Routing Security 101

Amreesh Phokeer
Research Manager
SAFNOG-5, JNB, ZA

Routing security

BGP is based entirely on trust

- No in-built security mechanism to validate BGP announcements
- No single point of control
- Work on the basis of unreliable sources of data (WHOIS, IRR, etc)

AFRINIC
The Internet Numbers Registry for Africa

How a Nigerian ISP Accidenta… Offline

Share Like 1.4K Tweet

Tom Paseka

November 15, 2018 5:22PM

How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Off… Today

Share Like 4.8K Tweet

Tom Strickx

June 24, 2019 7:58PM

Massive route leak impacts major pa… Internet, including Cloudflare

China hijacking internet traffic using BGP, claim researchers

30 OCT 2018 2

Privacy, Security threats

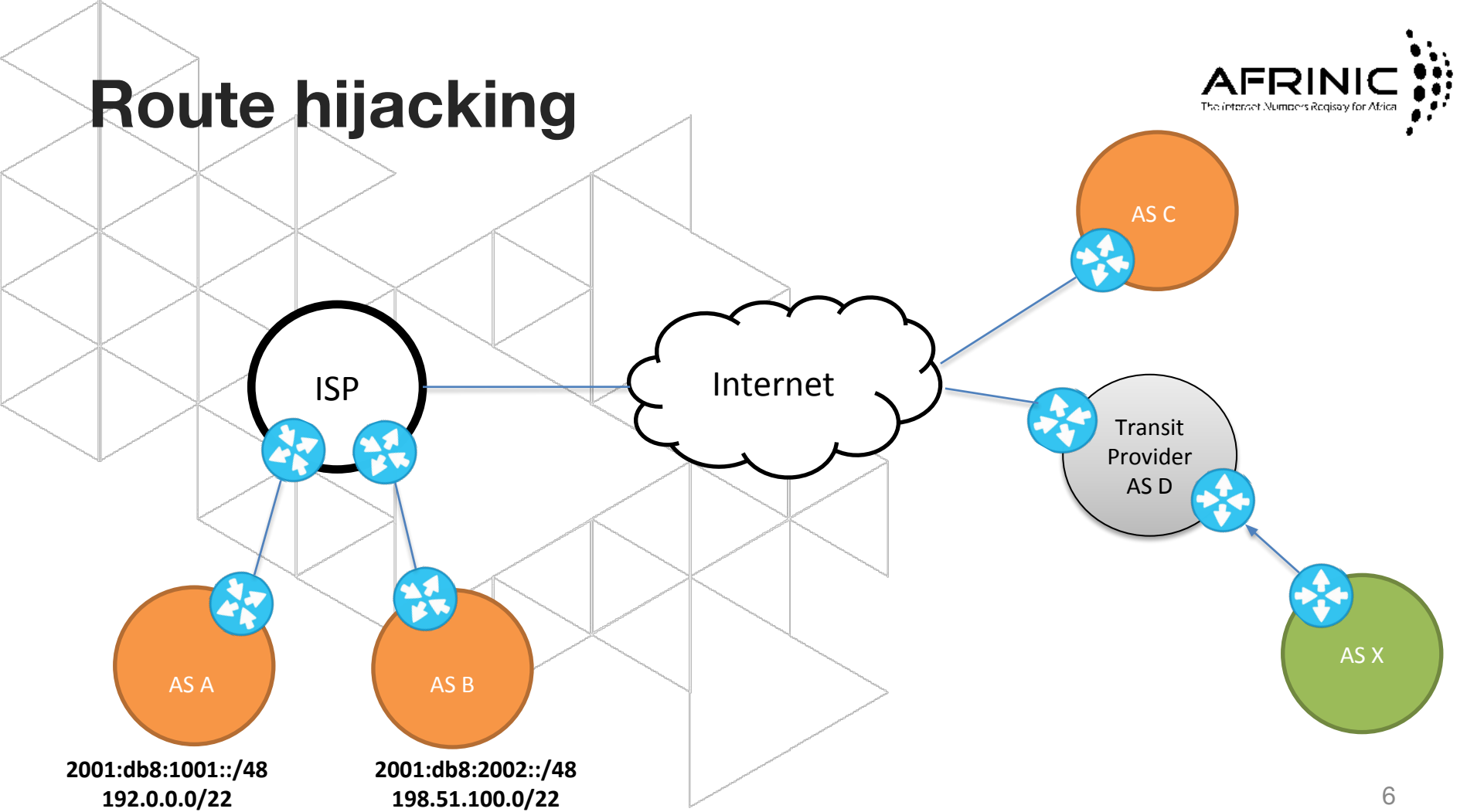
Route hijacking

- When a network operator impersonates another network operator (I advertise your prefix) or pretends that announced prefixes are their clients
- BGP principles: More specifics and Shortest path
- Malicious or unintentional
- Might create outages

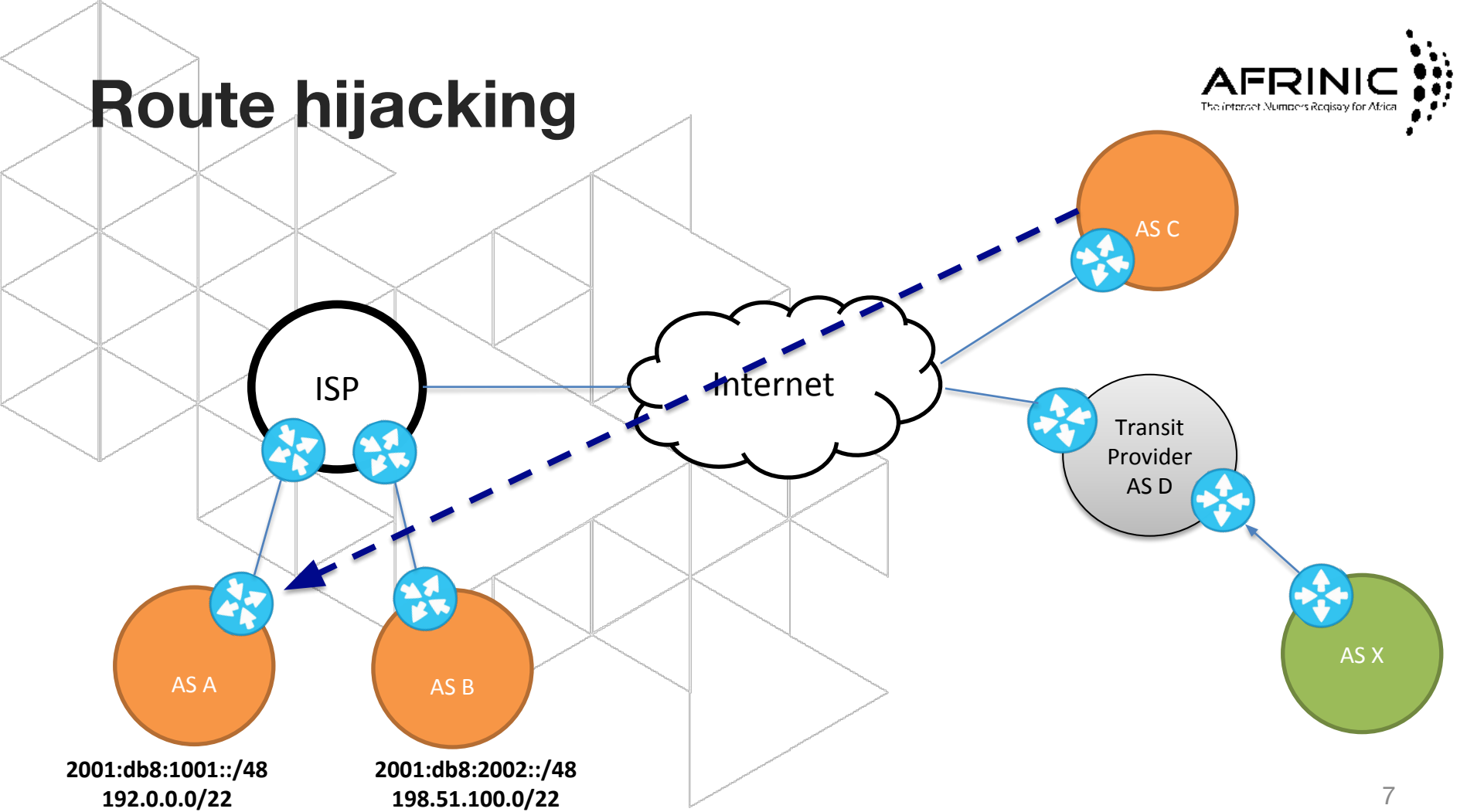
Route hijacking

- When a network operator impersonates another network operator (I advertise your prefix) or pretends that announced prefixes are their clients
- BGP principles: More specifics and Shortest path
- Malicious or unintentional
- Might create outages

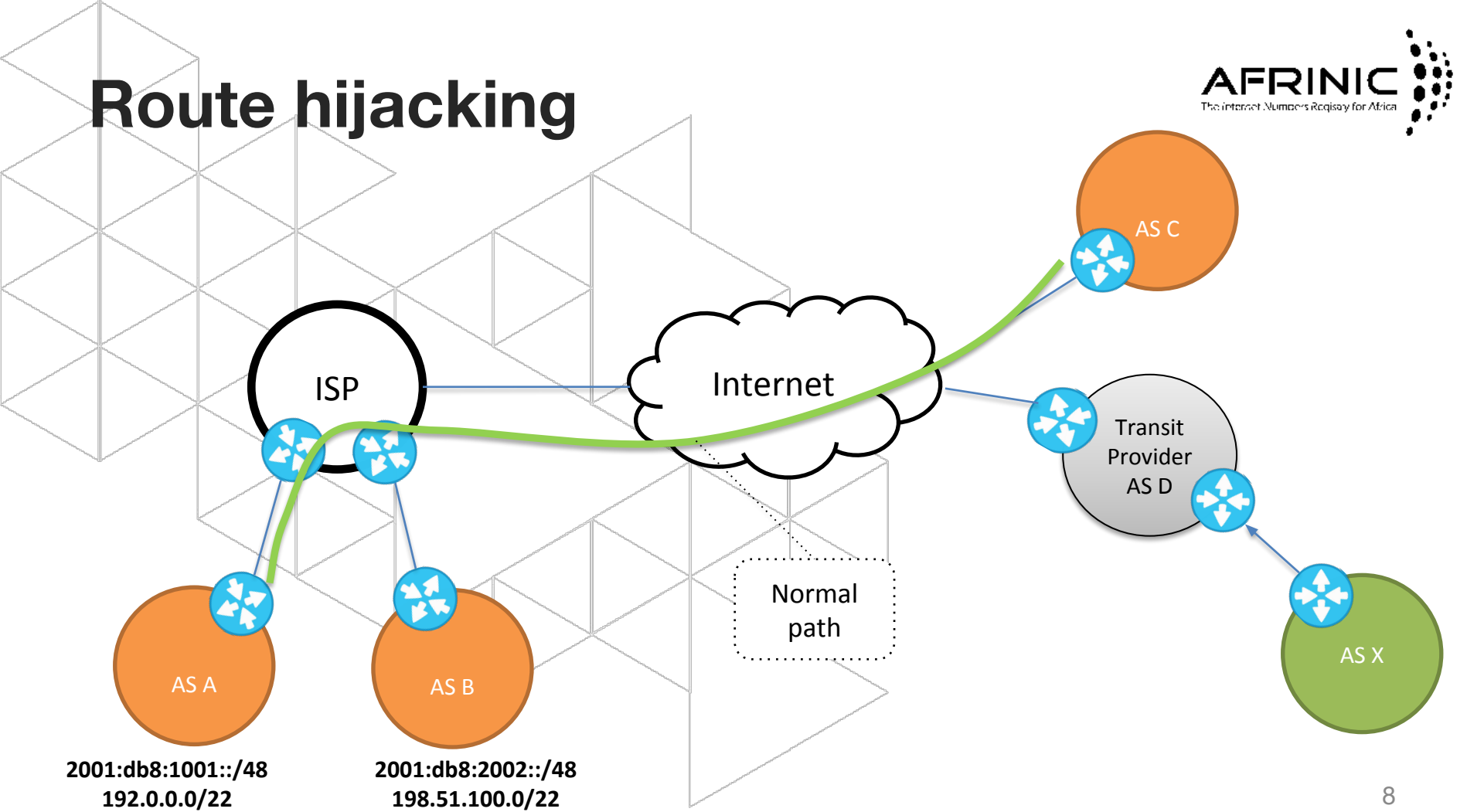
Route hijacking



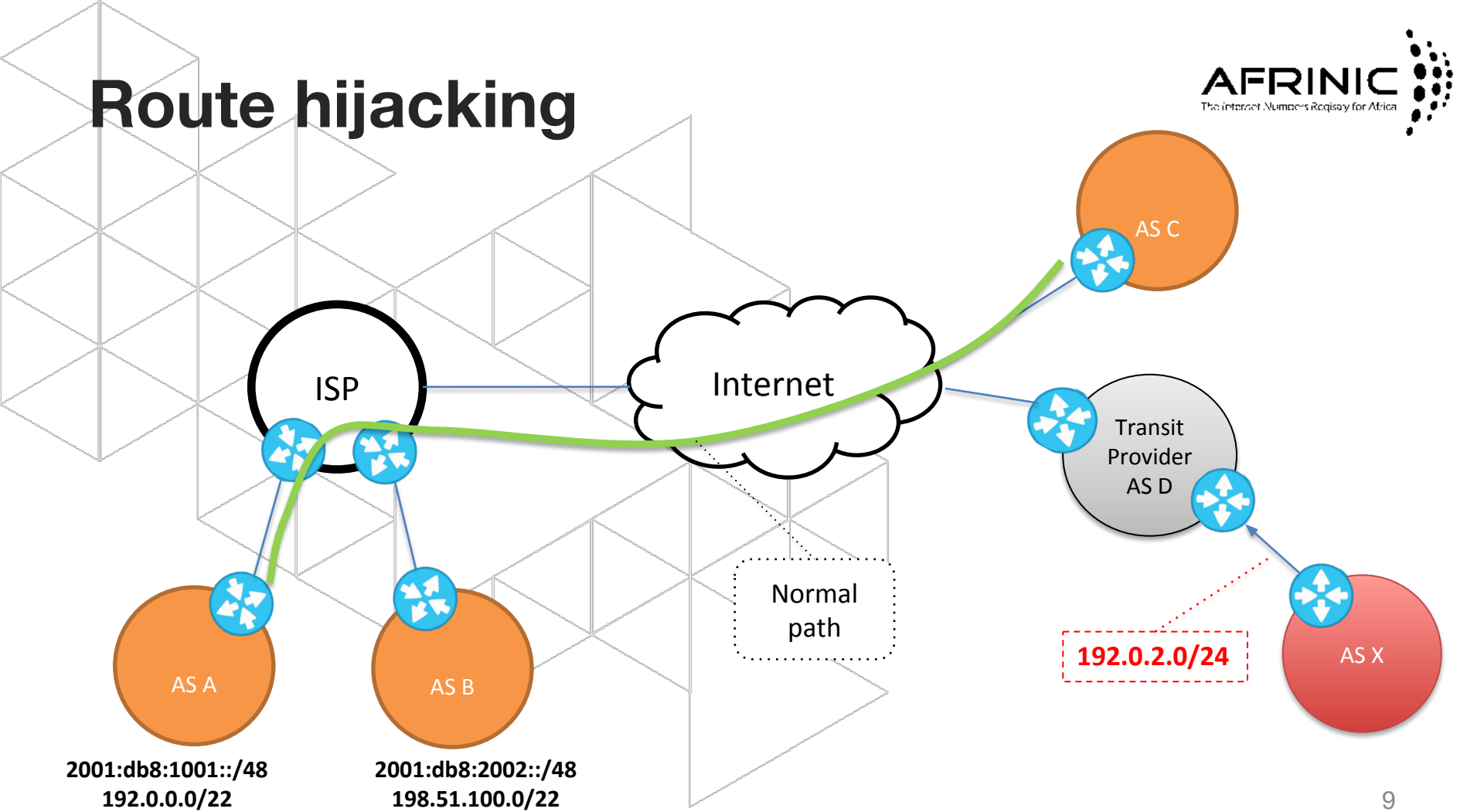
Route hijacking



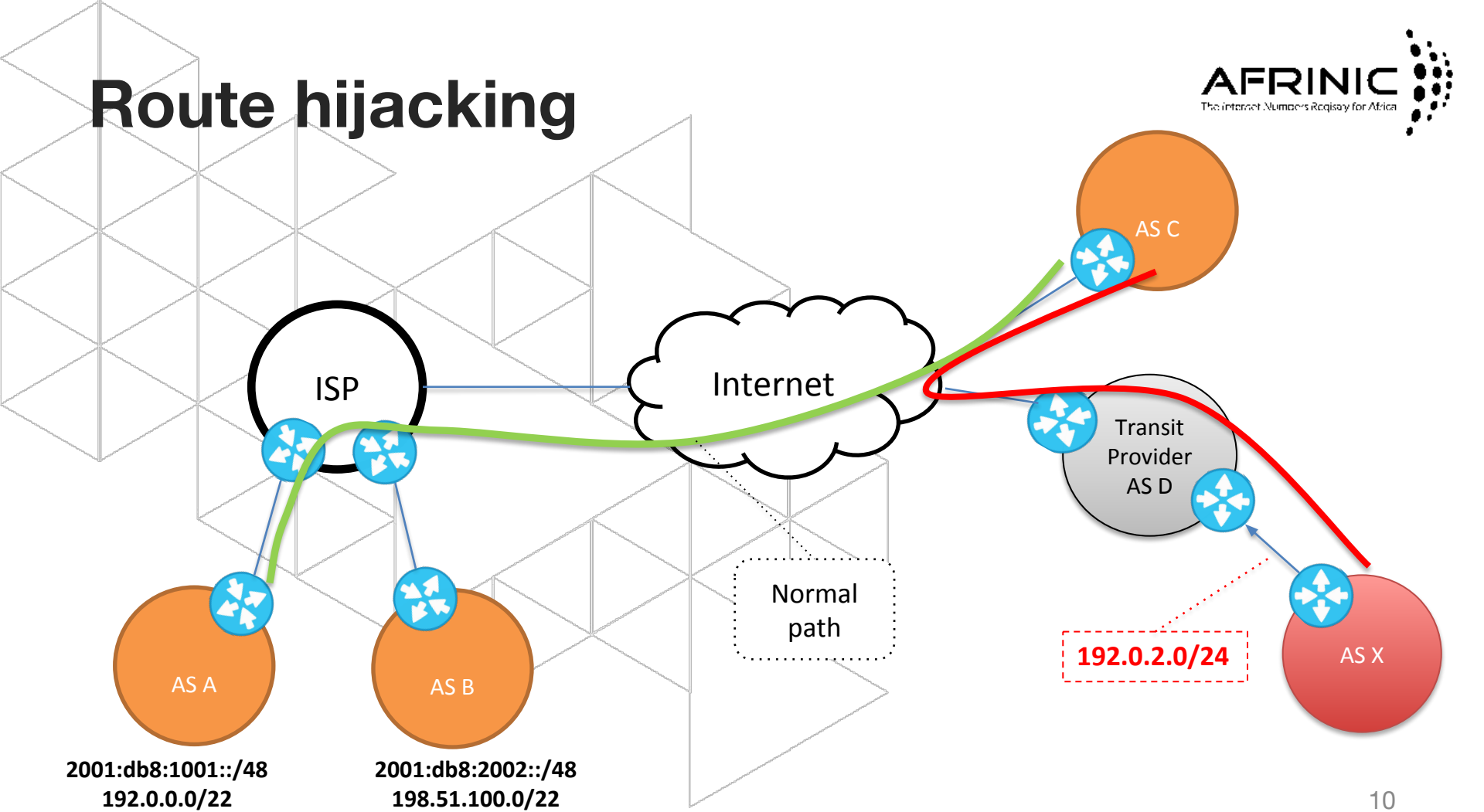
Route hijacking



Route hijacking



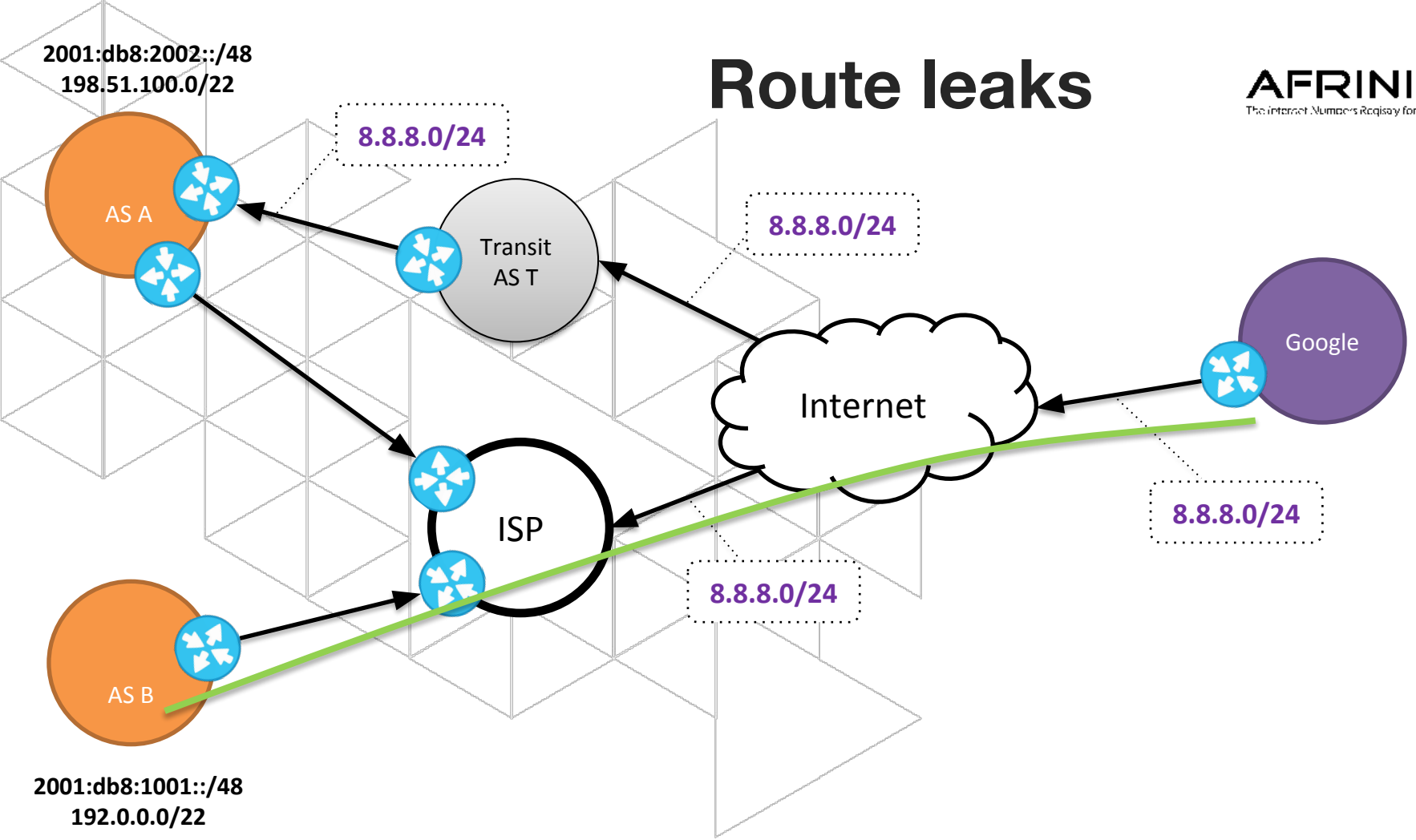
Route hijacking



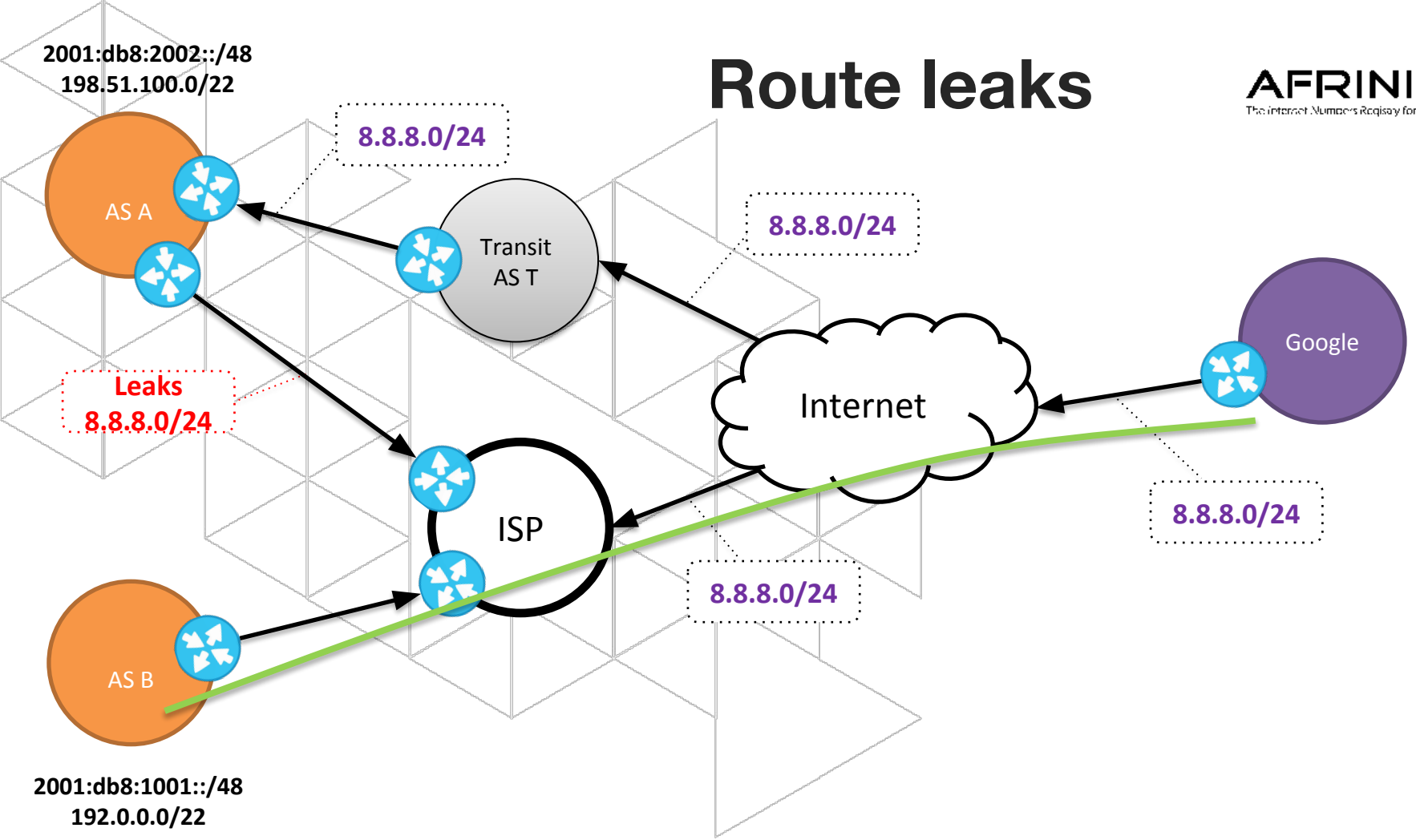
Route leaks

- When a network operator who is multi-homing (2 upstream) accidentally announces routes learned from one upstream to the other upstream
- Customer AS become an intermediary
- Usually unintentional

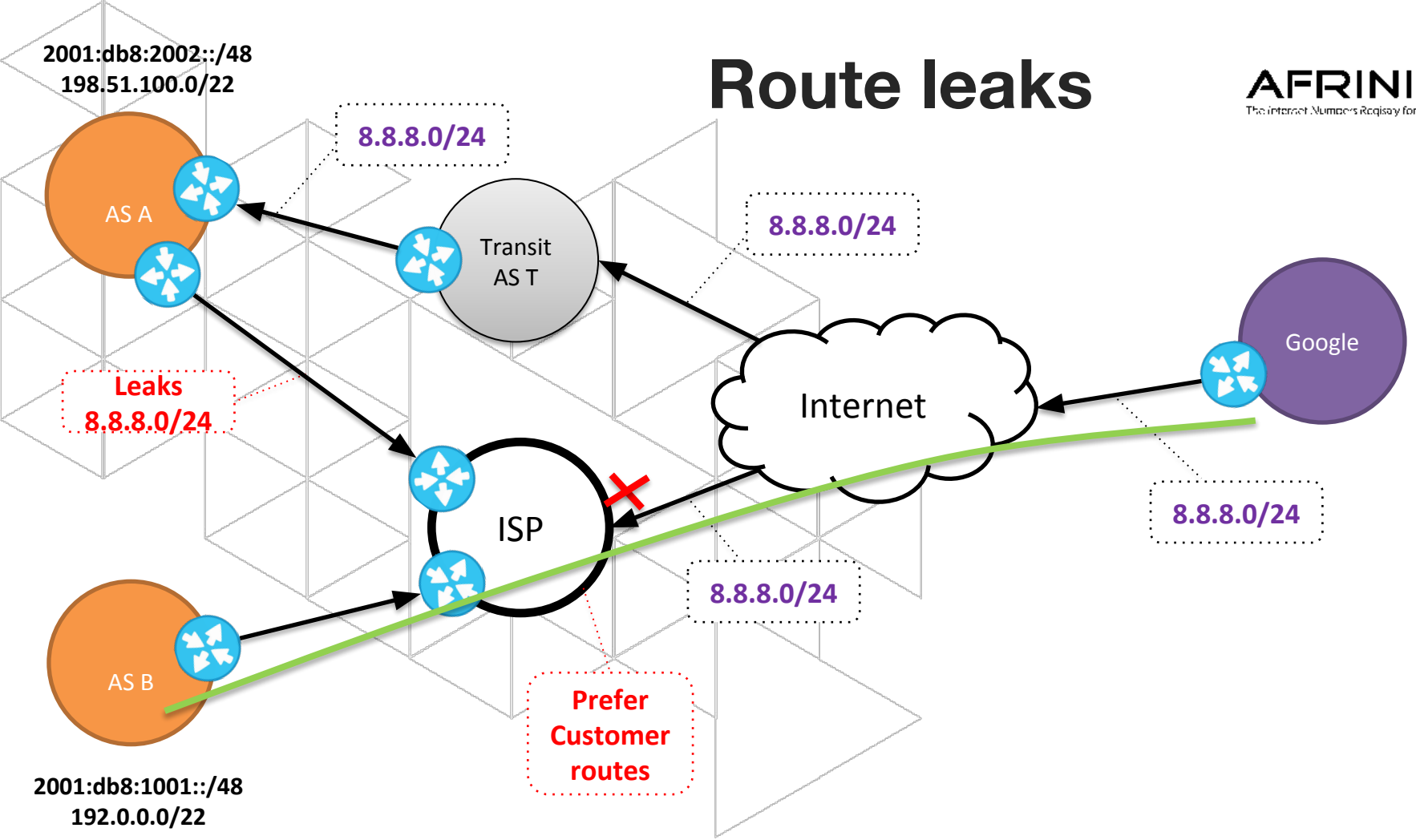
Route leaks


2001:db8:2002::/48
198.51.100.0/22
8.8.8.0/24
AS A
Transit
AS T
8.8.8.0/24
Google
Internet
ISP
8.8.8.0/24
8.8.8.0/24
AS B
2001:db8:1001::/48
192.0.0.0/22

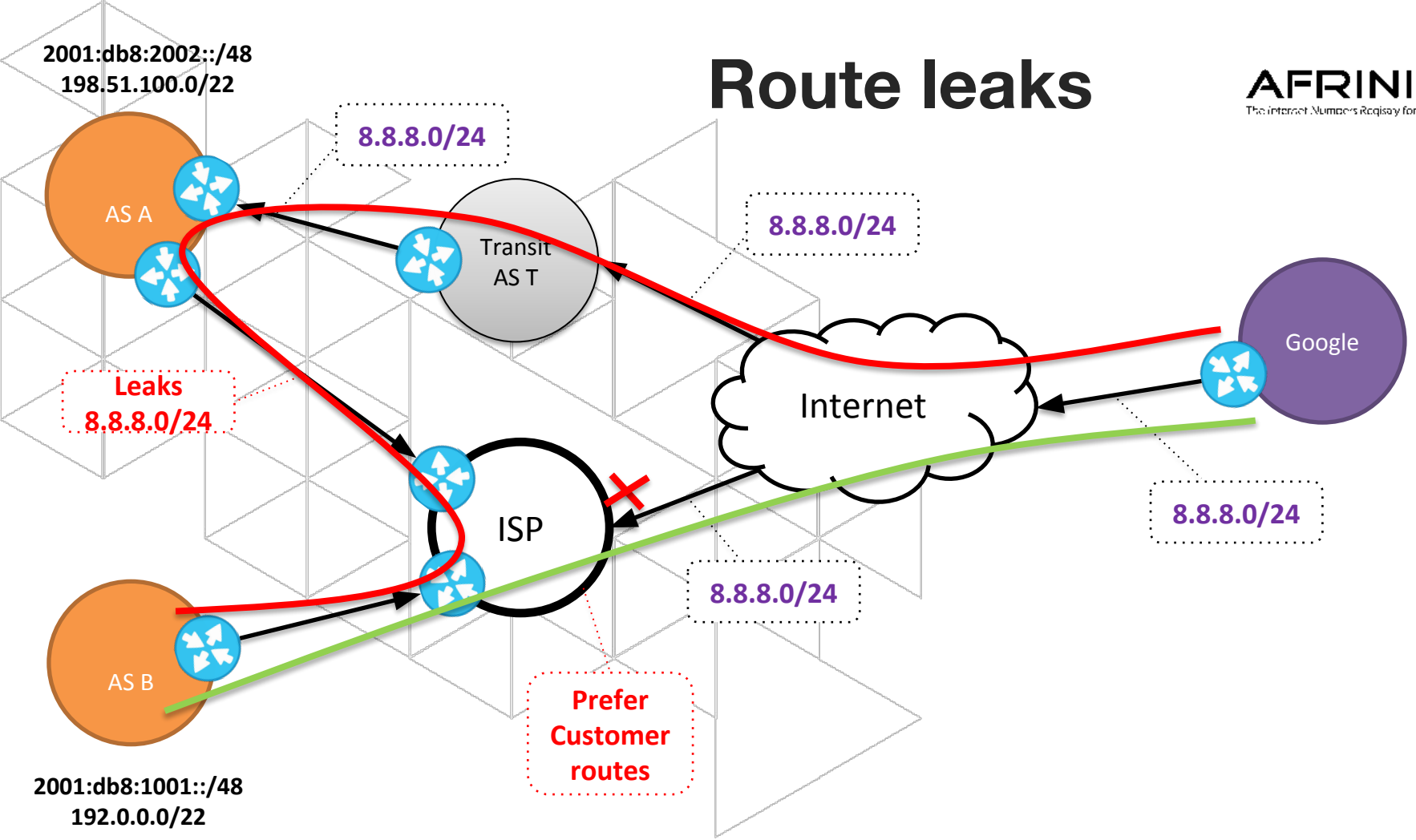
Route leaks


2001:db8:2002::/48
198.51.100.0/22
8.8.8.0/24
AS A
Transit
AS T
8.8.8.0/24
Google
Internet
Leaks
8.8.8.0/24
ISP
8.8.8.0/24
8.8.8.0/24
AS B
2001:db8:1001::/48
192.0.0.0/22

Route leaks


2001:db8:2002::/48
198.51.100.0/22
8.8.8.0/24
AS A
Transit
AS T
8.8.8.0/24
Google
Internet
Leaks
8.8.8.0/24
ISP
8.8.8.0/24
8.8.8.0/24
AS B
Prefer
Customer
routes
2001:db8:1001::/48
192.0.0.0/22

Route leaks


2001:db8:2002::/48
198.51.100.0/22
8.8.8.0/24
AS A
Transit
AS T
8.8.8.0/24
Google
Internet
Leaks
8.8.8.0/24
ISP
8.8.8.0/24
8.8.8.0/24
AS B
Prefer
Customer
routes
2001:db8:1001::/48
192.0.0.0/22

Solutions

Yes a few:

- Prefix and AS-PATH filtering
- RPKI, IRR
- BGPSEC (now standardised)

Issues

- Lack of incentives for deployment
- Lack of reliable data

Build filters!

Yes a few:

- Prefix and AS-PATH filtering
- RPKI, IRR
- BGPSEC (now standardised)

Issues

- Lack of incentives for deployment
- Lack of reliable data

Some Stats for 2018:

- **12,600** total incidents (outages or route leaks)
- Over **4%** of ASNs were affected
- **2,737** ASNs were victim of a least one routing incident
- **1,294** networks caused routing incidents

Source: BGPStream

Tragedy of the commons

Internet Routing:

Security is more often in the hands of your peers. Securing you own network does not necessarily make it more secure.

Mutually

Agreed

Norms for

Routing

Security

Principles

1. **Filtering** – Prevents announcements of incorrect routing information
    1. Filter your own announcements
    2. Filter incoming announcements from your peers and customers
    3. Filter AS-PATH
    4. Build filters using IRR, RPKI
    5. Big Network filters
2. **Anti-spoofing** – Prevent traffic with spoofed source IP addresses
    - Source address validation for stub customers
4. **Coordination** – Facilitate global operational communication and coordination between network operators
    - Maintain up-to-date data on IRR, WHOIS, etc
5. **Global Validation** – Facilitate validation of routing information on a global scale
    - Publish your routing policies

Thank you for your Attention

Questions?

twitter.com/ afrinic

flickr.com/ afrinic

facebook.com/ afrinic

linkedin.com/company/ afrinic

youtube.com/ afrinic media

www. afrinic .net