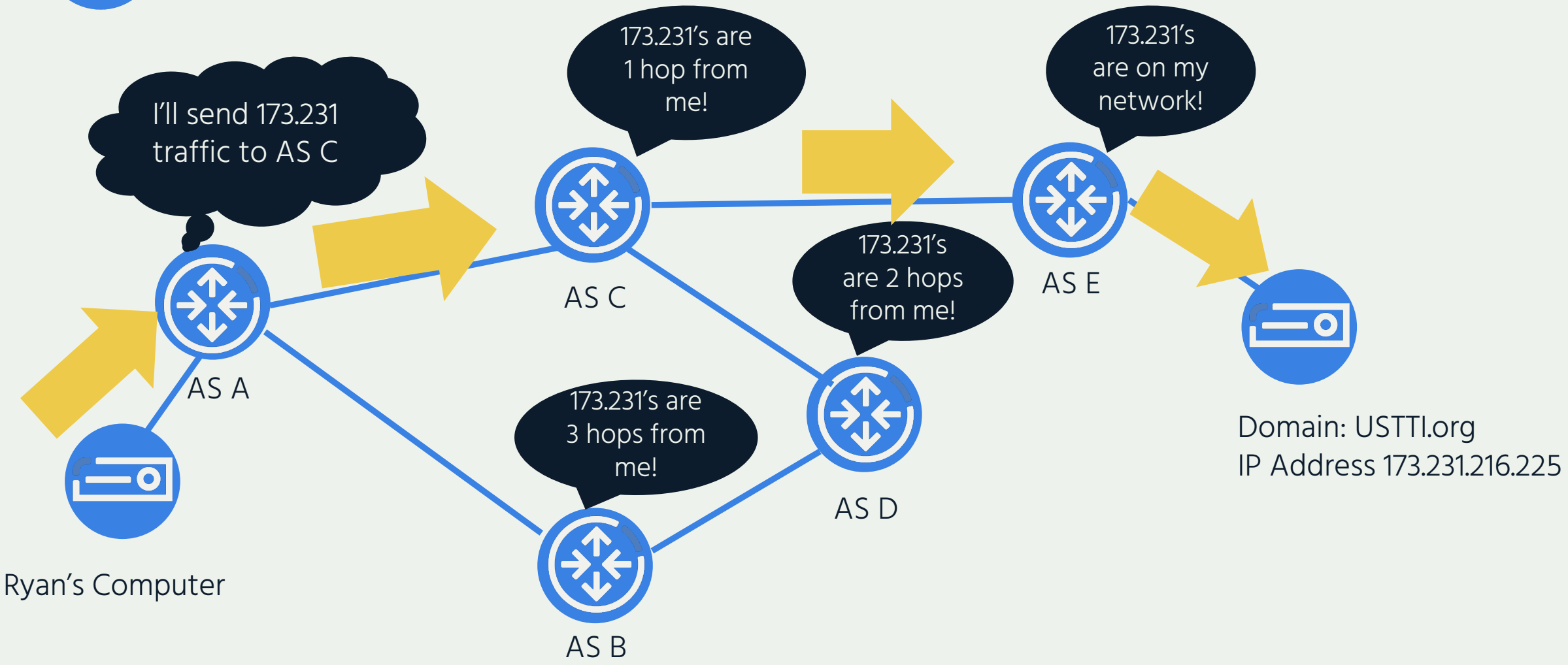
24 May 2023

Routing Security in the Decentralized Internet

A Critical Role for Governments to Protect the Internet

John B. Morris, Jr.
Principal, U.S. Policy & Advocacy
Internet Society

Example: BGP Routing



Distributed routing delivers a resilient and adaptable network of networks, allowing for local optimizations while maintaining worldwide connectivity.

Remember:

- As a network of networks, the Internet's infrastructure is based on nearly 80,000[7] independent networks choosing to collaborate and connect together
- Each networks makes independent decisions on how to route traffic to its neighbors, based on its own needs and local requirements.
- And each network makes independent decisions on how to route traffic to its neighbors, based on its own needs and local requirements.
- Routing decisions are often based on trust and relationships.

But what about when the routing system doesn't work as intended?

What happens when one of these networks makes the wrong decision?

What happens when a network acts maliciously?

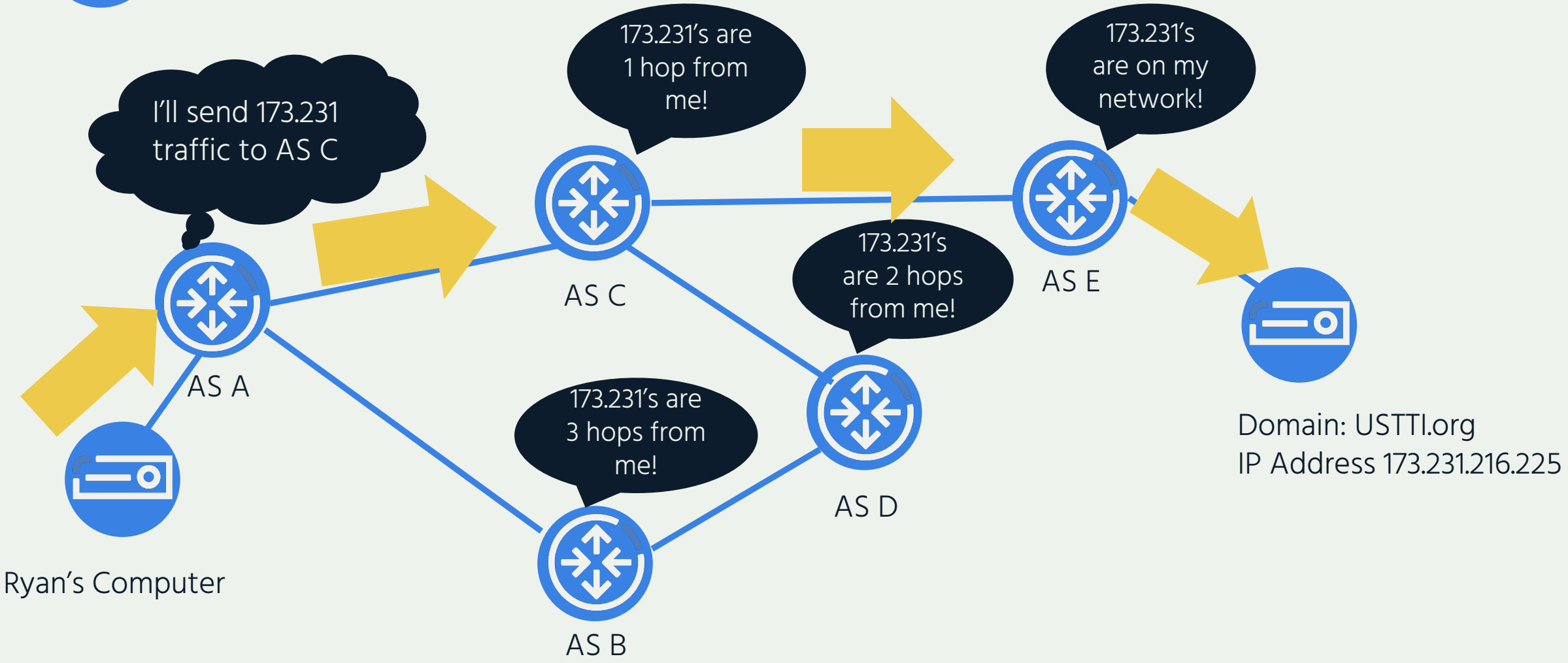
What happens when a network just makes a mistake?

Answer: a routing incident

Types Of Routing Incidents

- **Route leak:** when a network mis-announces a route to a neighbor.
- **Route hijacking:** a network operator or attacker impersonates another network operator, pretending that it is the correct path to the server or network being sought on the Internet. This can cause packets to be forwarded to the wrong place, denial of service (DoS) attacks or traffic interception.
- **IP Spoofing:** someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system. IP spoofing can be used to perform domain name server (DNS) amplification attacks.

Example: BGP Routing



How to secure the decentralized routing system?

What we can't lose: a distributed routing system delivers several key benefits: global reach, resilience, and optimized connectivity.

That means that: a top-down approach to security won't work in a globally distributed routing system

If you begin telling network who can and cannot interconnect with who, that won't scale and will break the Internet.

The good news

Best practices in routing security are already available and are largely effective against these forms of routing incidents.

- For both route leaks and route hijacks, network operators can use **stronger filtering policies** to determine when bad announcements are made by neighboring networks.
- This is improved by registering of verified routes in Internet Routing Registries (IRRs) or cryptographically through Routing Public Key Infrastructure (RPKI).
- IP source validation can be used to find spoofed traffic as it moves to leave or enter a network. Spoofed traffic can then be filtered, preventing it from reaching its destination.

Challenges in Improving Routing Security

Despite the availability of solutions to common routing incidents, ecosystem challenges limit their use:

- Routing incidents are hard to address far from the source and must instead be addressed collectively.
- Economic externalities.
- Routing security is not a market differentiator.

Improving routing security

- Large, yearly improvements in RPKI deployment jumping from **18.6% in December 2019 to 41.5%** in December 2022 (Table 1).
- By the end of 2023, more than half of the Internet is expected to be RPKI-enabled
- Industry led initiatives like the **Mutually Agreed Norms for Routing Security** are pushing these improvements.

MONTH June 2023 COUNTRY Singapore USE GRIP DATA

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

Route misoriginations	6
Route leaks	2
Bogon announcements	7
Total	15

Culprits

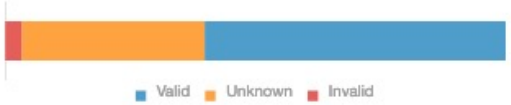
Culprits	13

Routing Information (IRR)

Unregistered	403	4.4%
Registered	8,695	95.6%

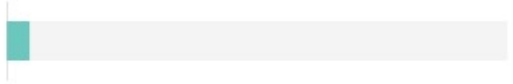
Routing Information (RPKI)

Valid	5,489	60.2%
Unknown	3,323	36.5%
Invalid	299	3.3%



Route Origin Validation

ROV-based Filtering Rate (%)	4.5%



MANRS Readiness

How Governments can help!

- Lead by Example, including procurement!
- Facilitate/encourage the adoption of common practices for routing security
- Support efforts to develop new, or strengthen existing, routing security tools
- Encourage the use of security as a competitive differentiator
- Strengthen communication and cooperation between network operators and other stakeholders
- Identify and address legal barriers to information sharing, the implementation of routing security technologies and research on routing incidents and threats.

Questions?

- Natalie Campbell, campbell@isoc.org
- John Morris, jmorris@isoc.org