How to use this template:

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

1. Opening the 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 manrs@isoc.org

MANRS

Mutually Agreed Norms for Routing Security

NAME

EMAIL

Why Does Routing Security Matter?

A Routing Overview

The Basics: How Routing Works

There are ~70,000 core 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

- Created before security was a concern
- Assumes all networks are trustworthy
- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

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.

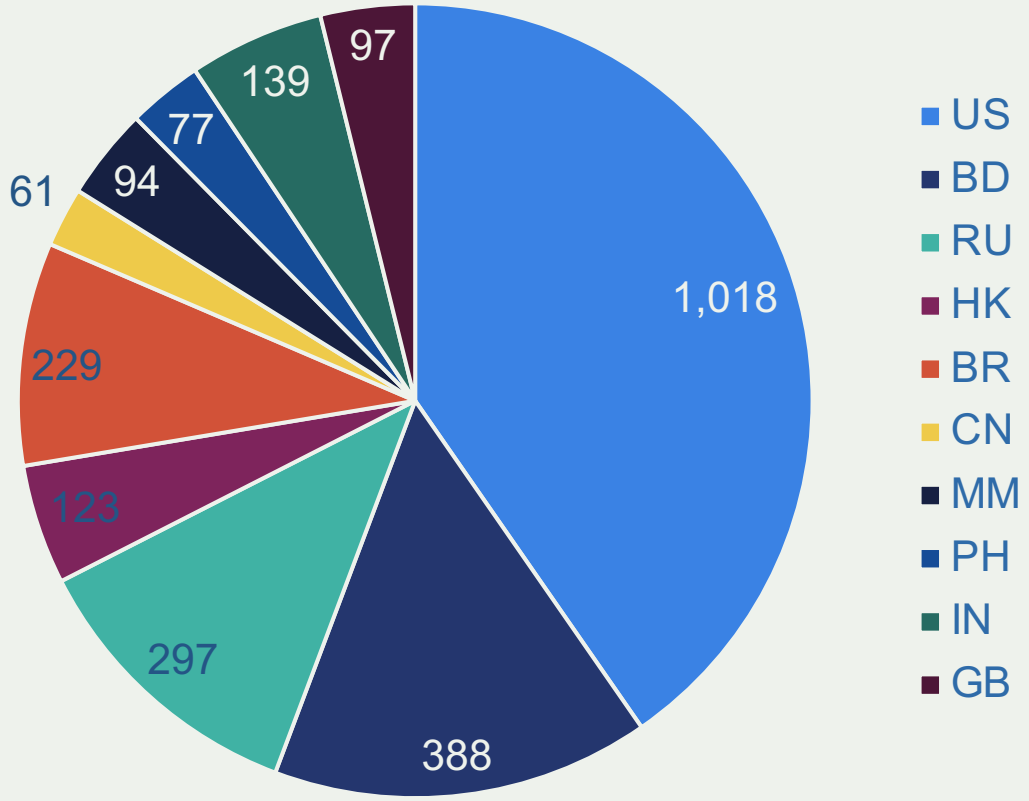
About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet were affected.

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

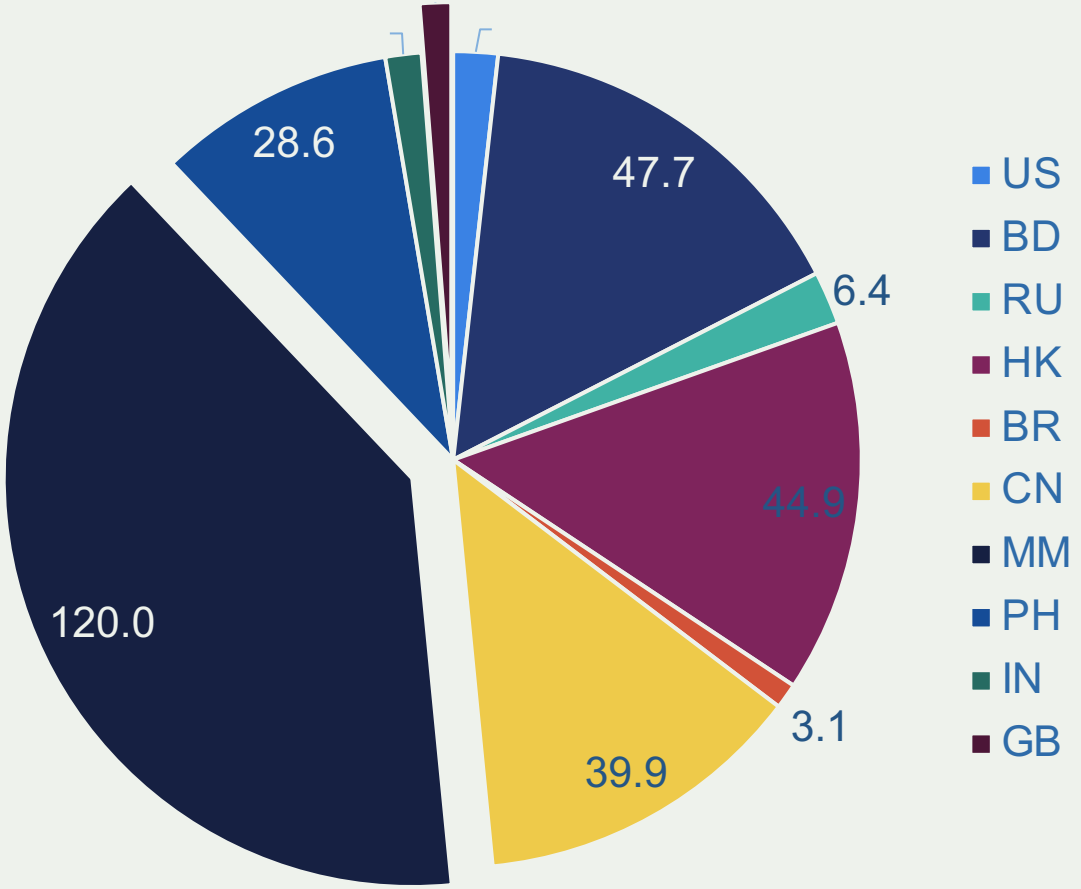
https://www.manrs.org/2019/02/routing-security-getting-better-but-no-reason-to-rest/

Routing Incidents Happen Everywhere

Number of incidents (a route leak or hijack) that affected networks in a country



Incidents (a route leak or hijack) in a country, normalized by the number of advertised ASNs (top 10)



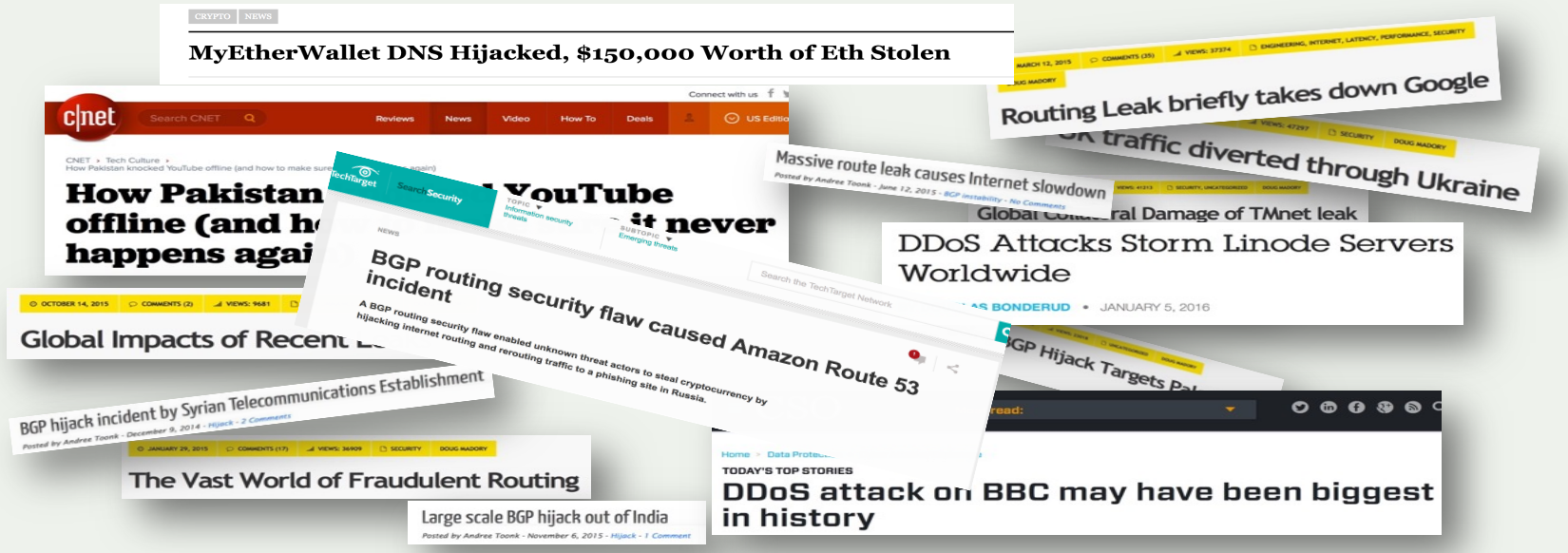
(Based on MANRS Observatory data)

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?

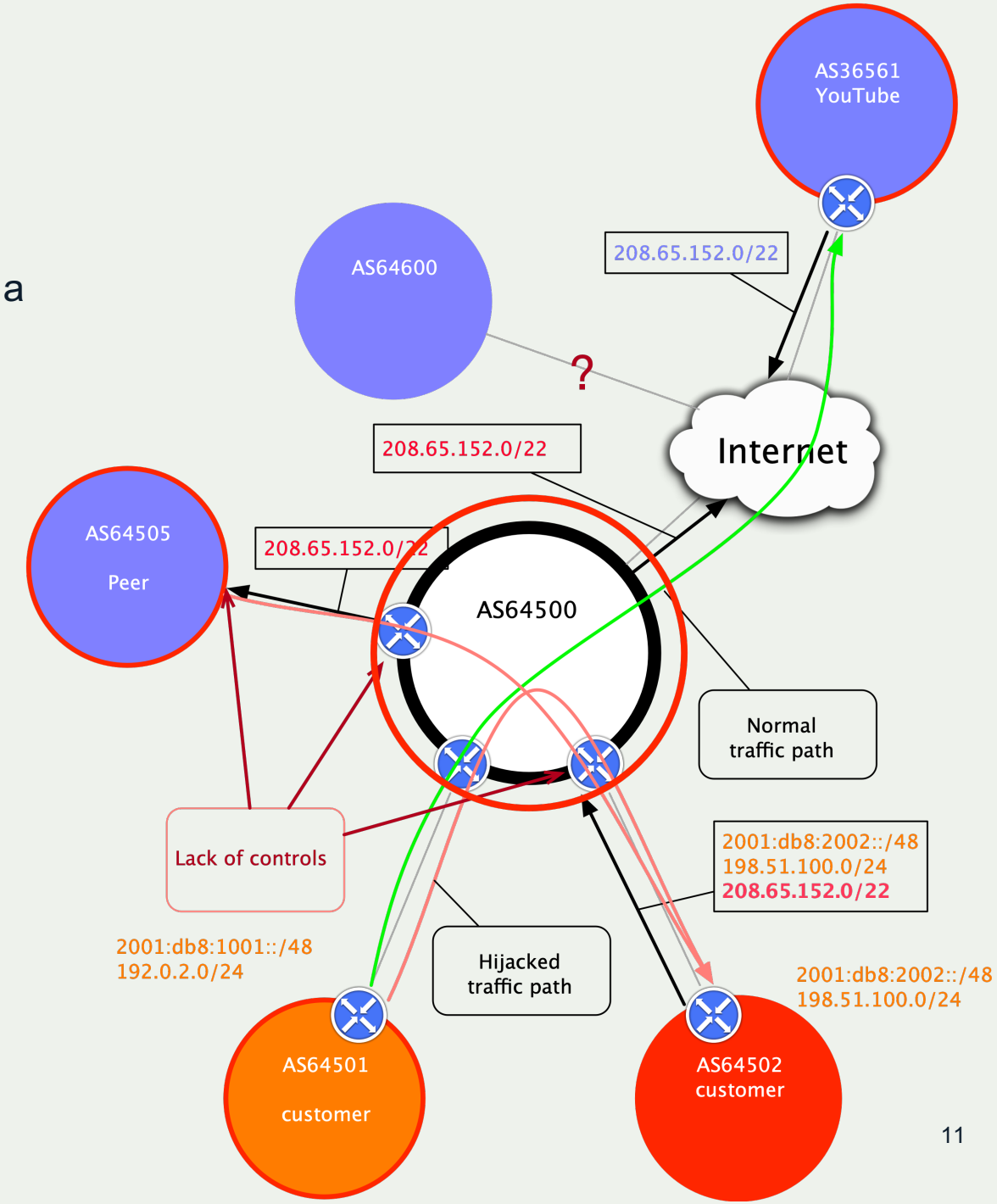
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place; this can cause Denial of Service (DoS) attacks or traffic interception.	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

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).

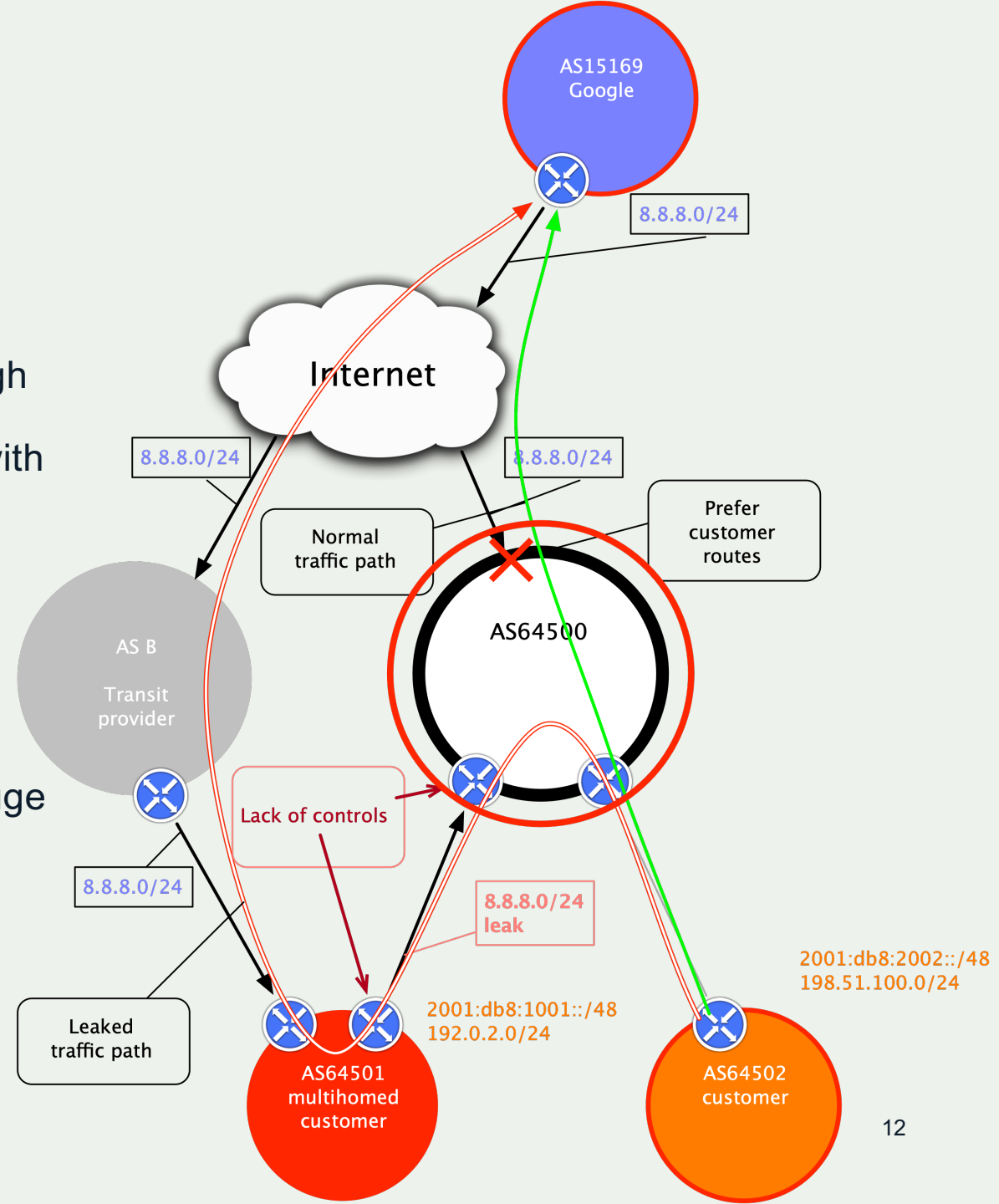


Route Leak

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.

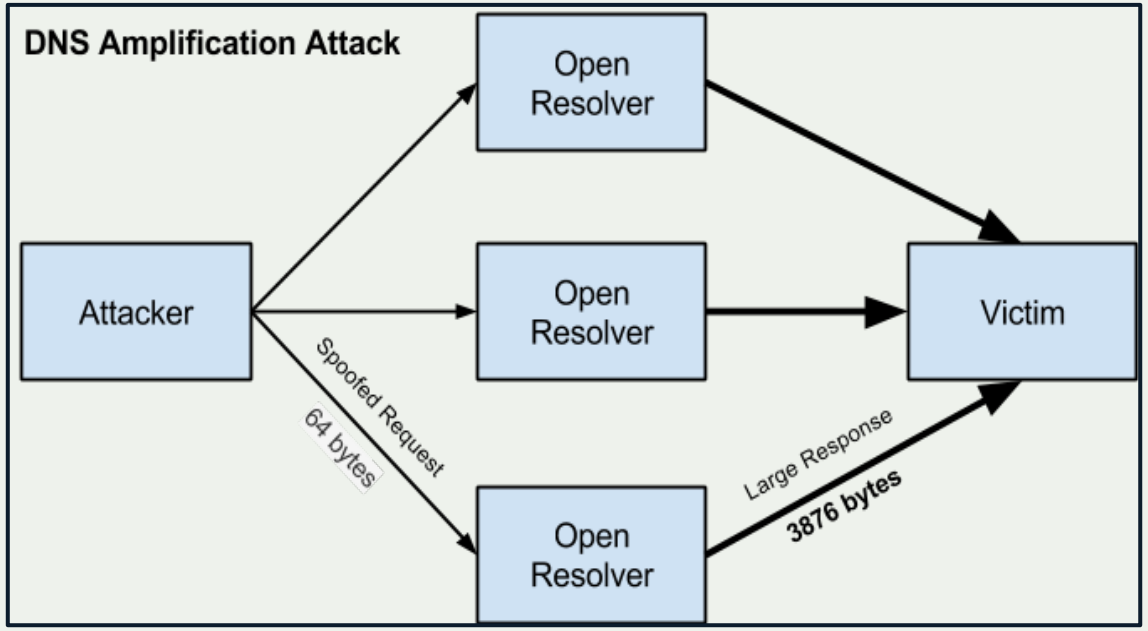
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).



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.

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.

MANRS Programmes

- Network Operators
- Internet Exchange Points
- Content Delivery Networks (CDNs) and Cloud Providers

MANRS Network Operators Programme

Launched in 2014 by a handful of network operators with the following goals:

- Raise awareness of routing security problems and encourage the implementation of actions that can address them.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.
- Demonstrate the ability of the Internet industry to address routing security problems.
- Provide a framework for network operators to better understand and address issues relating to the security and resilience of the Internet's global routing system.

MANRS Actions for 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

Blue shading = Mandatory Action

MANRS IXP Programme

Internet Exchange Points (IXPs) are a collaborative focal point to discuss and promote the importance of routing security.

Launched in 2018, the IXP Programme addresses the unique needs and concerns of IXPs with a separate set of MANRS actions.

IXPs can implement actions that demonstrate their commitment to routing security and bring significant improvement to the resilience and security of their peering relationships.

MANRS Actions for Internet Exchange Points

Action 1
Prevent propagation of incorrect routing information

Implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2
Promote MANRS to the IXP membership

Provide encouragement or assistance for IXP members to implement MANRS actions.

Action 3
Protect the peering platform

Have a published policy of traffic not allowed on the peering fabric and perform filtering of such traffic.

Action 4
Facilitate global operational communication and coordination

Facilitate communication among members by providing necessary mailing lists and member directories.

Action 5
Provide monitoring and debugging tools to the members.

Provide a looking glass for IXP members.

Blue shading = Mandatory Action

MANRS CDN and Cloud Programme

Launched in 2020, the CDN and Cloud Provider Programme helps by requiring egress routing controls so networks can prevent incidents from happening.

Leveraging CDNs' and cloud providers' peering power can have significant positive spillover effect on the routing hygiene of networks they peer with.

Goals include:

- Create a secure network peering environment
- Encourage better routing hygiene from peering partners
- Demonstrate responsible behavior
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting

MANRS Actions for CDNs & Cloud Providers

Action 1
Prevent propagation of incorrect routing information

Ensure correctness of own announcements and of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.

Action 2
Prevent traffic with illegitimate source IP addresses

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

Action 3
Facilitate global operational communication and coordination

Maintain globally accessible, up-to-date contact information in PeeringDB and relevant RIR databases.

Action 4
Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties (IRR and/or RPKI)

Action 5
Encourage MANRS adoption

Actively encourage MANRS adoption among the peers.

Action 6
Provide monitoring and debugging tools to the peering partners

Provide a mechanism to inform peering partners if announcements did not meet the requirements of the peering policy.

Blue shading = Mandatory Action

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.

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

Provide a factual state of security and resilience of the Internet routing system and track 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

Publicly launched in August 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

Caveats:

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

MONTH September 2019 RIR REGIONS APNIC

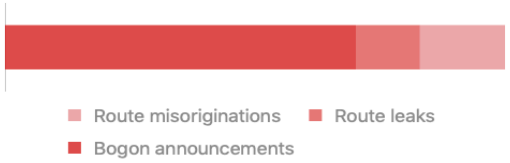
Overview

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

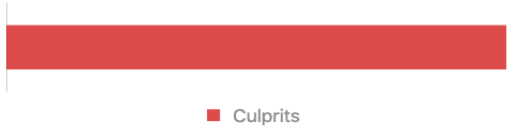
Incidents

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



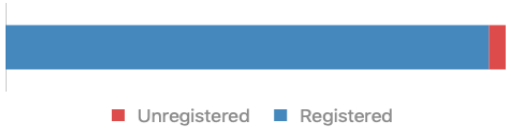
Culprits

Total		
180	*Culprits*	180



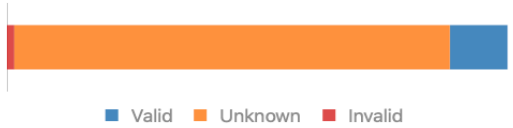
Routing completeness (IRR)

Total		
100%	*Unregistered*	3%
	Registered	97%



Routing completeness (RPKI)

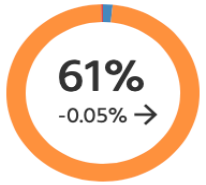
Total		
100%	*Valid*	12%
	Unknown	87%
	Invalid	1%



MANRS Readiness

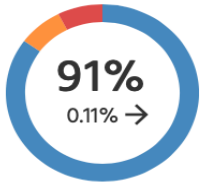
Filtering

Anti-spoofing



Coordination

Global Validation IRR



Global Validation RPKI

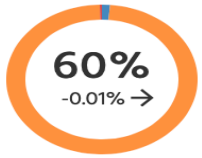
Ready Aspiring Lagging

MANRS Observatory

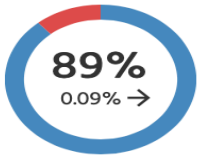
OVERVIEW HISTORY COMPARISON ABOUT

Filtering

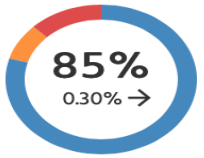
Anti-spoofing



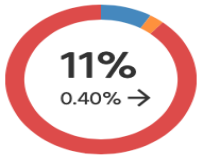
Coordination



Global Validation IRR



Global Validation RPKI

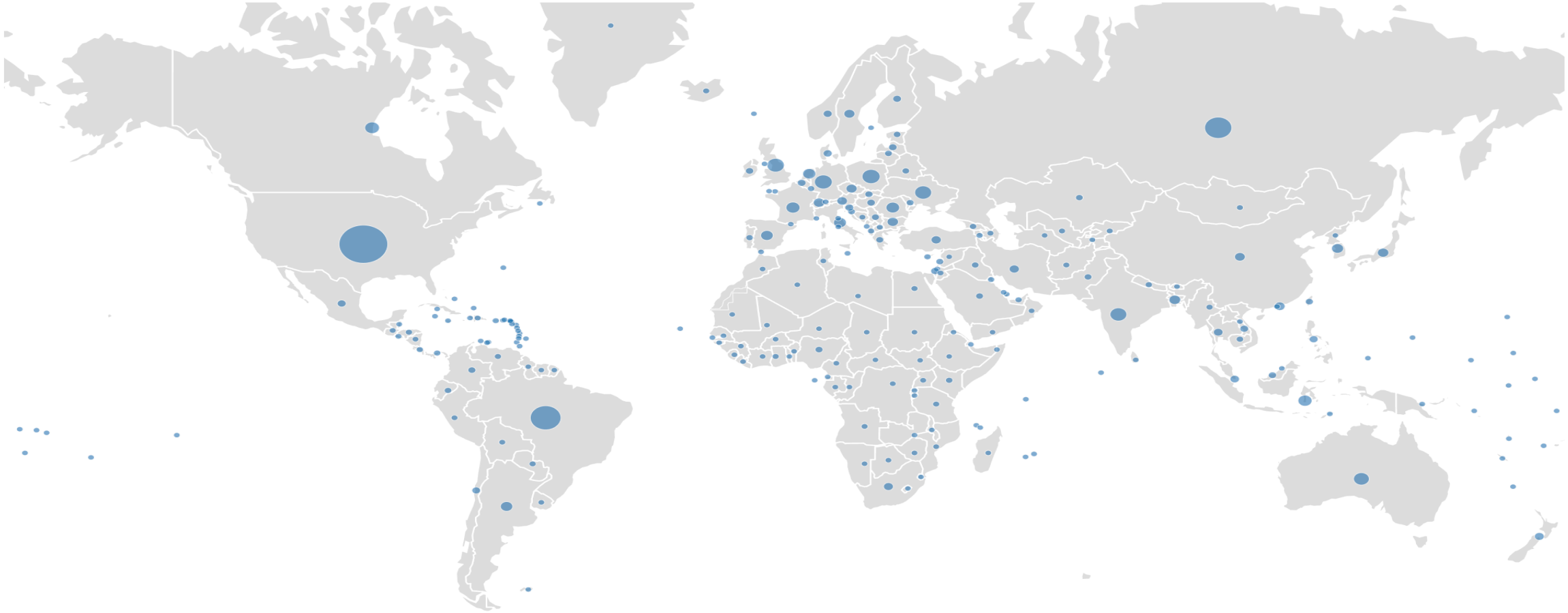


Ready Aspiring Lagging

Global view

Size: Count | Incidents | Culprits

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



MANRS Ambassadors and Fellows

Overview

Launched in 2020, Ambassadors and Fellows make the global routing infrastructure more robust and secure.

They work in one of three categories: training, research, or policy.

Ambassadors are representatives from current MANRS participants who provide mentorship, guidance, and feedback to others in the routing security community.

Fellows are emerging leaders who believe that routing security is essential and are ready to contribute to its improvement.

MANRS Ambassadors

Support the Fellows

Provide mentorship and guidance to help Fellows fulfill their obligations

Promote MANRS

Generate awareness in local and regional communities through speaking, writing, and promoting routing security

Capacity building

Contribute to building the MANRS community through moderating training courses, coordinating with Ambassadors in other regions, providing technical assistance to network operators, and more

MANRS Fellows

Training

Develop, plan, improve, and conduct tutorials and trainings/workshops

Research

Analyze routing incidents that significantly impact the Internet

Policy

Review and provide feedback on existing policy documents regarding issues that can be addressed through MANRS actions; improve existing policy documents for MANRS

Promote MANRS

Develop content, highlight MANRS and routing security via social media, promote in local communities.

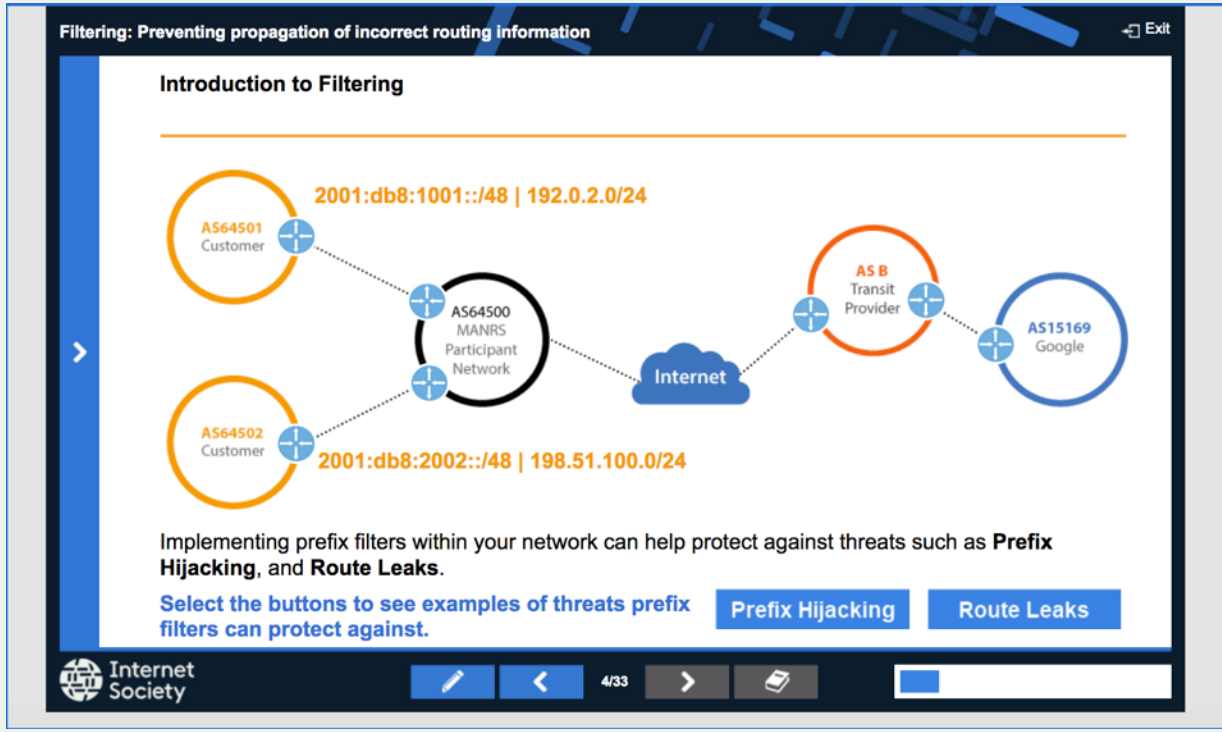
Learn More and Join Us

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

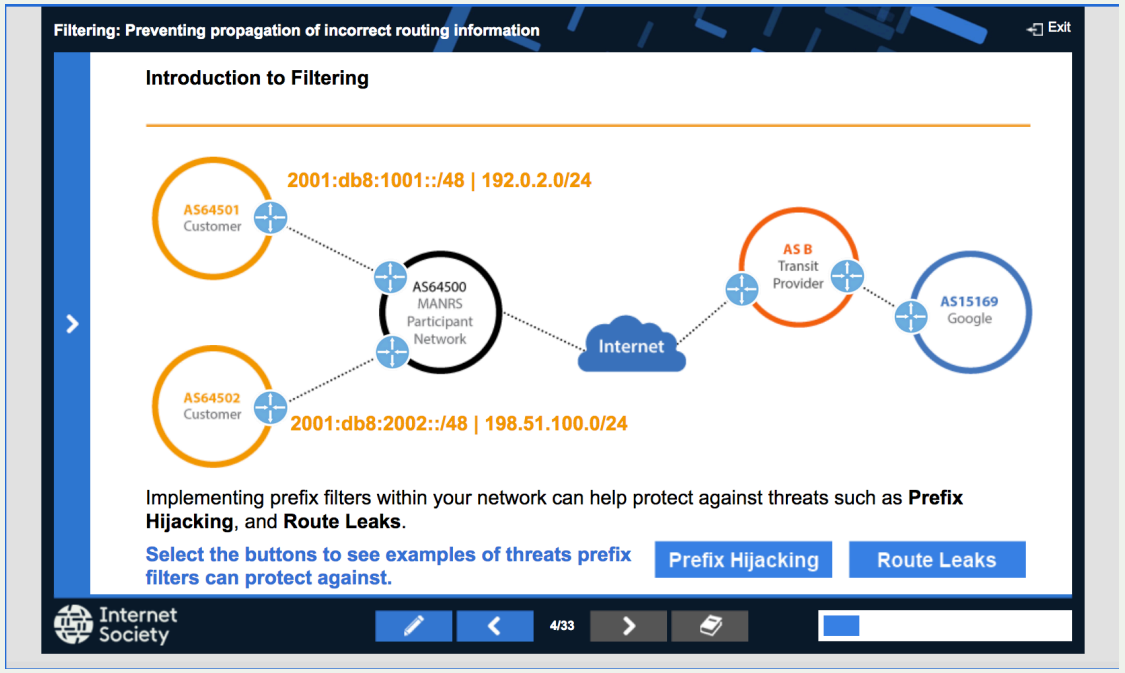
MANRS Tutorials

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

- 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