Internet Society
Armenia Chapter

MANRS

Webinar: 05.30.2020

Name: Valeri Stepanyan

Email: valery@aua.am

COVID 19 – Stay at home. Be healthy.

MANRS

Internet Society Armenia Chapter

Networks & Internet : interconnection of networks, incidents, attacks.

- The overall volume of data is expected to reach 44 zettabytes by 2020.

  ZB zettabyte : $1\ 000^7$ octets

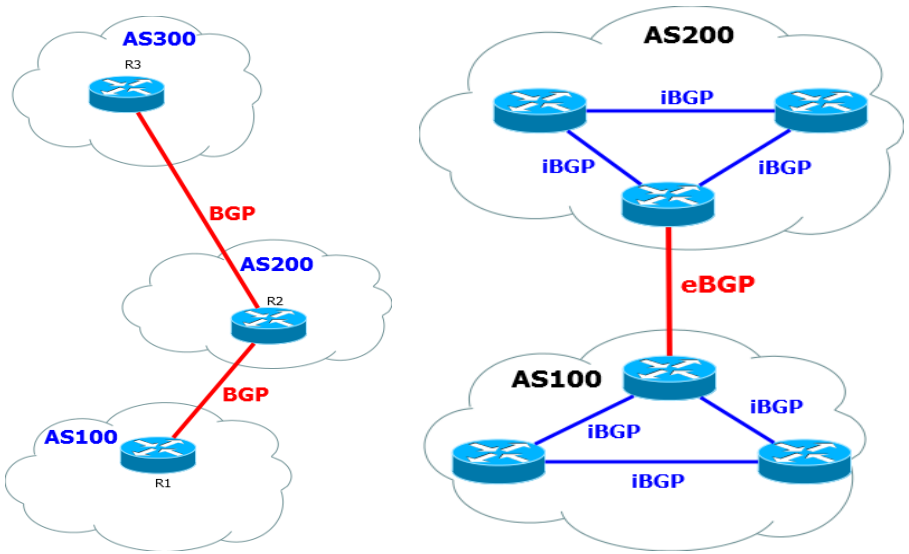
  1 000 000 000 000 000 000 000 Bytes
- There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.
- In 2017 alone, 14,000 routing outages or attacks such as hijacking, leaks, and spoofing -led to a range of problems including stolen data, lost revenue, reputational damage, and more.
- About 40% of all network incidents are attacks, with the mean duration per incident lasting 19 hours.
- Incidents are global in scale, with one operator's routing problems cascading to impact others.

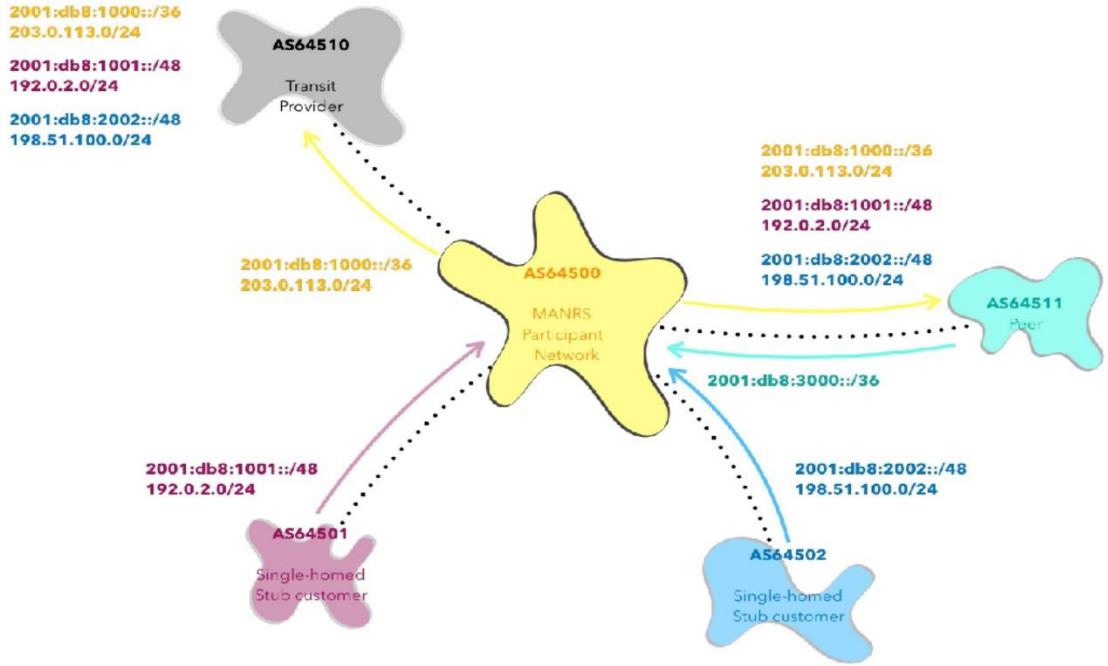
MANRS

Internet Society Armenia Chapter

Routers, connections. How routing works?

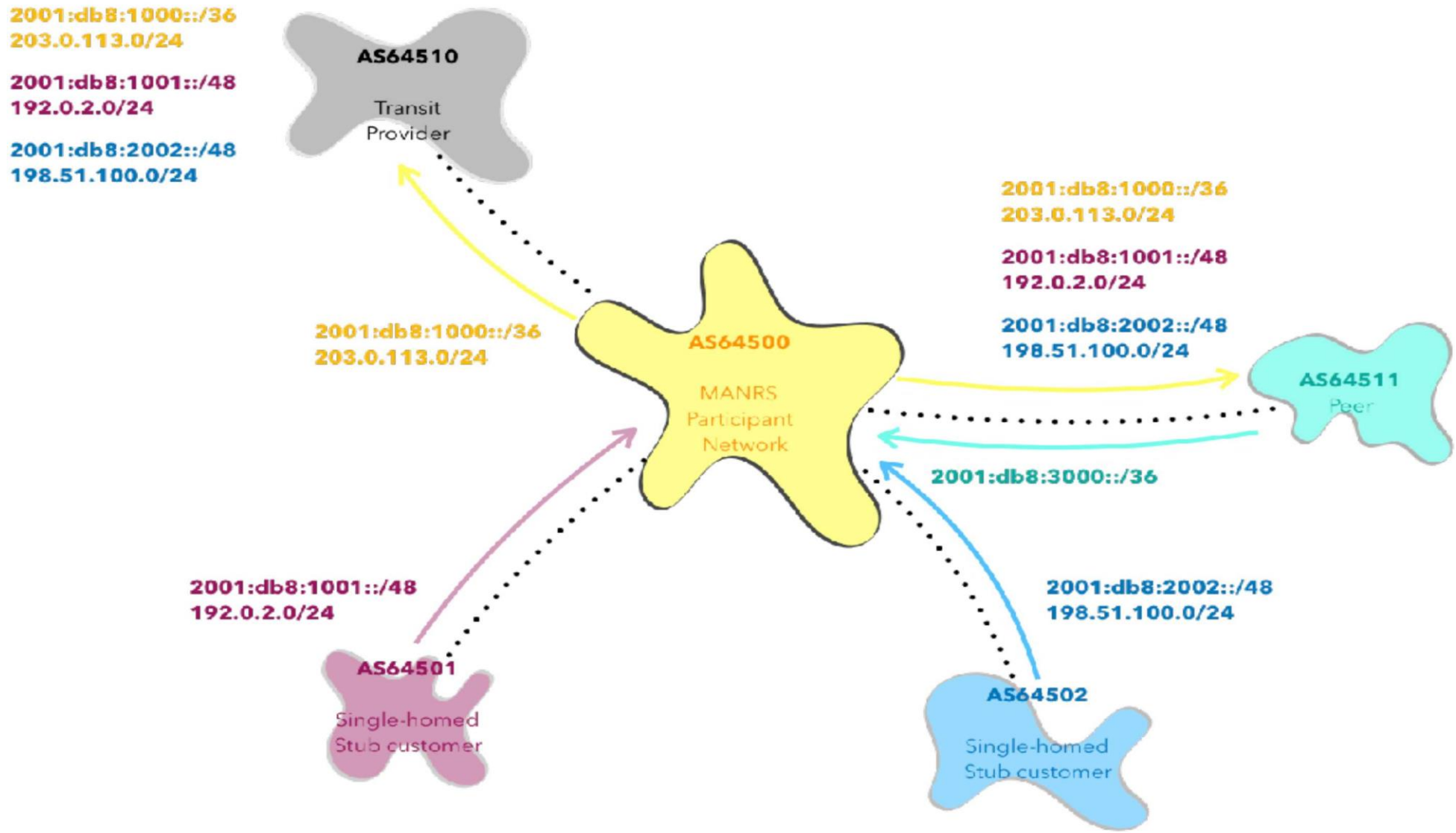
- **Routers use Border Gateway Protocol (BGP) to exchange "reachability information" - networks they know how to reach.**
- **Routers build a "routing table" and pick the best route when sending a packet, typically based on the shortest path.**





MANRS

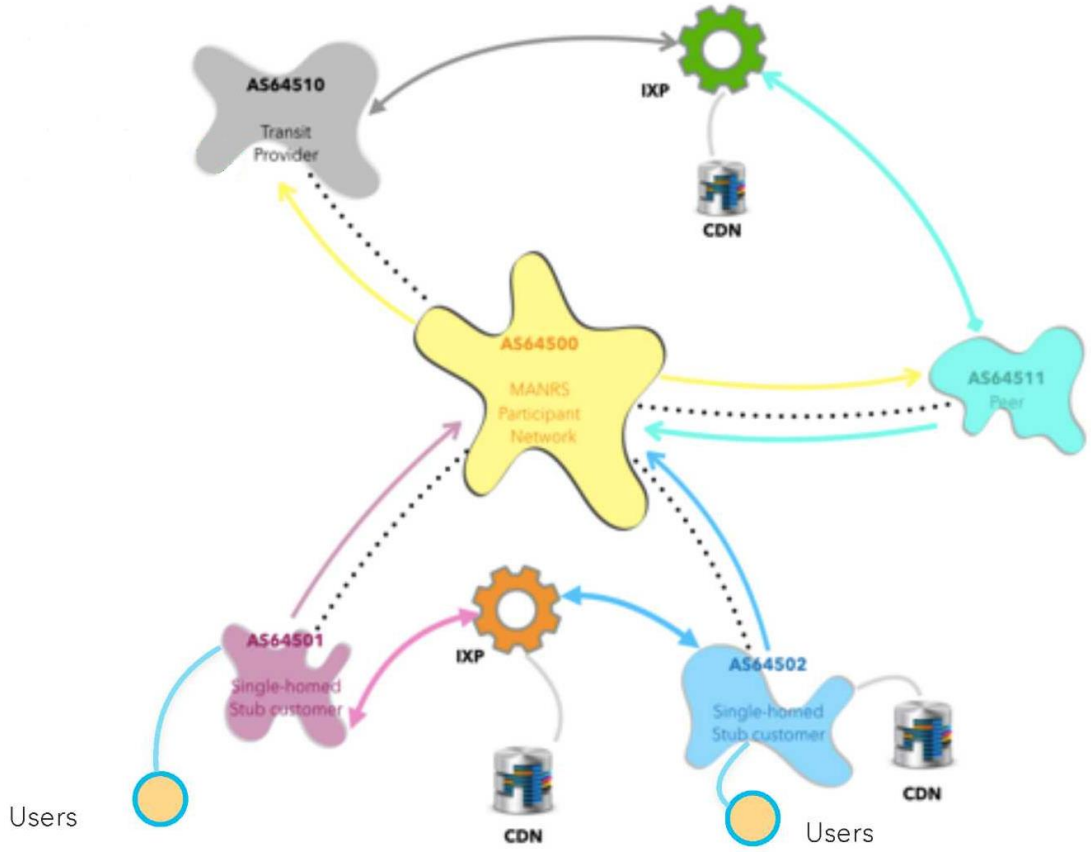
Internet Society
Armenia Chapter

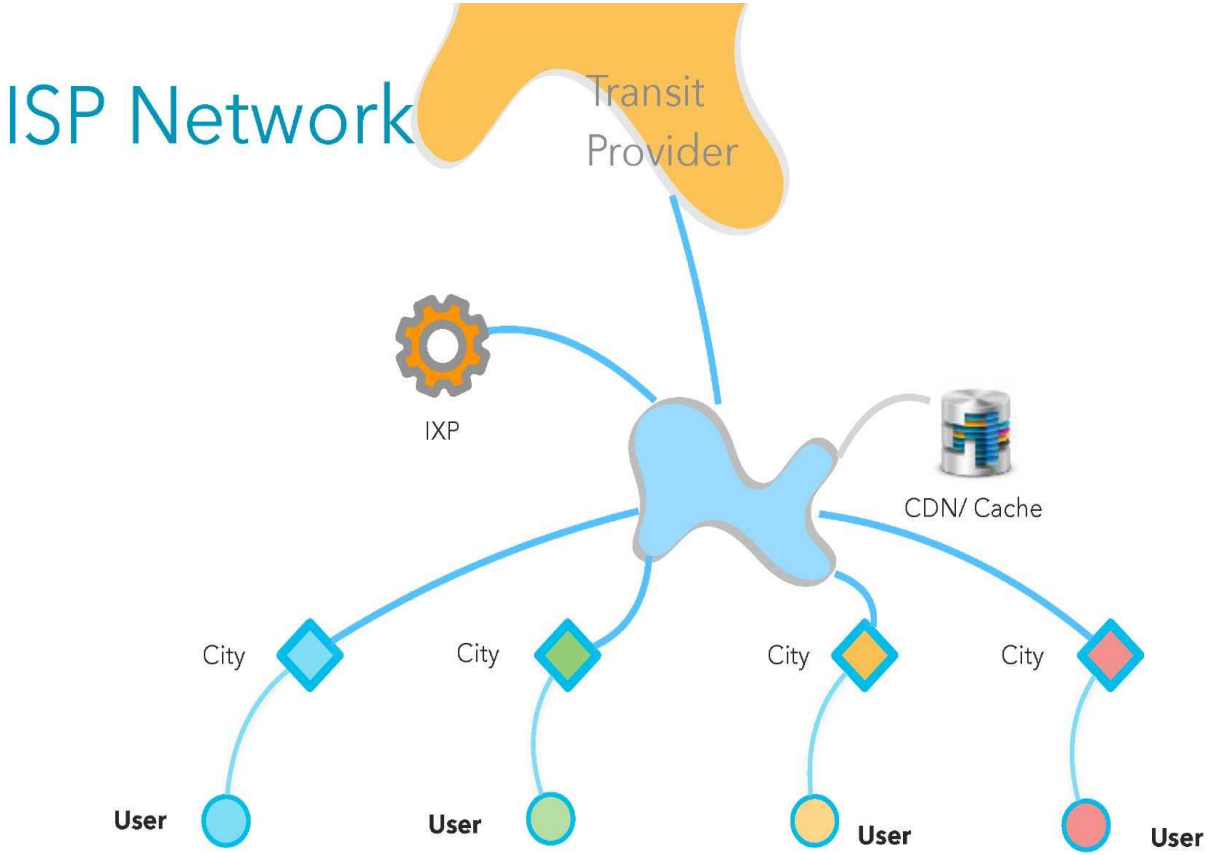


MANRS

Internet Society
Armenia Chapter

Internet Architecture





MANRS

Internet Society Armenia Chapter

Routing threats :

- THE THREATS- BGP HIJACKING

- BGP hijacking is when an attacker disguises itself as another network;
it announces network prefixes belonging to another network as it those prefixes are theirs. If this false information is accepted by neighboring networks and propagated further using BGP, it distorts the "roadmap" of the Internet.

- THE THREATS- ROUTE LEAKS

- A route leak is the propagation of routing announcement(s) beyond their intended scope. That is, an announcement from an Autonomous System (AS) of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender, and/or one of the ASes along the preceding AS path.

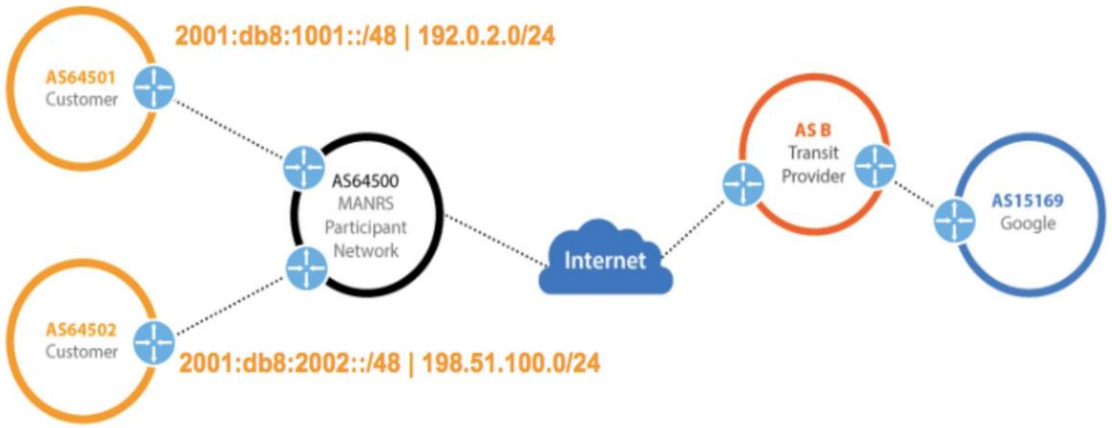
- THE THREATS - IP ADDRESS SPOOFING

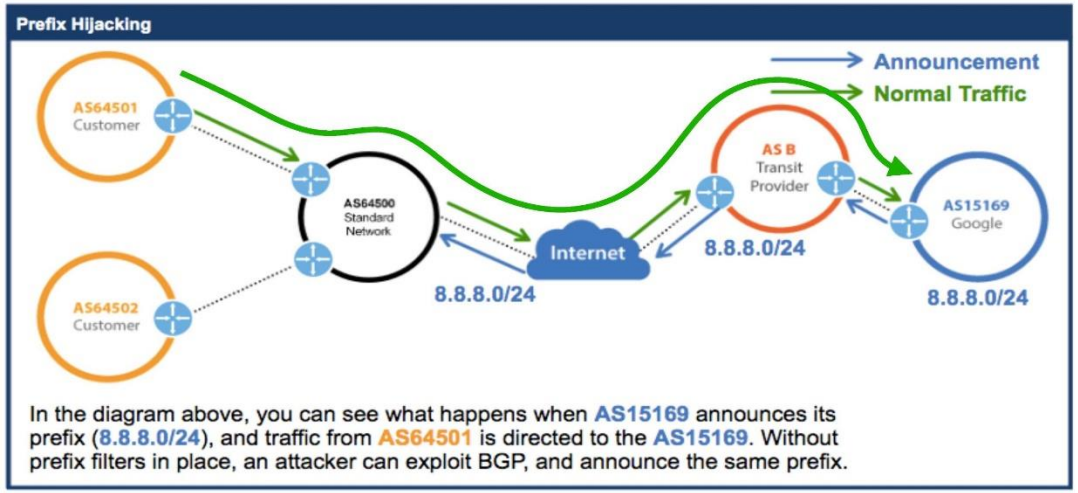
- IP address spoofing, or IP spoofing, is the forging of a source IP address field in IP packets with the purpose of concealing the identity of the sender or impersonating another computing system.

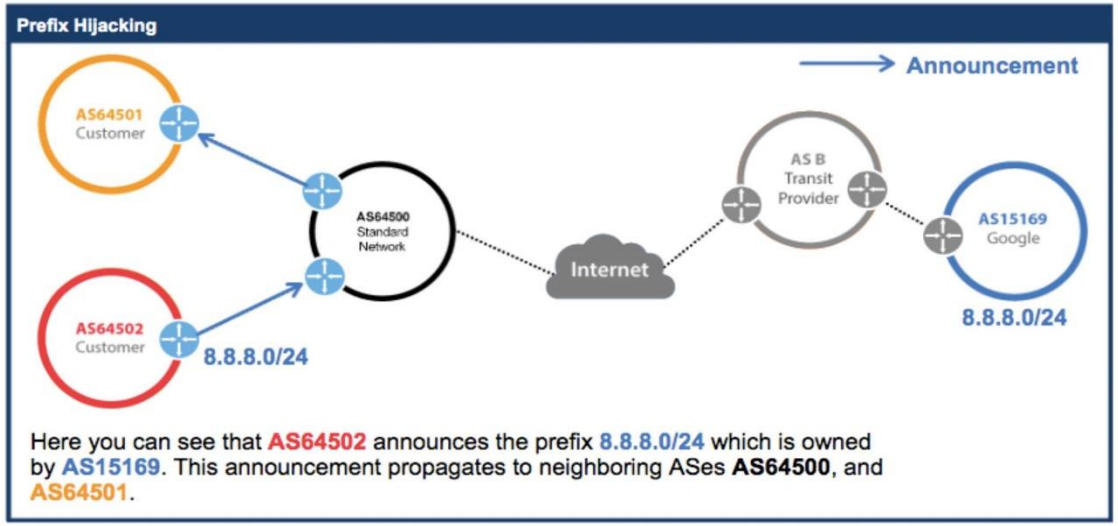
MANRS

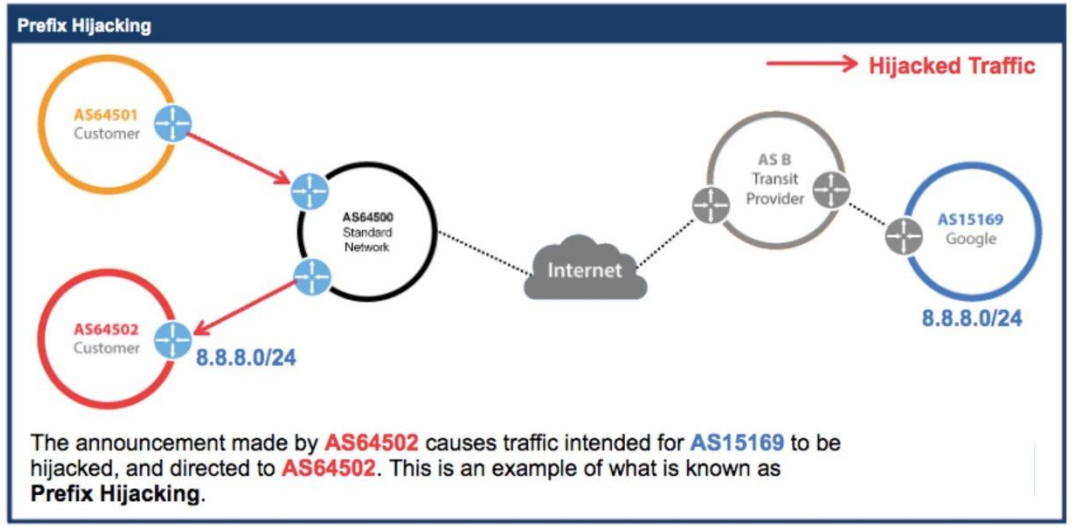
Internet Society
Armenia Chapter

THE THREATS - BGP HIJACKING









MANRS

Internet Society
Armenia Chapter

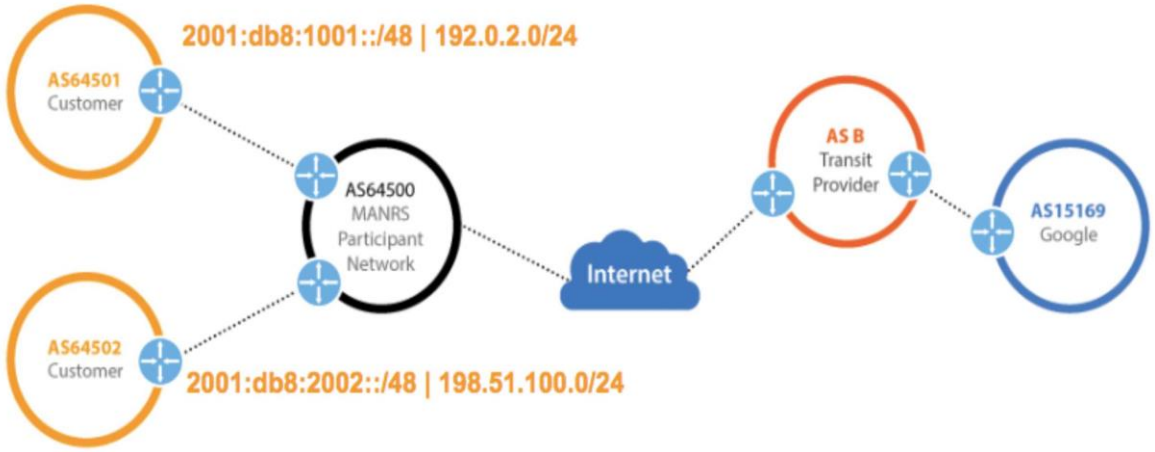
Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger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

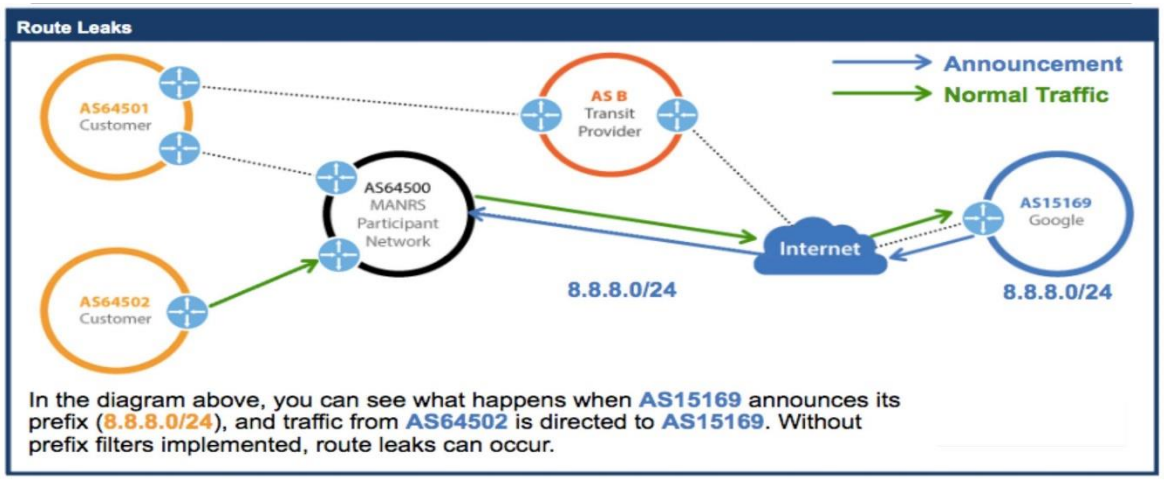
COVID 19 – Stay at home. Be healthy.

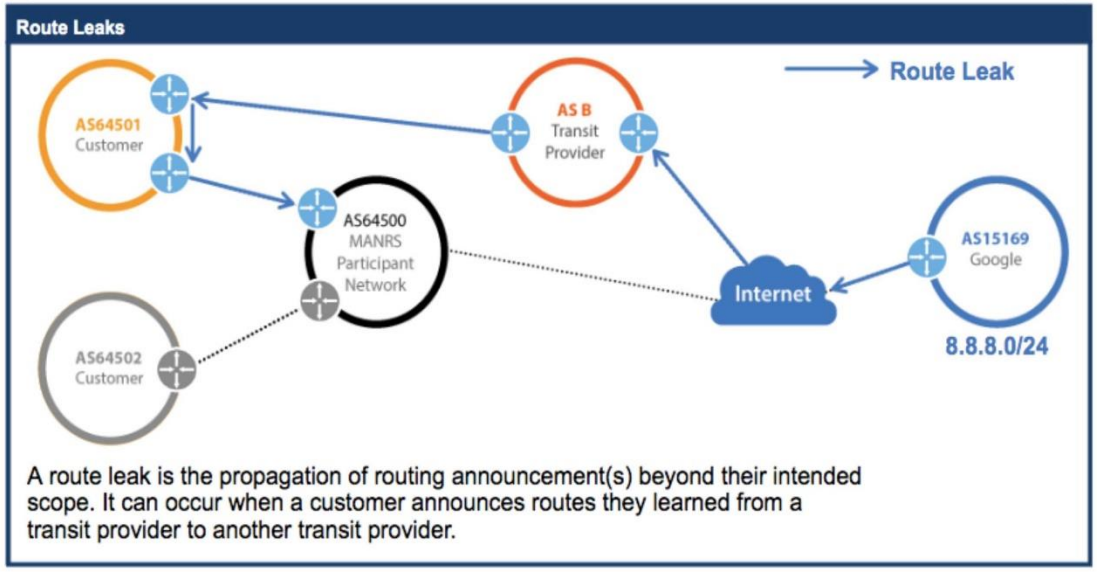
MANRS

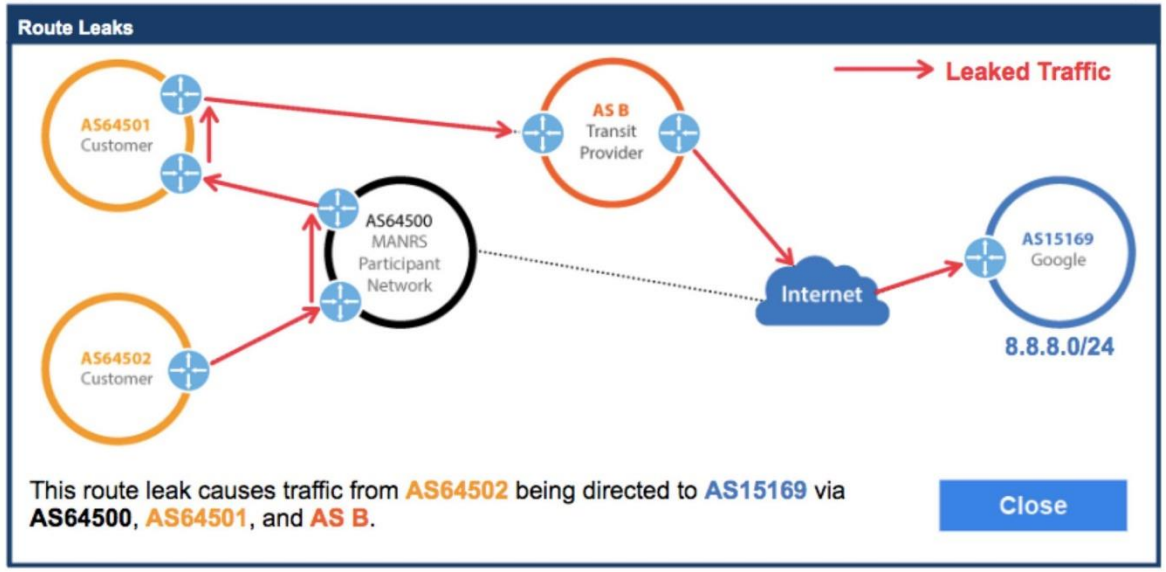
Internet Society
Armenia Chapter

THE THREATS – ROUTE LEAKS









MANRS

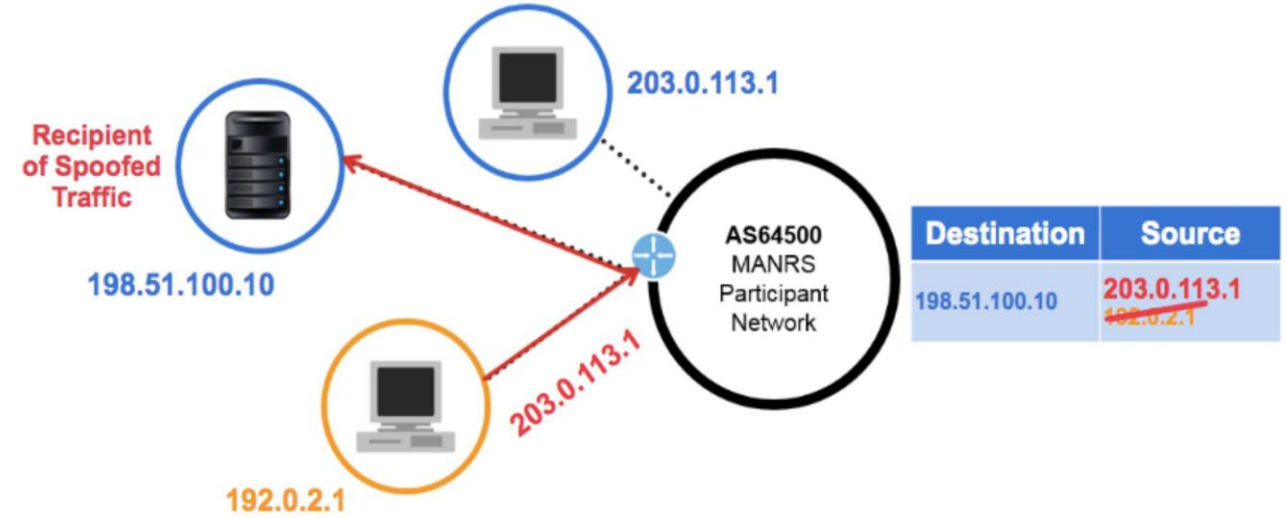
Internet Society
Armenia Chapter

Event	Explanation	Repercussions	Solution
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

MANRS

Internet Society Armenia Chapter

THE THREATS – IP ADDRESS SPOOFING



IP source address spoofing is the practice of originating IP datagrams with source addresses other than those assigned to the host of origin. Put simply, the host pretends to be some other host.

Reflection occurs when an attacker sends traffic to a victim via a third party. Amplification is achieved by small queries resulting in much larger responses. Open DNS resolvers and ntp servers are commonly used as reflectors/amplifiers

Spoofing can be exploited in various ways, most notably to execute a DDoS Reflection-Amplification attack.

MANRS

Internet Society
Armenia Chapter

Event	Explanation	Repercussions	Solution
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

COVID 19 – Stay at home. Be healthy.

MANRS

Internet Society Armenia Chapter

Who join Internet

Service Providers

Enterprises

IXPs

CDN & Cloud Providers

Who can Join MANRS ?

Network operators (Enterprise, ISP, CDN, Cloud providers . . .) have a responsibility to ensure a globally robust and secure routing infrastructure

COVID 19 – Stay at home. Be Healthy.

MANRS

Internet Society Armenia Chapter

Why an ISP would Join MANRS?

Service Providers will benefit from joining MANRS for a variety of reasons including:

* To add competitive value, and differentiate in a flat, price-driven market
* Show security proficiency and commitment to your customers
* To obtain “lock-in” from a connectivity provider to a security partner
* To help solve global network problems
* Enterprises indicate willingness to pay more for secure services

MANRS

Internet Society Armenia Chapter

Why an Enterprise would Join MANRS?

Enterprises should demand service providers join MANRS to:

* **Improve your organizational security posture**
* **Address security problems that affect your network**
* **Provide a foundation for security value-added services**

MANRS

Internet Society Armenia Chapter

Why an IXP would Join MANRS?

IXPs represent active communities with common operational objectives and already contribute to a more resilient and secure Internet infrastructure.MANRS can help IXPs build safe neighborhoods, leveraging the MANRS security baseline. It also demonstrates an IXP's commitment to security and sustainability of the Internet ecosystem, and dedication to providing high quality services. IXPs can be a collaborative focal point to discuss and promote the importance of routing security.

MANRS

Internet Society Armenia Chapter

Why an CDN/Cloud Providers would Join MANRS?

CDNs and cloud providers typically exchange traffic with thousands of other networks so data can flow efficiently around the world. This makes them large hubs of the Internet interconnection infrastructure. Their participation in MANRS amplifies the positive effect they have on routing security, and the routing hygiene of networks they peer with.

According to industry estimates, over half of all web traffic is served over CDNs, and their use continues to grow to meet Internet users' growing appetite for media content, such as video, music, gaming, and software downloads. CDNs are therefore in a unique position to help to secure the global Internet.

MANRS

The Internet Society recommends that you join the MANRS community to improve your security posture and reduce both the number and impact of routing incidents.

We are calling upon network operators around the world to join the Routing Resilience Manifesto Initiative, and to agree to the Mutually Agreed Norms for Routing Security (MANRS) Principles.

Having such a document, could serve at least two purposes:

- Ease deployment of measures required by MANRS (stub networks or small providers – the majority of ASNs).
- Help check if the network setup is compliant with MANRS

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

MANRS core principles

We (the ISP/network operator/ISP/CDN&Cloud Providers) recognize the interdependent nature of the global routing system and our own role in contributing to a secure and resilient Internet.

We will integrate best current practices related to routing security and resilience in our network management processes in line with the Actions.

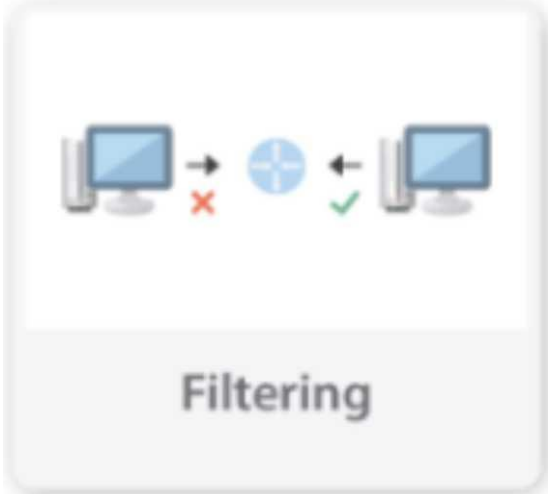
We are committed to preventing, detecting and mitigating routing incidents through collaboration and coordination with peers and other ISPs in ine with the Actions.

We encourage our customers and peers to adopt these Principles and Actions.

MANRS

Internet Society
Armenia Chapter

MANRS Four Pillars

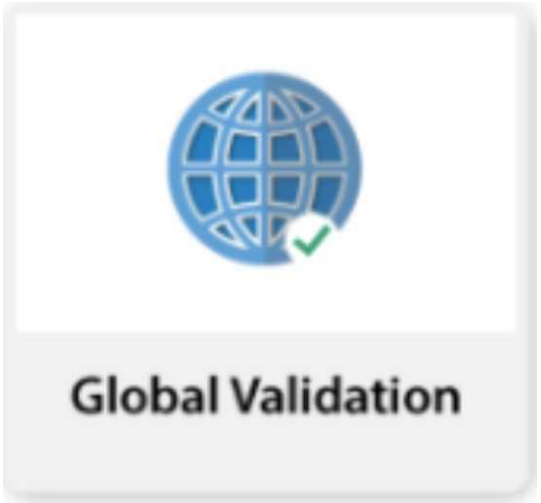


MANRS defines **four concrete actions** that network operators should implement. They are a technology-neutral baseline so that they can be globally adopted.

MANRS

Internet Society
Armenia Chapter

Pillar I – Global Validation



In order to ***facilitate validation of routing information on a global scale,*** network operators must publish their routing information so that other parties can validate it.

MANRS

Internet Society
Armenia Chapter

Pillar II – Filtering

In order to ***prevent propagation of incorrect routing information,*** network operators must ensure the correctness of their own announcements, and announcements from their customers to adjacent networks with prefix and AS-path granuarity.

MANRS

Internet Society
Armenia Chapter

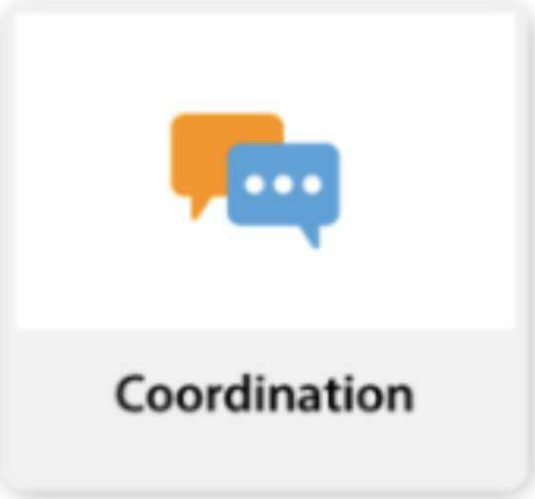
Pillar III – Anti-Spoofing

In order to ***prevent traffic with spoofed source IP addresses,***network operators must enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure.

MANRS

Internet Society
Armenia Chapter

Pillar IV – Coordination



In order to ***facilitate global operational communication and coordination between network operators,*** they must maintain globally accessible and up-to-date contact information.

MANRS

Internet Society
Armenia Chapter


Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

To assist you in implementing the steps necessary to be compliant with the Mutually Agreed Norms for Routing Security, the community of MANRS participants developed an implementation Guide. This document captures the best current operational practices deployed by network operators around the world.

https://www.manrs.org/isps/guide/

MANRS

Internet Society
Armenia Chapter

MANRS COURSE CONTENTS

IRRs, RPKI, and Peering DB

Global Validation

Filtering

Anti-Spoofing

Coordination

MANRS

Internet Society
Armenia Chapter

CONCLUSION

Many say that networking is unnecessarily complex and costly, not because the infrastructure cannot be protected, but because it isn’t protected. We, as an industry, are capable of verifiably identifying the prefixes we use and preventing them from being misused—either in routing or as a source address when accessing a service. And it is our responsibility to do so.

MANRS

Internet Society
Armenia Chapter

CONCLUSION

Fulfilling that responsibility starts with the following next steps:

1. There are no disadvantages to a network filing IRR and RPKI data to protect its assets. RIRs should require members to file IRR and RPKI data when possible, and companies advertising prefixes in BGP should register valid IRR registries and RPKI ROAs

2. For networks in which deployment is simple (e.g., networks that serve SOHO customers or enterprise customers), enforcement of IRRs and RPKI in routing and BCP 38 in data transmission is a low-cost way for a network to protect both itself and the networks that connect to it. They should deploy uRPF for each downstream customer and validate the routes that customers advertise to it.

3. Open- and closed-source development communities should clean routes via tools that are inexpensive to operate and that integrate RPKI and IRR technology with the data in each RIR’s delegated--latest allocation files.

MANRS

Internet Society
Armenia Chapter

It is significantly easier and less costly to implement MANRS than to lose your customers' data and your network's good name to a security breach.

MANRS

Internet Society
Armenia Chapter

References:

1. https://www.manrs.org/resources/tutorials/introduction/
2. https://www.manrs.org/resources/tutorials/
3. https://www.manrs.org/isps/guide/
4. http://irrexplorer.nlnog.net/
5. https://bgpmon.net/
6. https://www.peeringdb.com/
7. https://docs.peeringdb.com/
8. https://stat.ripe.net/
9. https://stat.ripe.net/widget/as-routing-consistency/
10. https://www.cloudflare.com/peering-policy
11. https://www.peering.google.com/#/options/peering
12. https://www.fastly.com/peering
13. https://github.com/irrtoolset/irrtoolset
14. https://github.com/NLnetLabs/routinator/blob/master/
15. https://www.arin.net/resources/manage/rpki/rpa.pdf

16. https://docs.peeringdb.com/presentation/20190507-BKNIX-PeeringforumArnold-Nipper.pdf
17. https://about.rdap.org/
18. https://rdap-web.lacnic.net/
19. https://www.lacnic.net/1040/2/lacnic/lacnics-whois/
20. https://www.lacnic.net/1018/2/lacnic/resource-certification-system-rpki
21. https://rpki.readthedocs.io/
22. https://my.afrinic.net/
23. https://myapnic.net/
24. https://account.arin.net/
25. https://milacnic.lacnic.net/
26. https://my.ripe.net/
27. https://www.arin.net/resources/manage/rpki/
28. https://www.arin.net/resources/manage/irr/
29. https://www.lacnic.net/en/web/lacnic/certificacion-de-recursos-rpki/
30. https://youtu.be/rxN4zWTNSds ttww.caida.org/projects/spoofer/
31. https://blog.cloudflare.com/the-deep-dive-into-how-verizon-and-a-bgpoptimizer-knocked-large-parts-of-the-internet-offline-Monday/
32. https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study/
33. https://www.caida.org/projects/spoofer/

34. https://www.youtube.com/watch?v=IzLPKuAOe50/
35. https://github.com/NLnetLabs/routinator/blob/master/doc/transports.md/
36. https://www.ntt.com/index.html
37. https://www.firstpost.com/tech/news-analysis/internet-service-providers-in-mumbai-targeted-in-ddos-attack-3685981.html
38. https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
39. https://www.ibtimes.co.uk/blizzards-battle-net-servers-knocked-offline-following-massive-ddos-attack-1573969
40. https://youtu.be/rxN4zWTNSds
41. http://www.ripe.net/ripe/docs/ripe-431
42. http://www.team-cymru.org/Services/Bogons/bogon-dd.html
43. https://tools.ietf.org/html/rfc2827