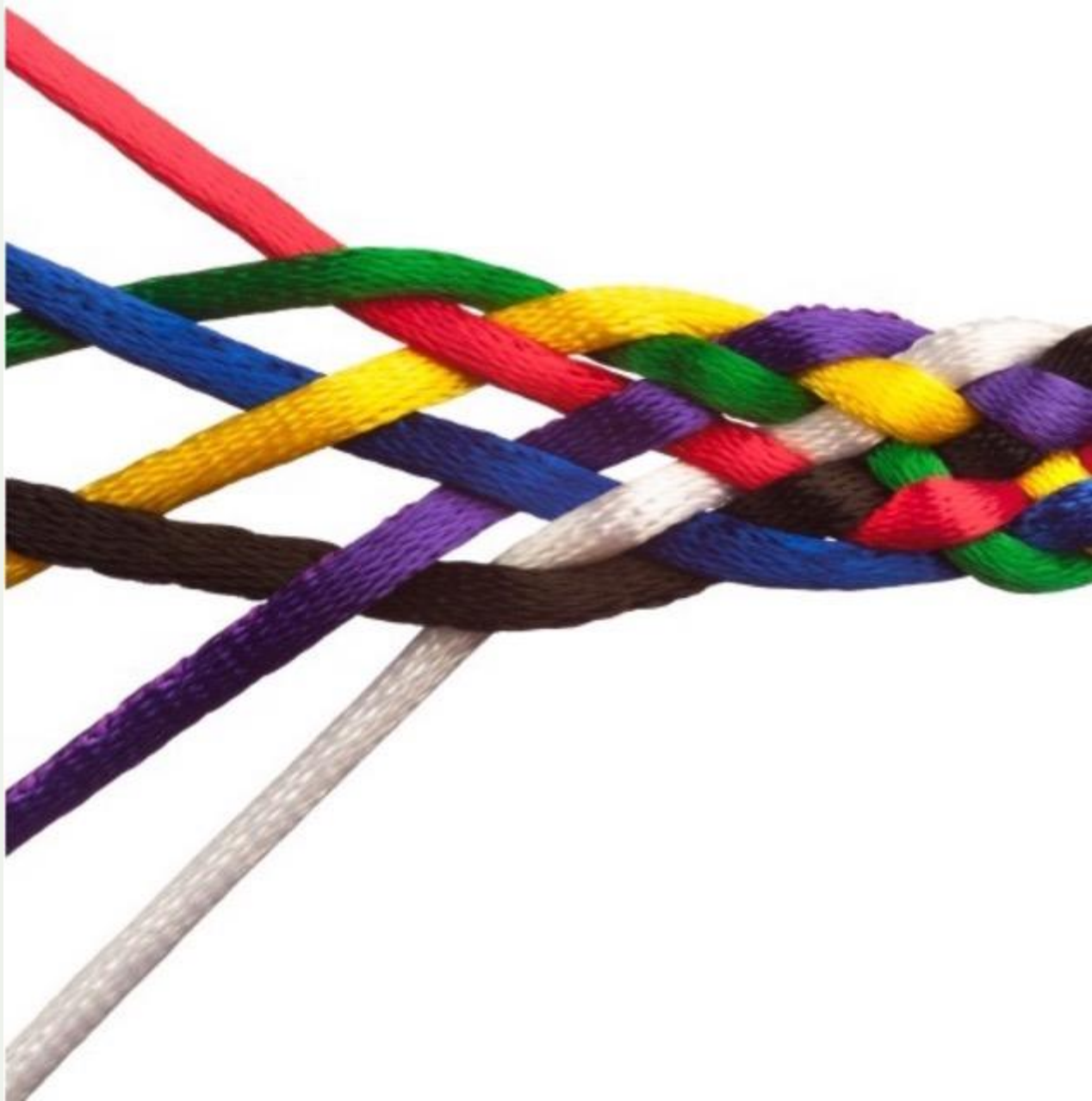
Join Us

Visit https://www.manrs.org/join

- Fill out the form with as much detail as possible.
- We will 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 documents and promote MANRS objectives



LEARN MORE:

https://www.manrs.org

FOLLOW US:

/RoutingMANRS

Thank you.

NAME

EMAIL

manrs.org