AFRINIC
The Internet Numbers Registry for Africa

Routing Security

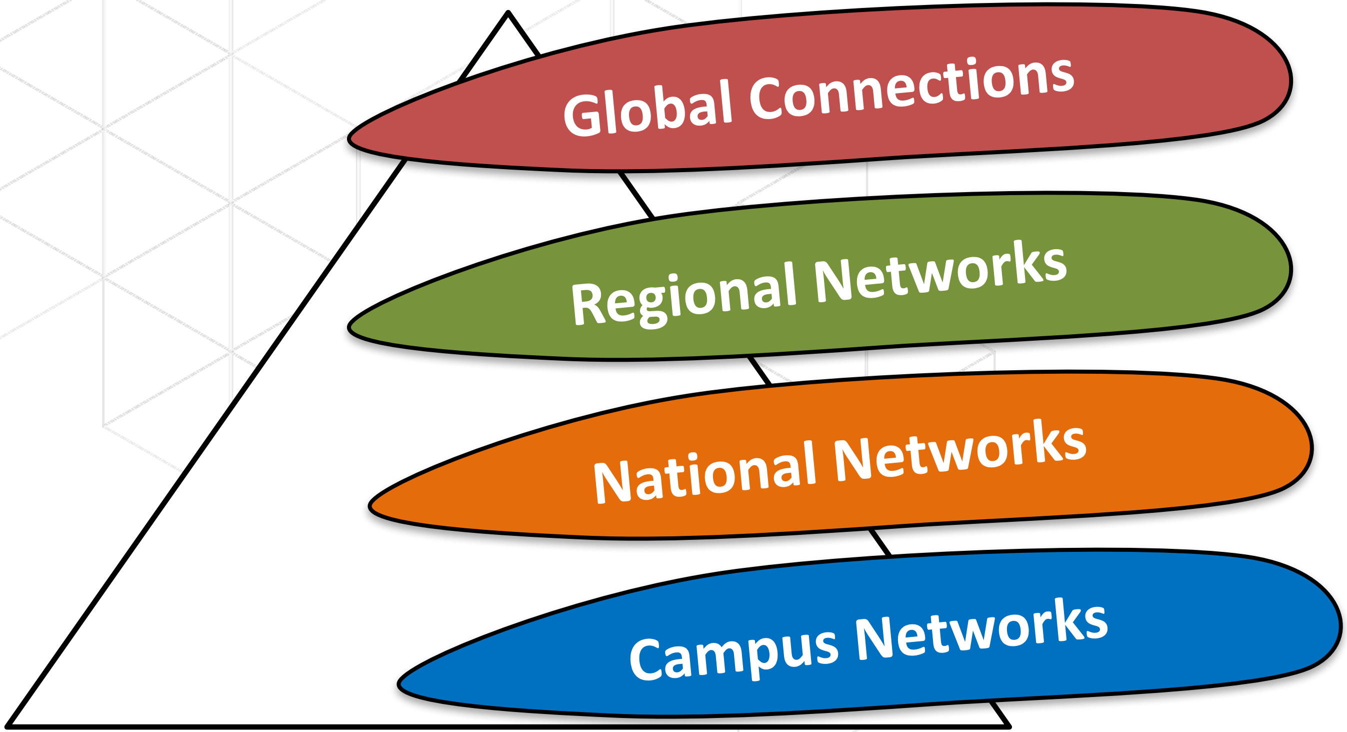
Implications for NRENs

Amreesh Phokeer
R&D Manager
amreesh@afrinic.net

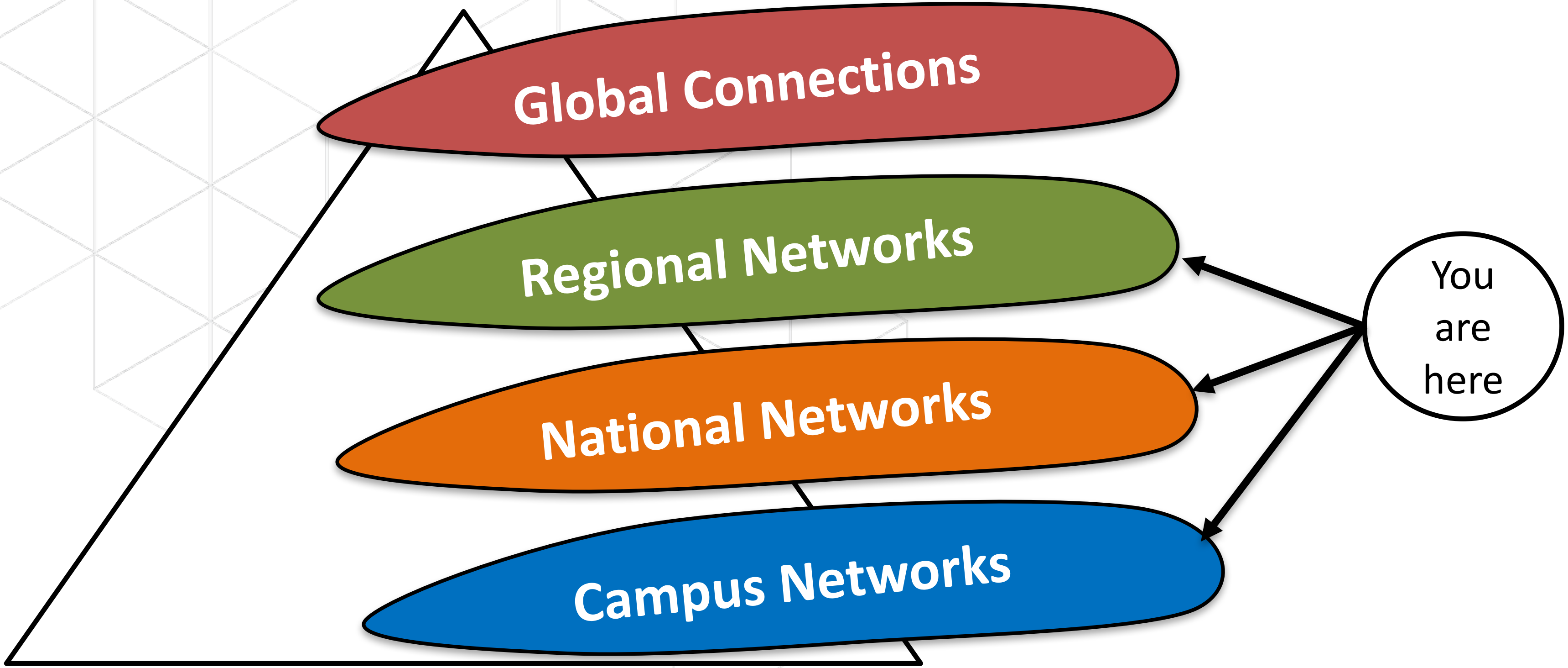
WACREN 2018

www.afrinic.net blog.afrinic.net /afrinic

NREN Ecosystem



NREN Ecosystem



Global Connections

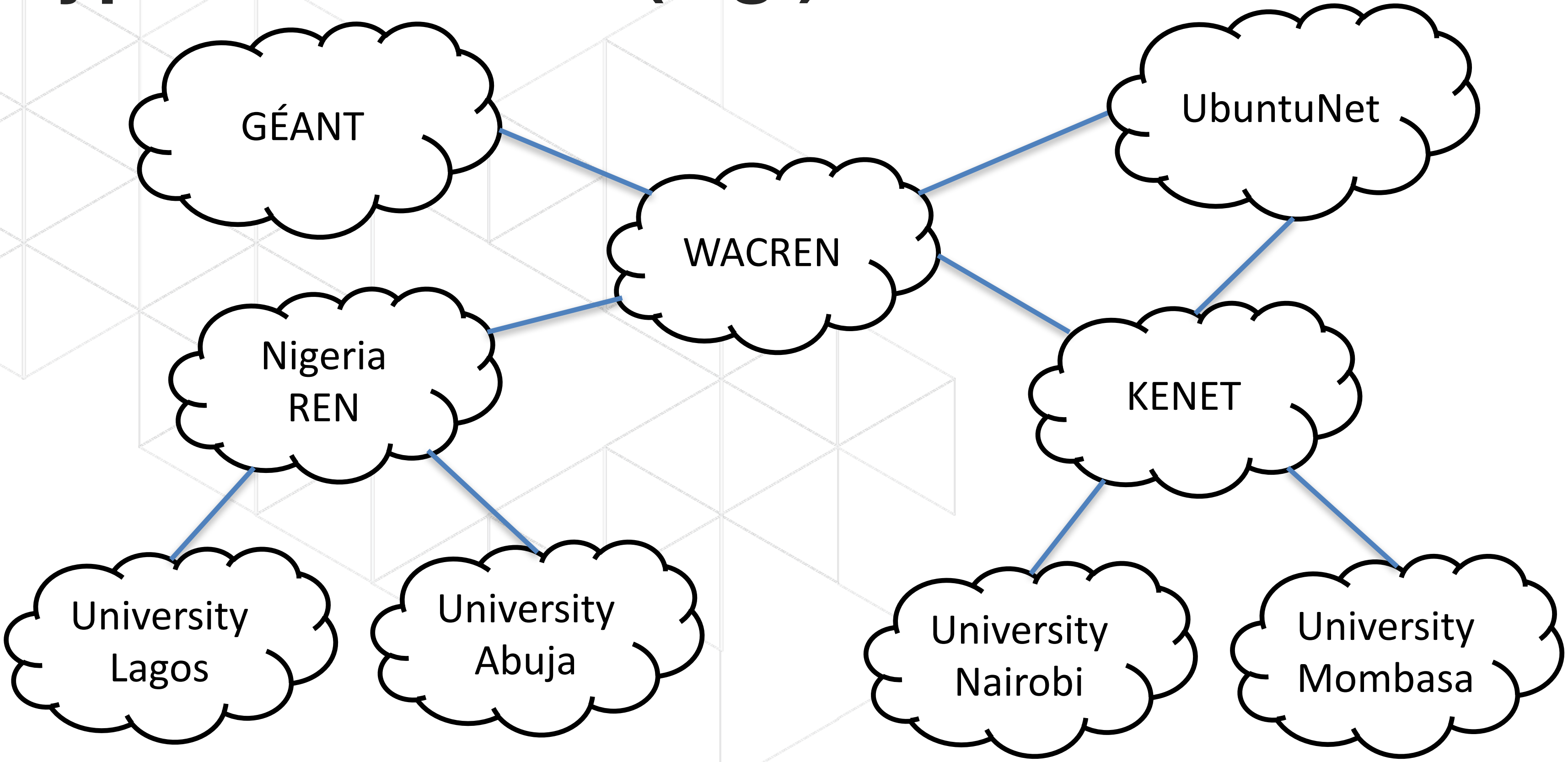
Regional Networks

National Networks

Campus Networks

You are here

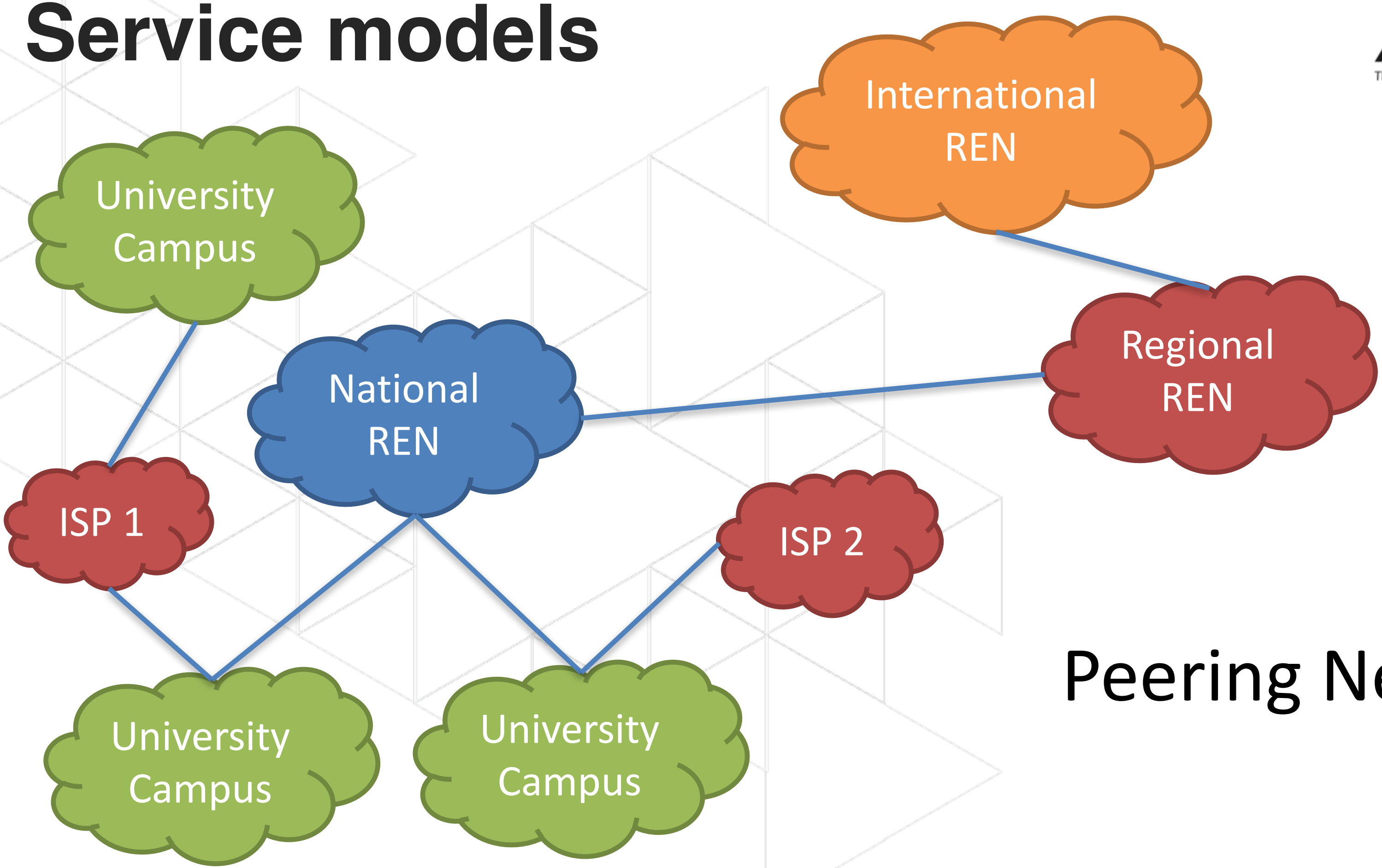
Typical scenario (e.g.)



Two modes of operations

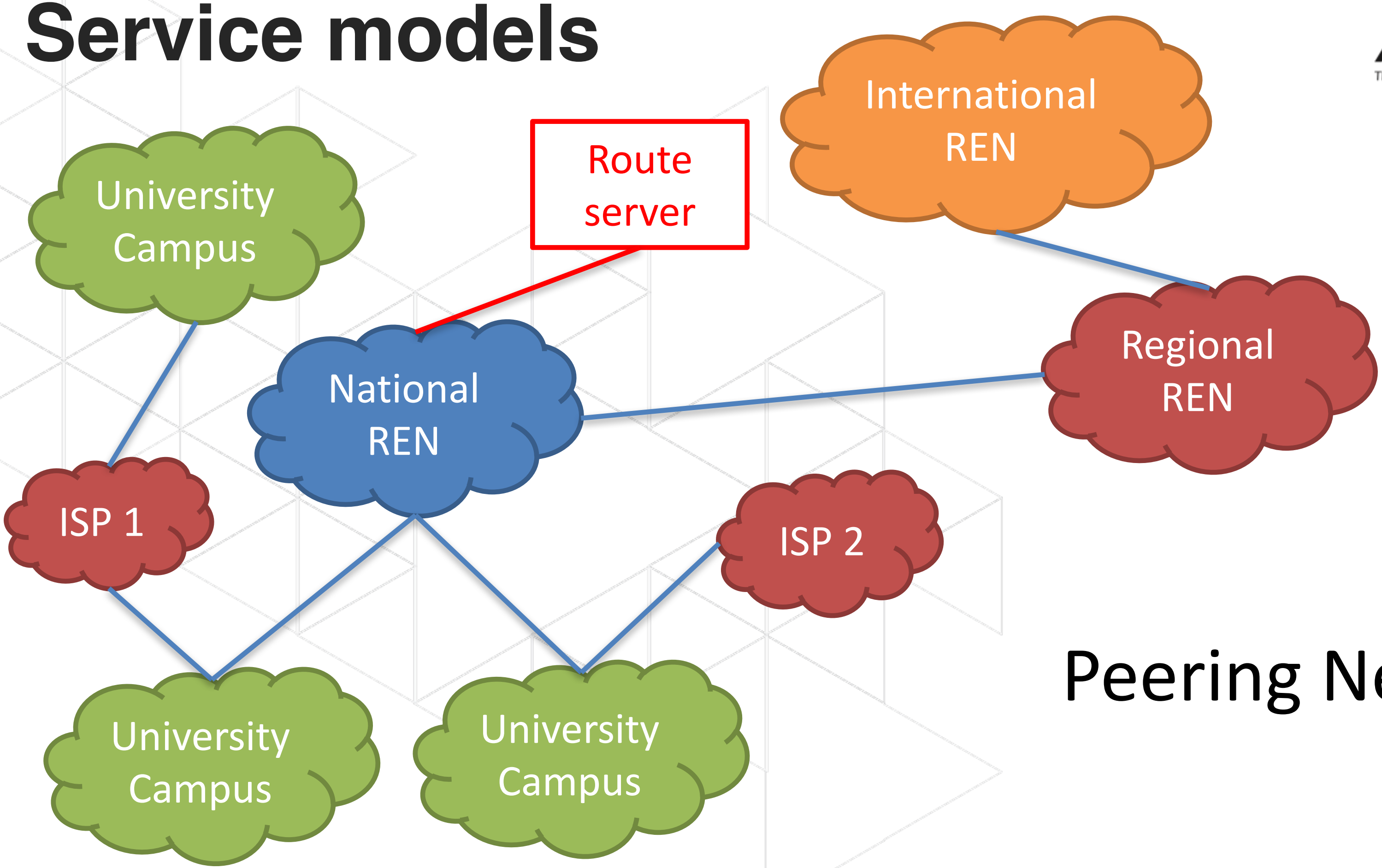
1. NREN as a peering network
   - Allow traffic exchange between members
   - Provide regional/international connections
   - Connects with local IXPs
2. NREN as an ISP
   - Sole connectivity provider
   - Also acts as peering network

Service models



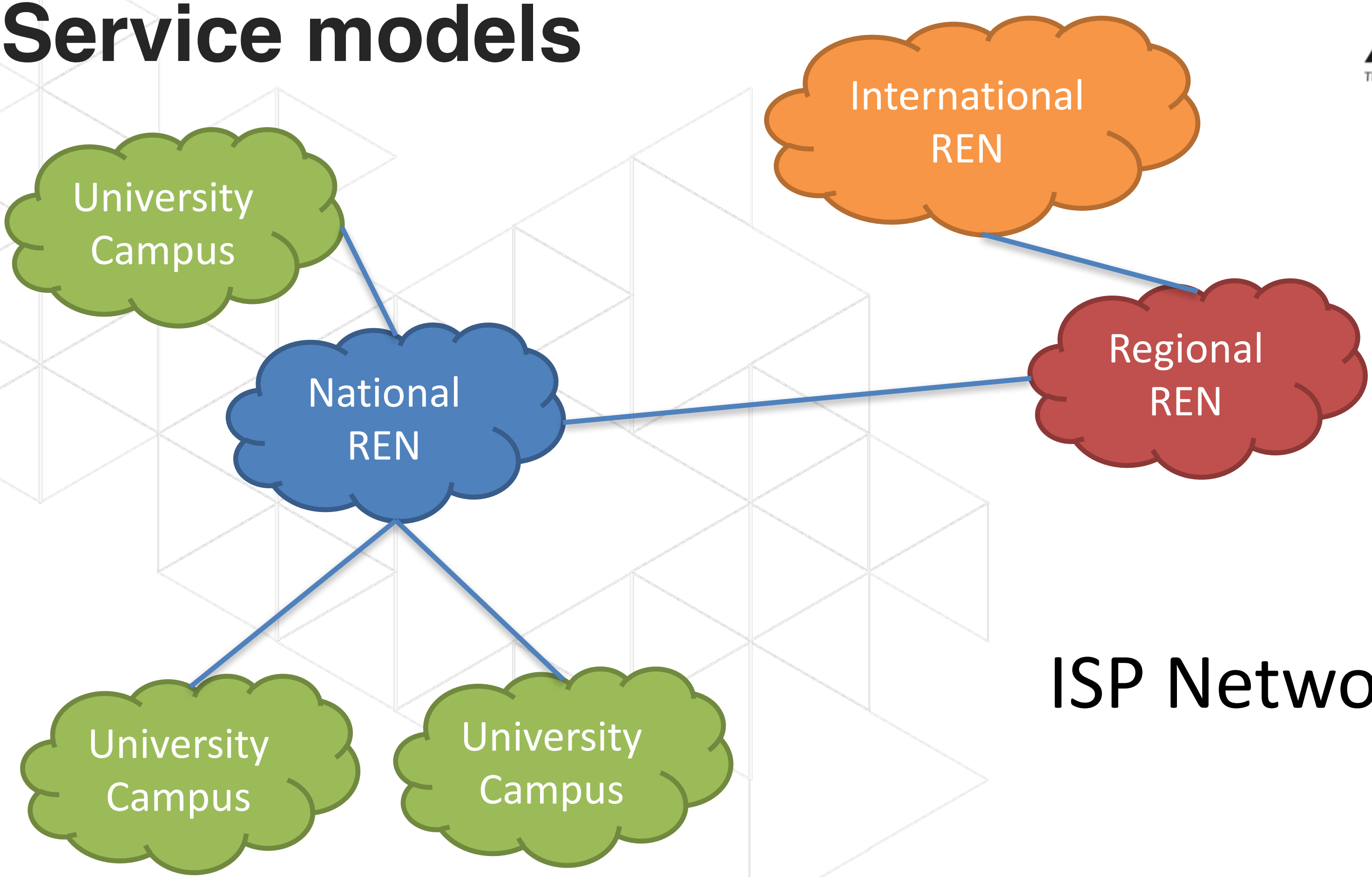
Peering Network

Service models



Peering Network

Service models

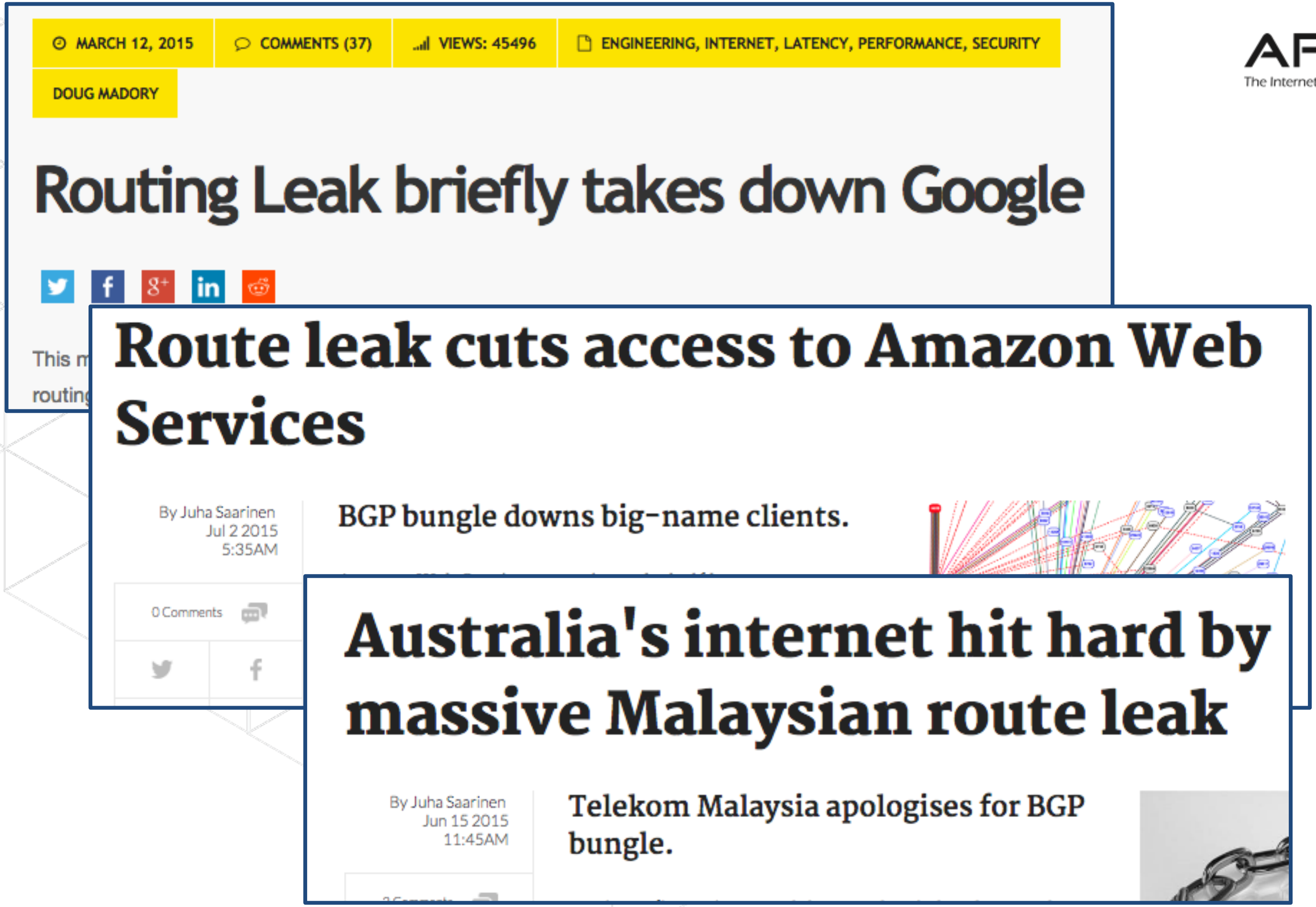


ISP Network

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)



MARCH 12, 2015 | COMMENTS (37) | VIEWS: 45496 | ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY

DOUG MADORY

Routing Leak briefly takes down Google

This m

routing

Route leak cuts access to Amazon Web Services

By Juha Saarinen
Jul 2 2015
5:35AM

0 Comments

BGP bungle downs big-name clients.

Australia's internet hit hard by massive Malaysian route leak

By Juha Saarinen
Jun 15 2015
11:45AM

Telekom Malaysia apologises for BGP bungle.

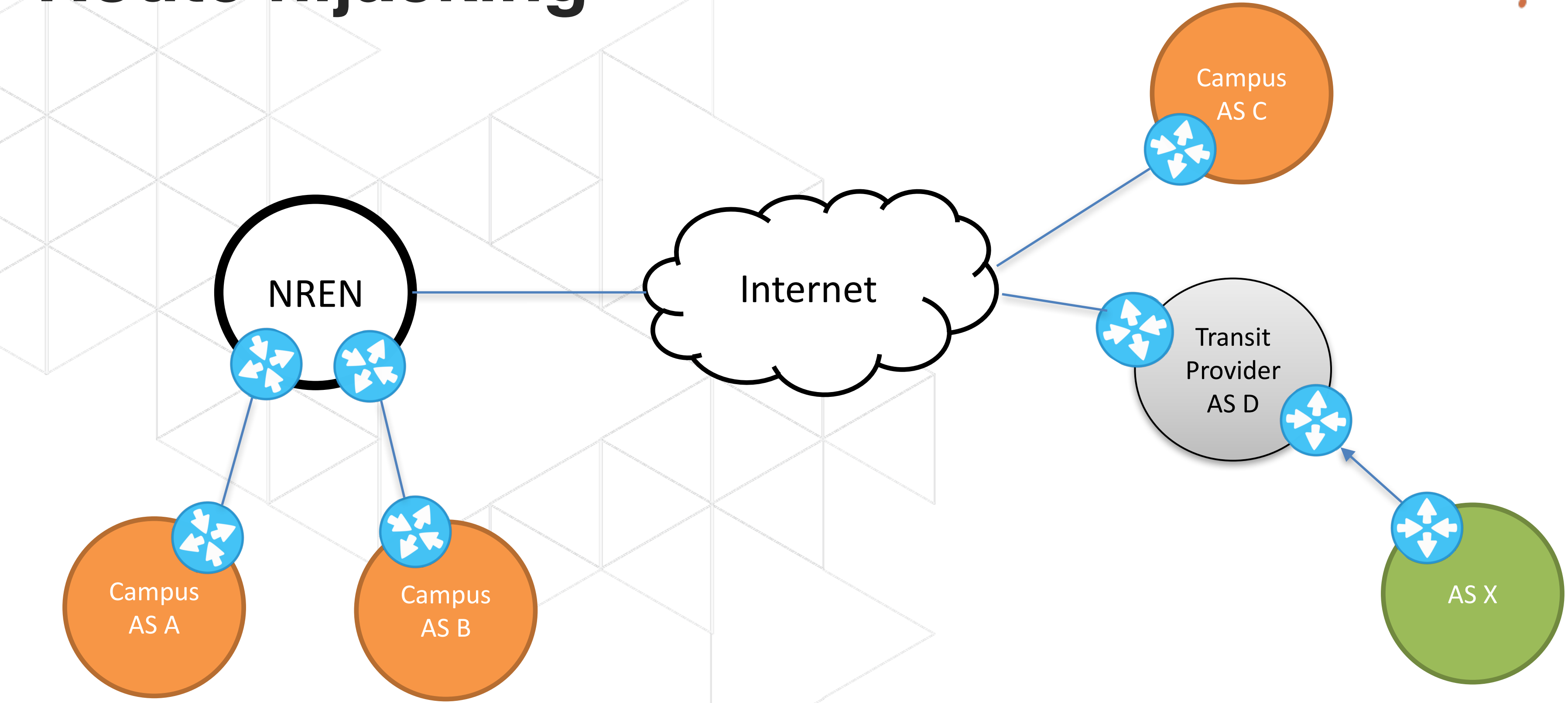
Route hijacking

- 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

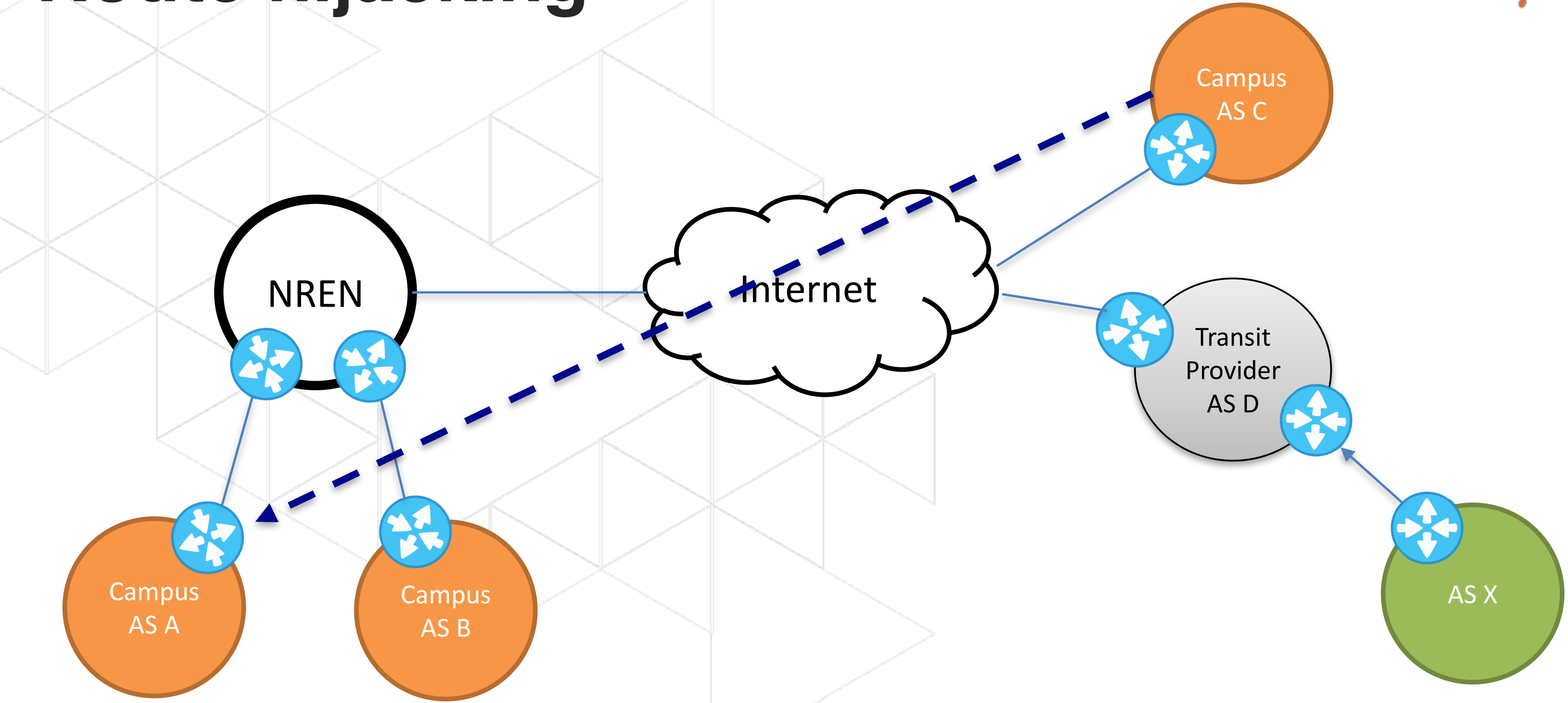
Route hijacking



2001:db8:1001::/48
192.0.2.0/24

2001:db8:2002::/48
198.51.100.0/24

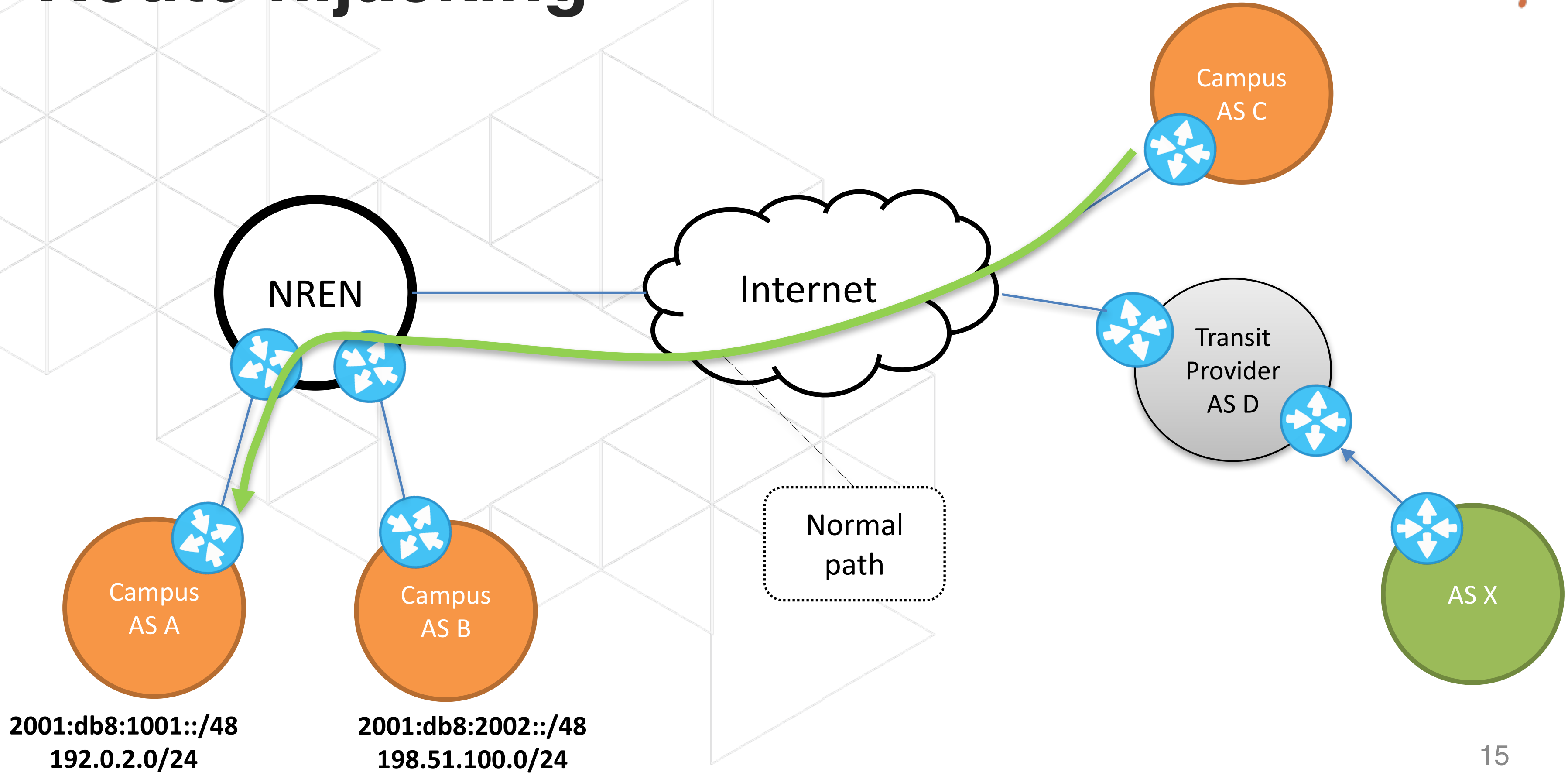
Route hijacking



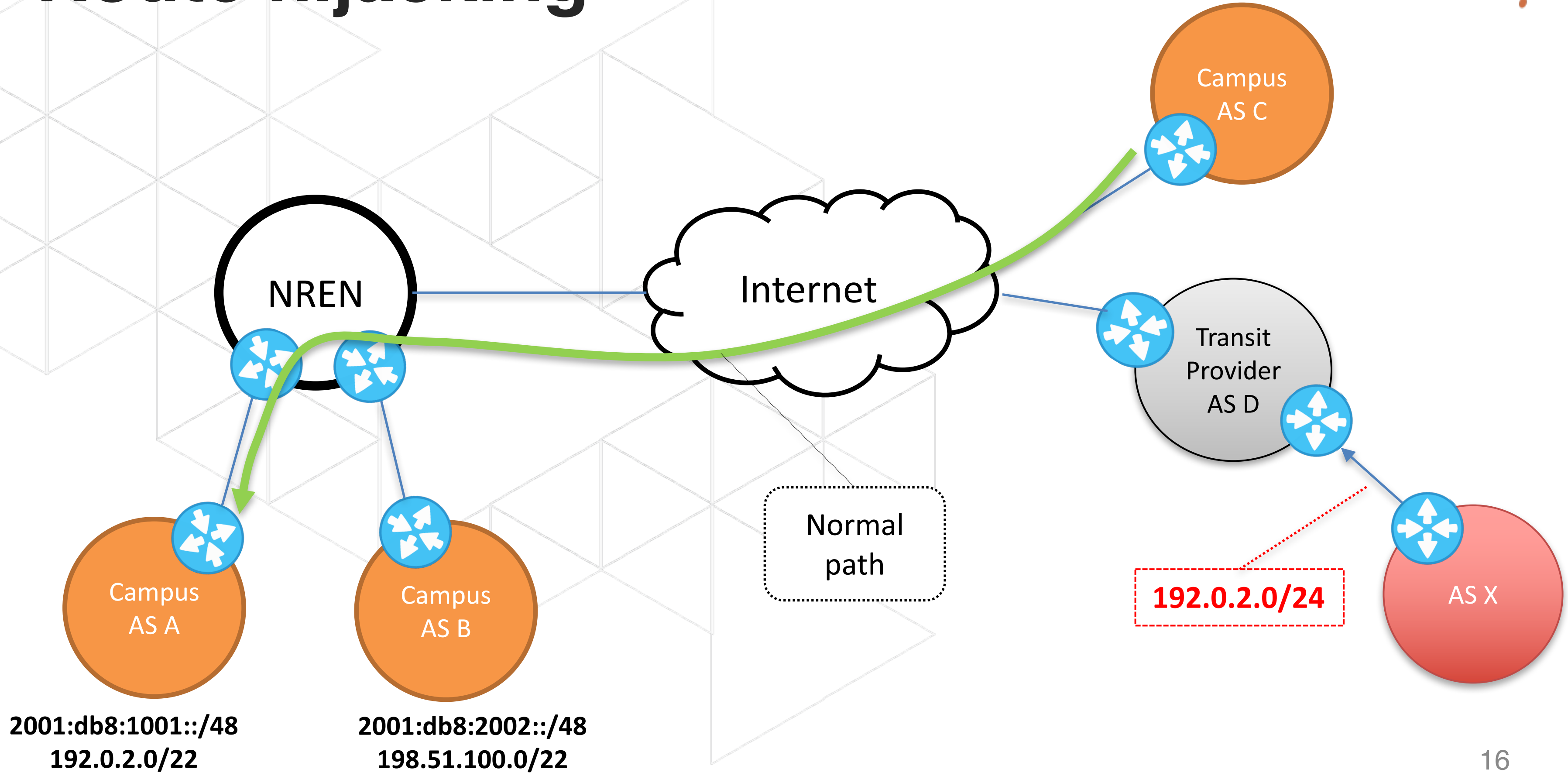
2001:db8:1001::/48
192.0.2.0/24

2001:db8:2002::/48
198.51.100.0/24

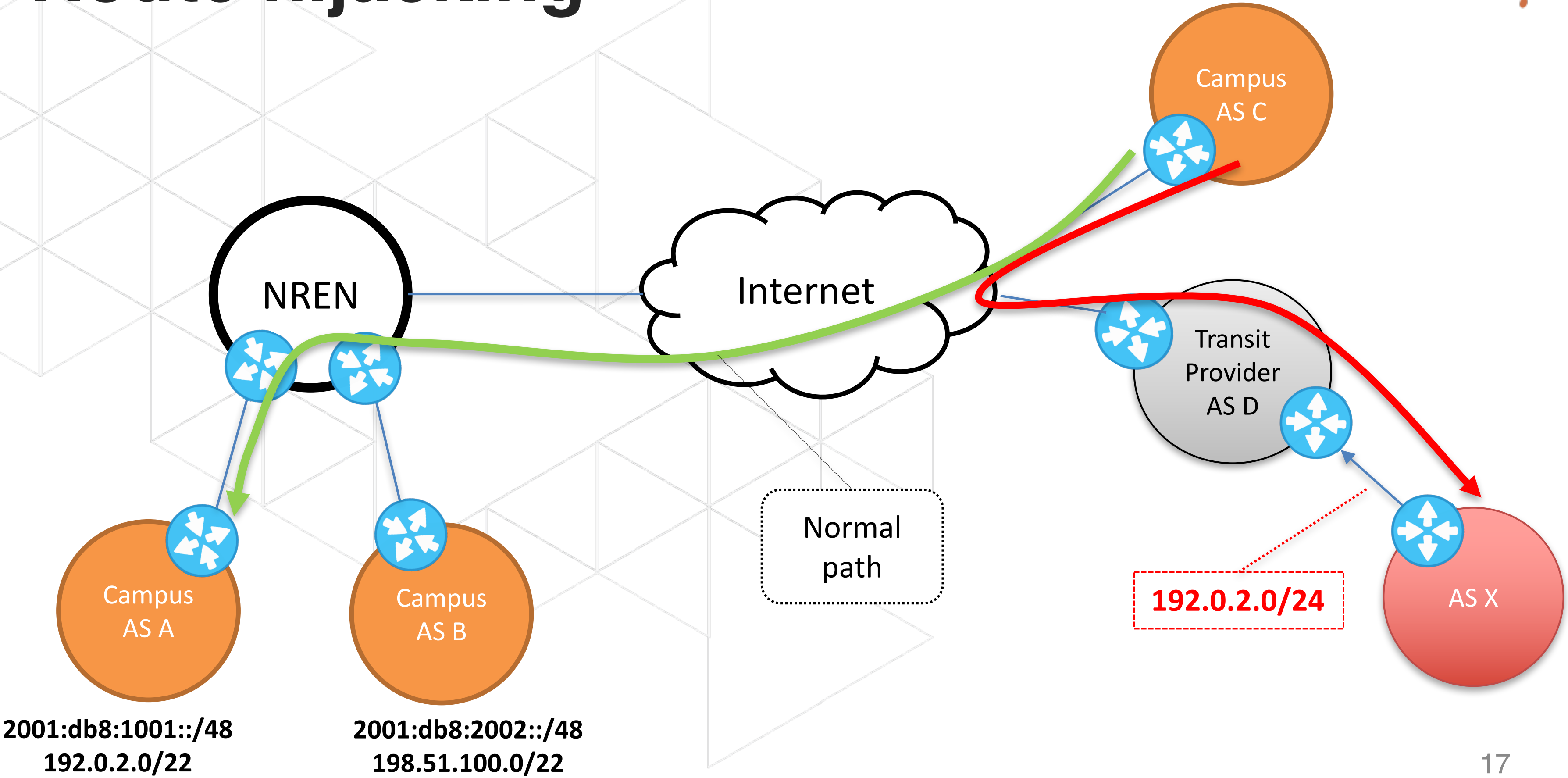
Route hijacking



Route hijacking



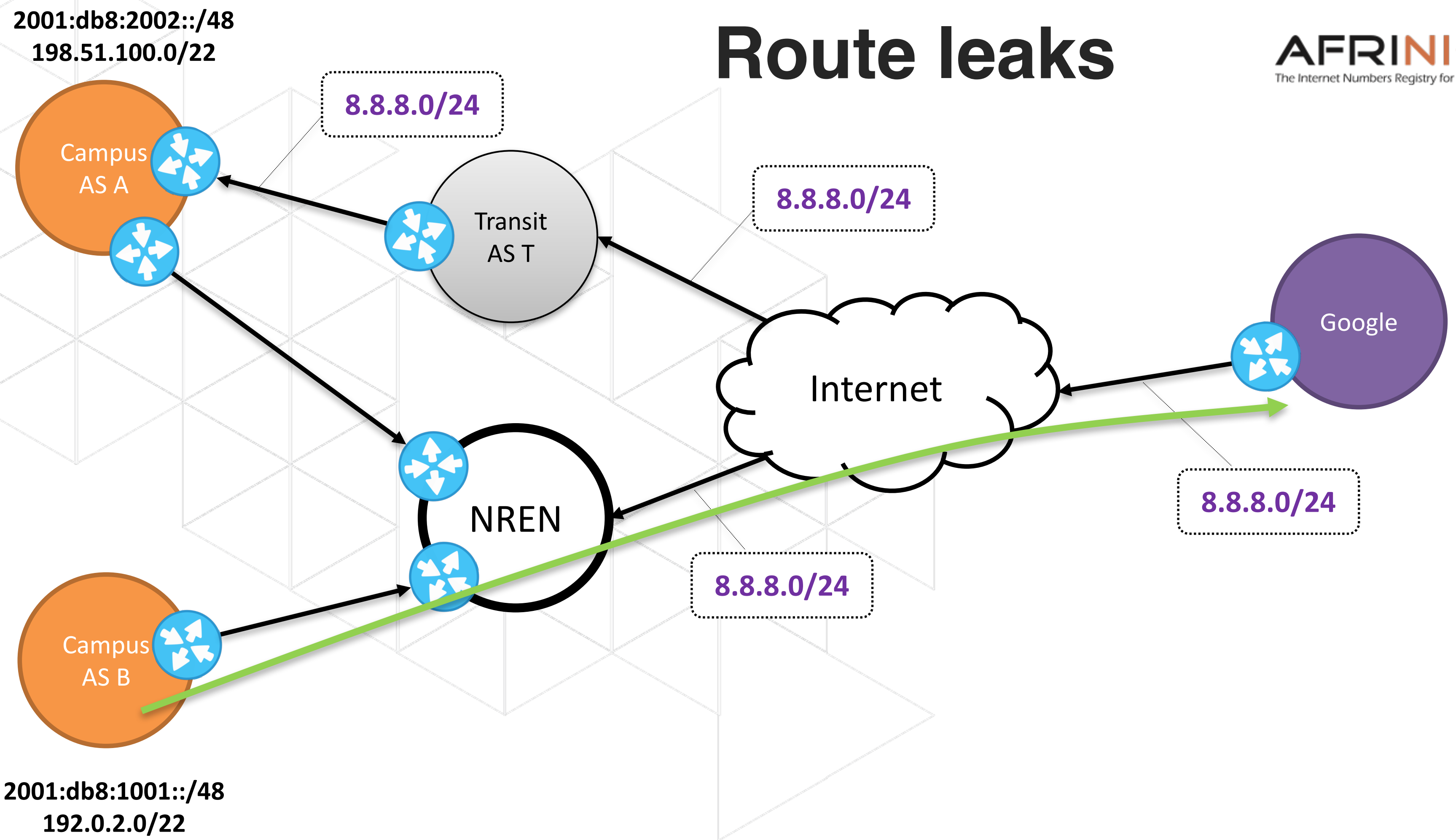
Route hijacking



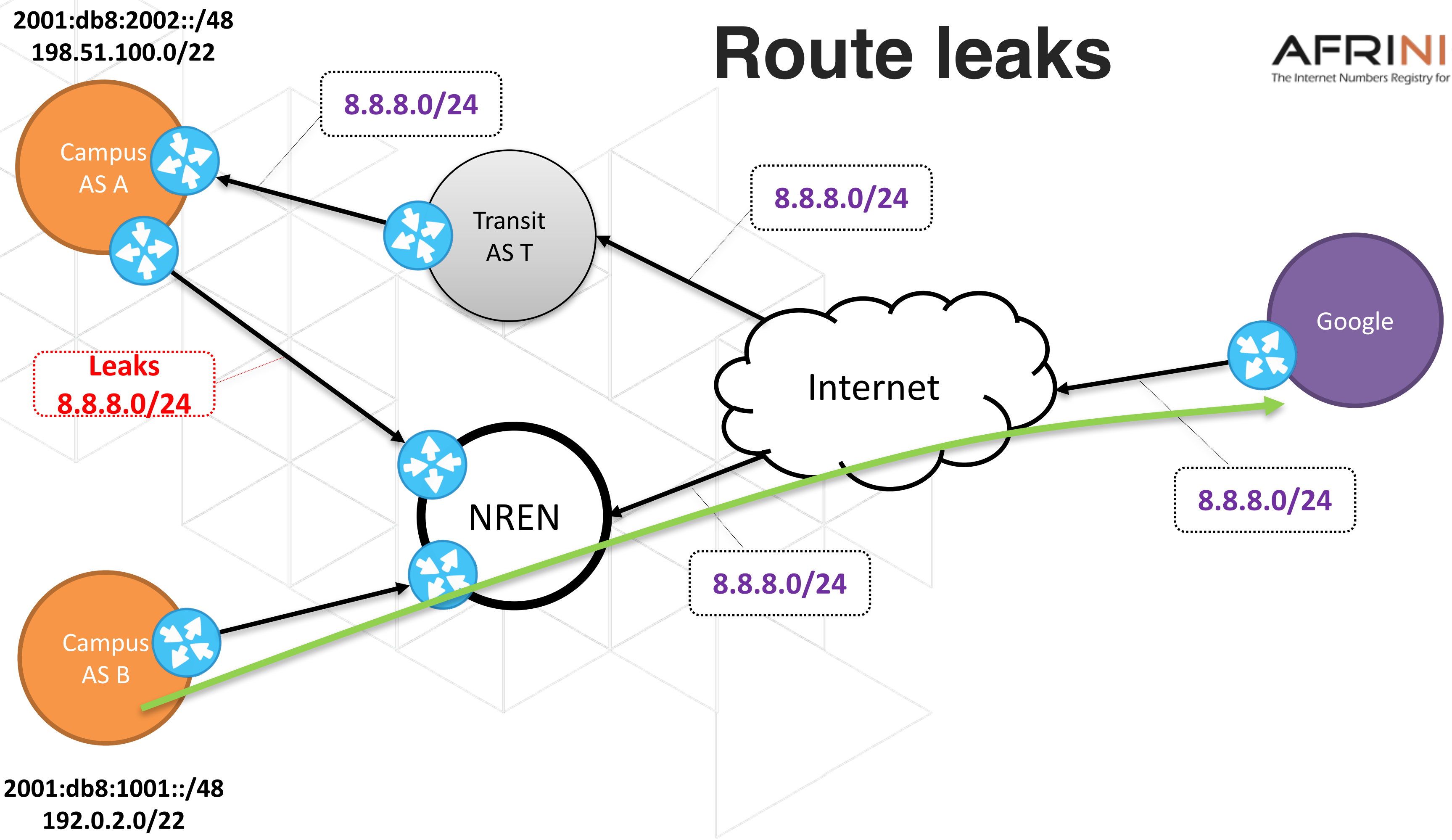
Route leaks

- 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

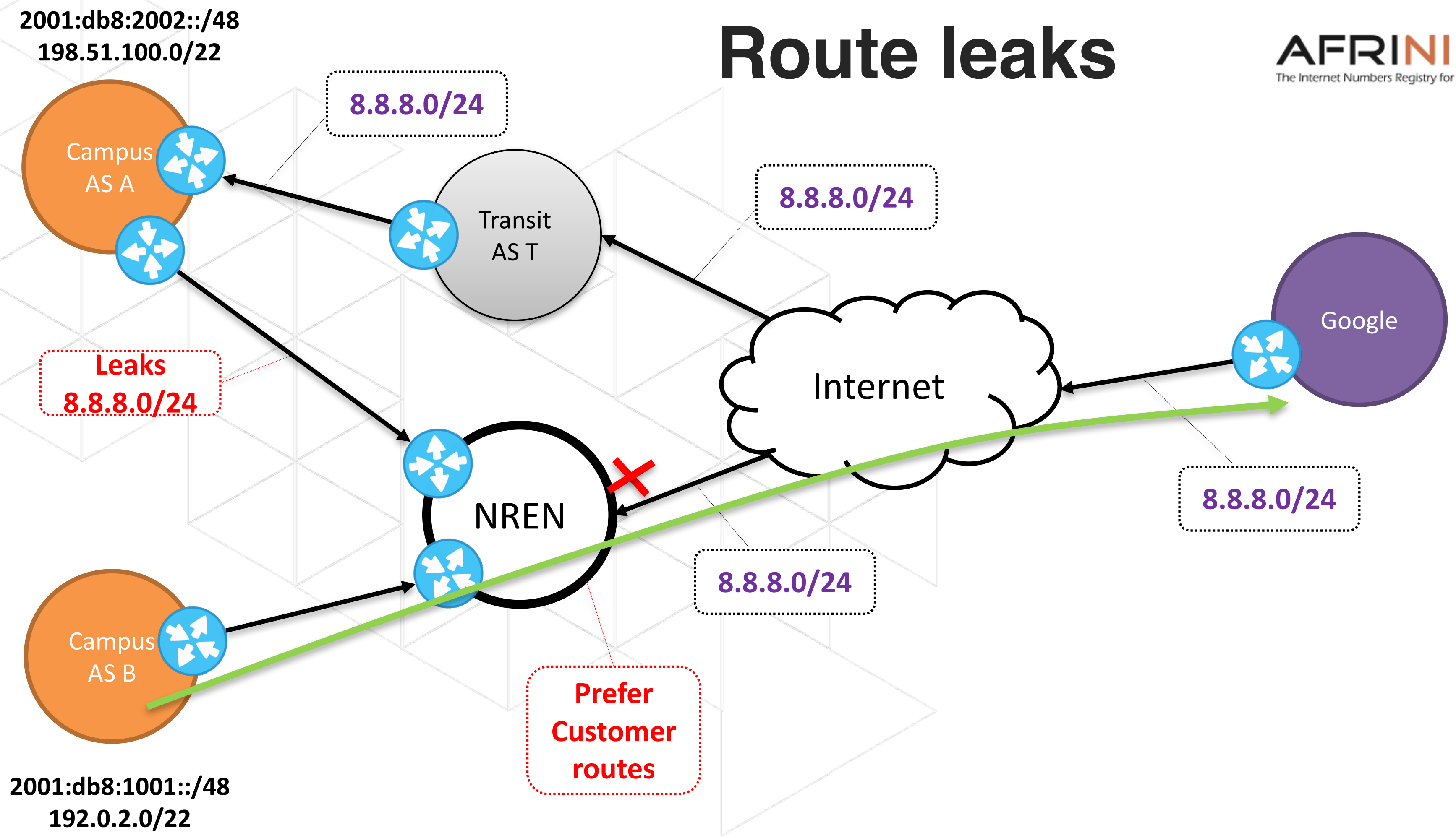
Route leaks


2001:db8:2002::/48
198.51.100.0/22
8.8.8.0/24
Campus
AS A
Transit
AS T
8.8.8.0/24
Google
Internet
NREN
8.8.8.0/24
8.8.8.0/24
Campus
AS B
2001:db8:1001::/48
192.0.2.0/22

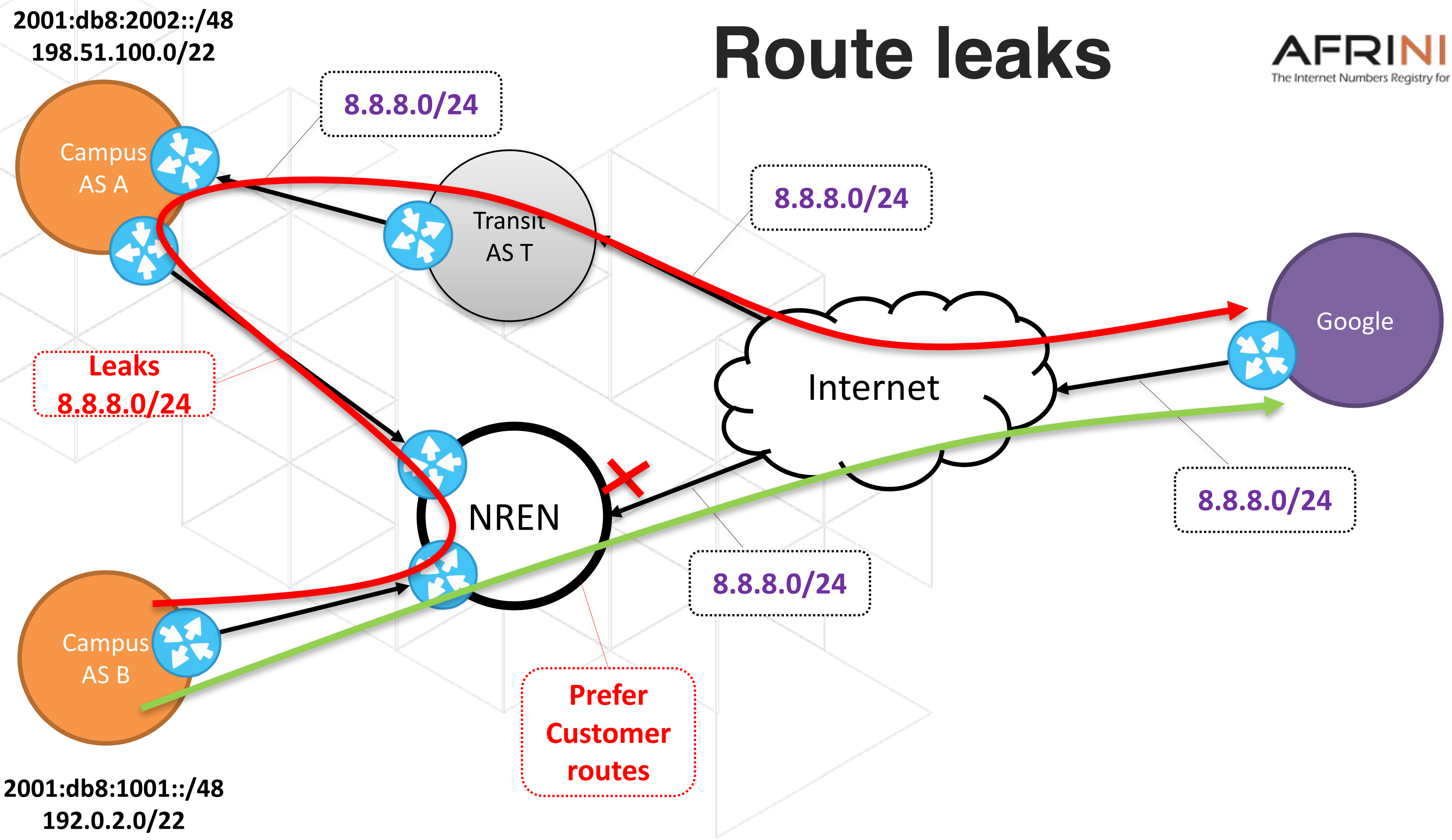
Route leaks


2001:db8:2002::/48
198.51.100.0/22
Campus
AS A
8.8.8.0/24
Transit
AS T
8.8.8.0/24
Leaks
8.8.8.0/24
Internet
Google
NREN
8.8.8.0/24
8.8.8.0/24
Campus
AS B
2001:db8:1001::/48
192.0.2.0/22

Route leaks


2001:db8:2002::/48
198.51.100.0/22
Campus AS A
8.8.8.0/24
Transit AS T
8.8.8.0/24
Google
Internet
Leaks 8.8.8.0/24
NREN
8.8.8.0/24
8.8.8.0/24
Campus AS B
Prefer Customer routes
2001:db8:1001::/48
192.0.2.0/22

Route leaks


2001:db8:2002::/48
198.51.100.0/22
Campus AS A
8.8.8.0/24
Transit AS T
8.8.8.0/24
Google
Leaks 8.8.8.0/24
Internet
NREN
8.8.8.0/24
8.8.8.0/24
Campus AS B
Prefer Customer routes
2001:db8:1001::/48
192.0.2.0/22

Solutions

Yes a few:

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

Issues

- Lack of incentives for deployment
- Lack of reliable data

Solutions

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 2017:

- **13,395** total incidents (outages or route leaks)
- Over **10%** of ASNs were affected
- **3,106** ASNs were victim of a least one routing incident
- **1,546** networks caused routing incidents

Source: Internet Society

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
3. **Coordination** – Facilitate global operational communication and coordination between network operators
   - Maintain up-to-date data on IRR, WHOIS, etc
4. **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

Join Us for AIS’18

AFRICA
INTERNET
SUMMIT’18
DAKAR SENEGAL
29 APRIL - 11 MAY 2018