RIPE NCC
RIPE NETWORK COORDINATION CENTRE

MANRS

How to behave on the internet

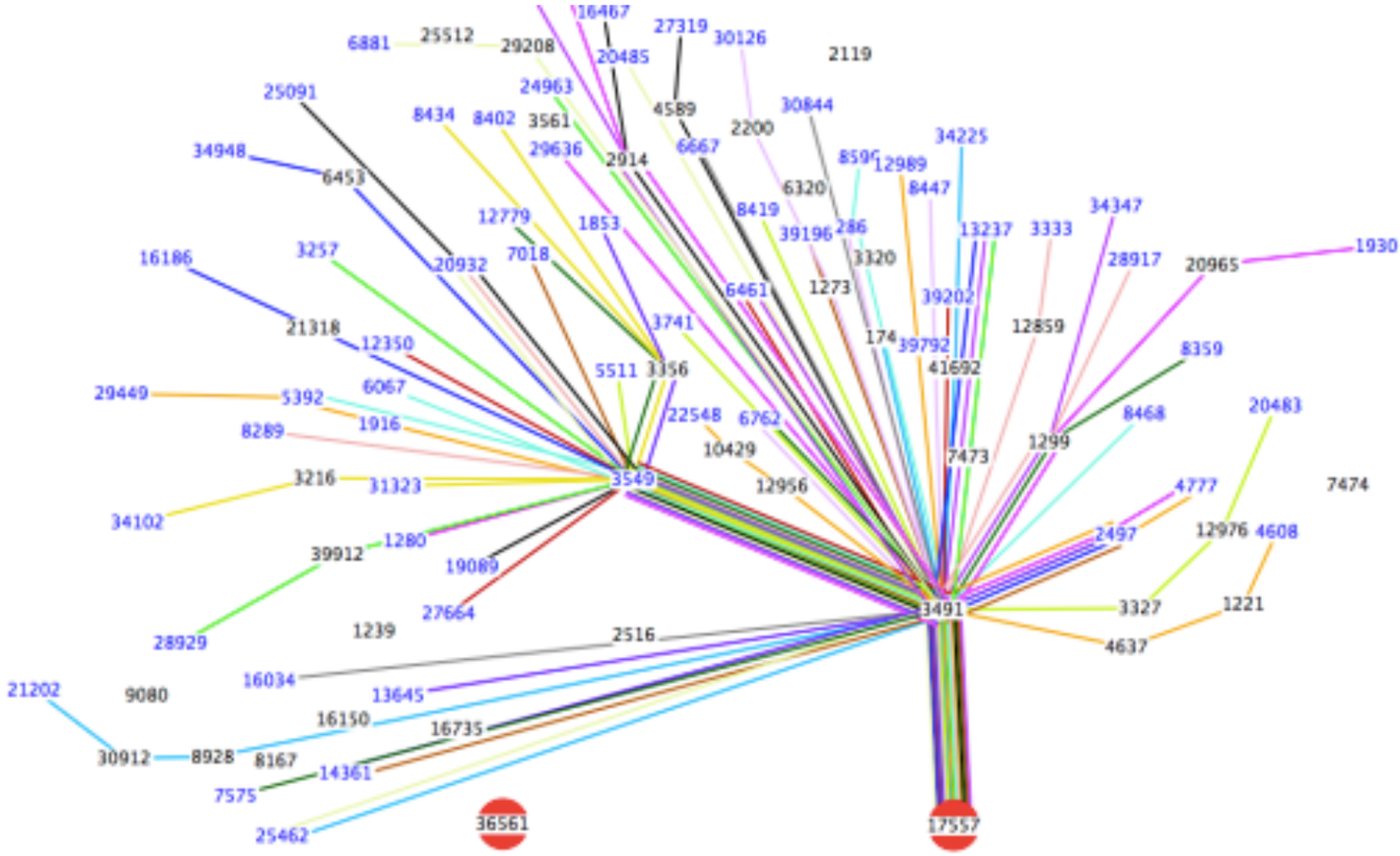
Massimiliano Stucchi | TOP-IX Meeting | January 2017

BGP

- BGP is based on trust
  - No built-in validation
  - Chain of trust is hard to establish
  - Data scattered over different sources

Routing Incidents Types

- Misconfiguration
  - No malicious intention
  - Software bugs
- Malicious
  - Competition
  - Claiming “unused” space
- Targeted Traffic Misdirection
  - Collect and/or tamper with data



Enters

MANRS - goals

- Mutually Agreed Norms for Routing Security

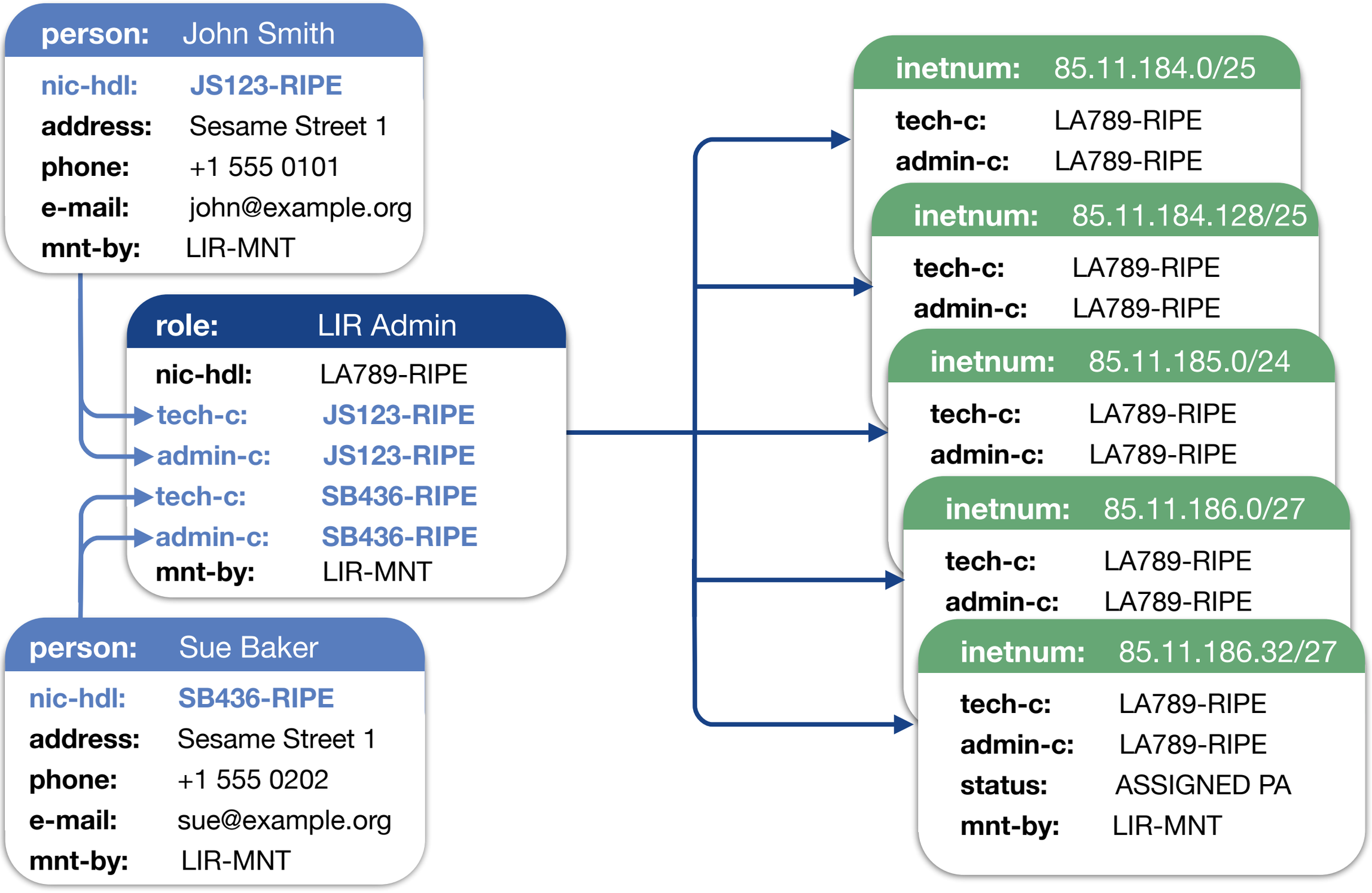
- Define four concrete actions network operators should implement

- Build a visible community of security-minded operators

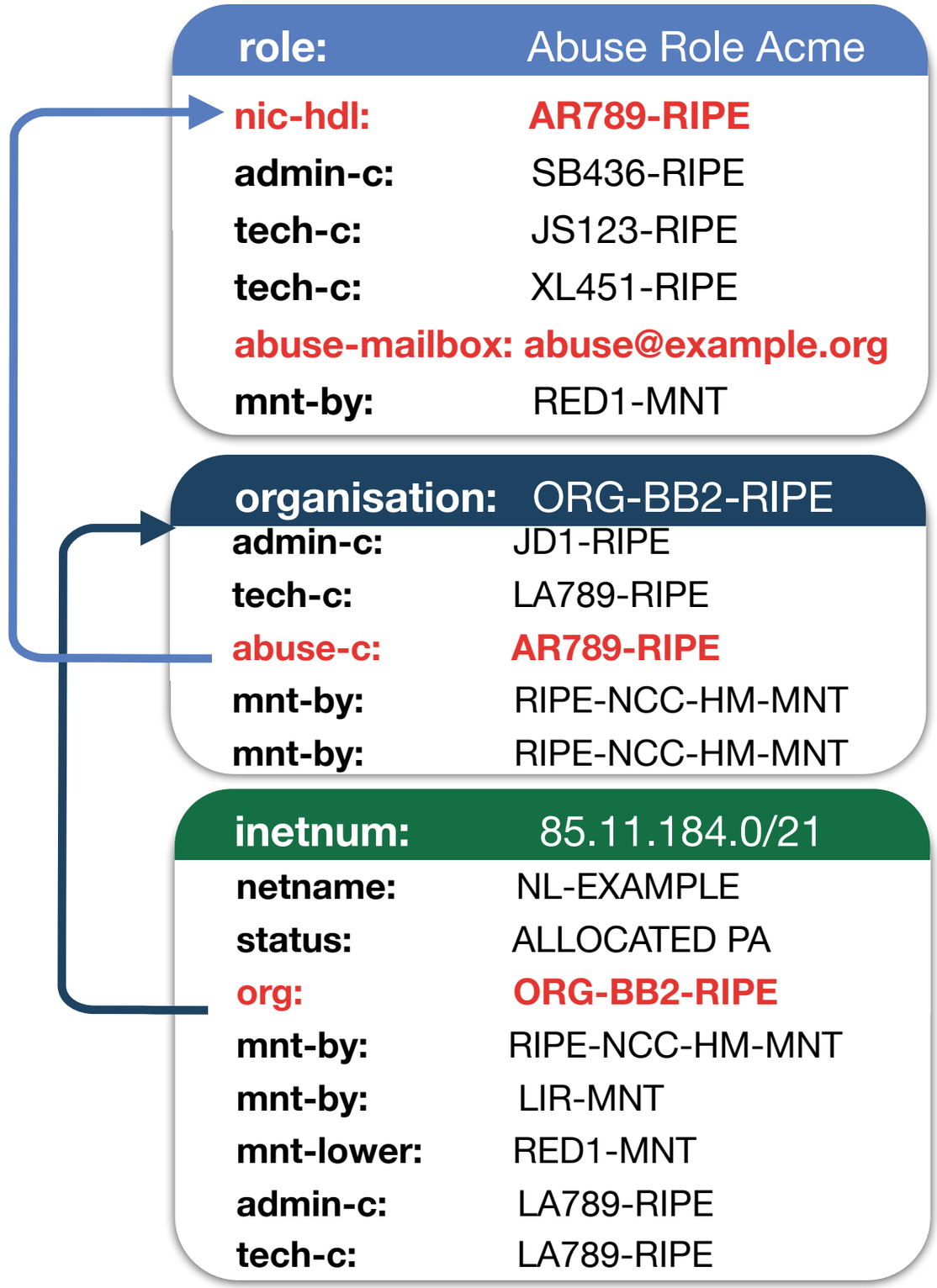
1 - Coordination

- Keep your contacts updated
  - RIPE Database (or any other RIR)
  - LIR Portal
  - PeeringDB

Person, role and inet{6,}num object



Abuse contacts for allocations



LIR / LIR Portal

Name of the organisation
or person operating the LIR

Contact Information

- Postal address
- Phone numbers
- Email addresses

User Accounts

Billing details

- Allocations
- PI assignments

IPv4 & IPv6

- Allocations
- PI assignments

AS Numbers

Preferences

2 - Validation

- Communicate which BGP announcements are correct
  - Route objects
  - RPKI
  - BGPSec
- Document your policy

Validation objects

aut-num	IRR	Policy Documentation
route/route6	IRR	NLRI/Origin
as-set	IRR	Customer cone
ROA	RPKI	NLRI/Origin

Registering IPv4 Routes

inetnum:	192.168.0.0/24
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
mnt-by:	RIPE-NCC-HM-MNT
mnt-routes:	LIR-MNT

aut-num:	AS64512
as-name:	GREEN-AS
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
mnt-by:	LIR-MNT

route:	192.168.0.0/24
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
origin:	AS64512
mnt-by:	LIR-MNT

Registering IPv6 Routes

inet6num:	2001:db8::/32
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
mnt-by:	RIPE-NCC-HM-MNT
mnt-routes:	LIR-MNT

aut-num:	AS64512
as-name:	GREEN-AS
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
mnt-by:	LIR-MNT

route6:	2001:db8::/32
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
origin:	AS64512
mnt-by:	LIR-MNT

aut-num Object and Routing Policy

aut-num:	AS64512
descr:	RIPE NCC Training Services
as-name:	GREEN-AS
tech-c:	LA789-RIPE
admin-c:	JD1-RIPE
import:	from AS64444 accept ANY
import:	from AS64488 accept ANY
export:	to AS64444 announce AS64512
export:	to AS64488 announce AS64512
mnt-by:	LIR-MNT
source:	RIPE

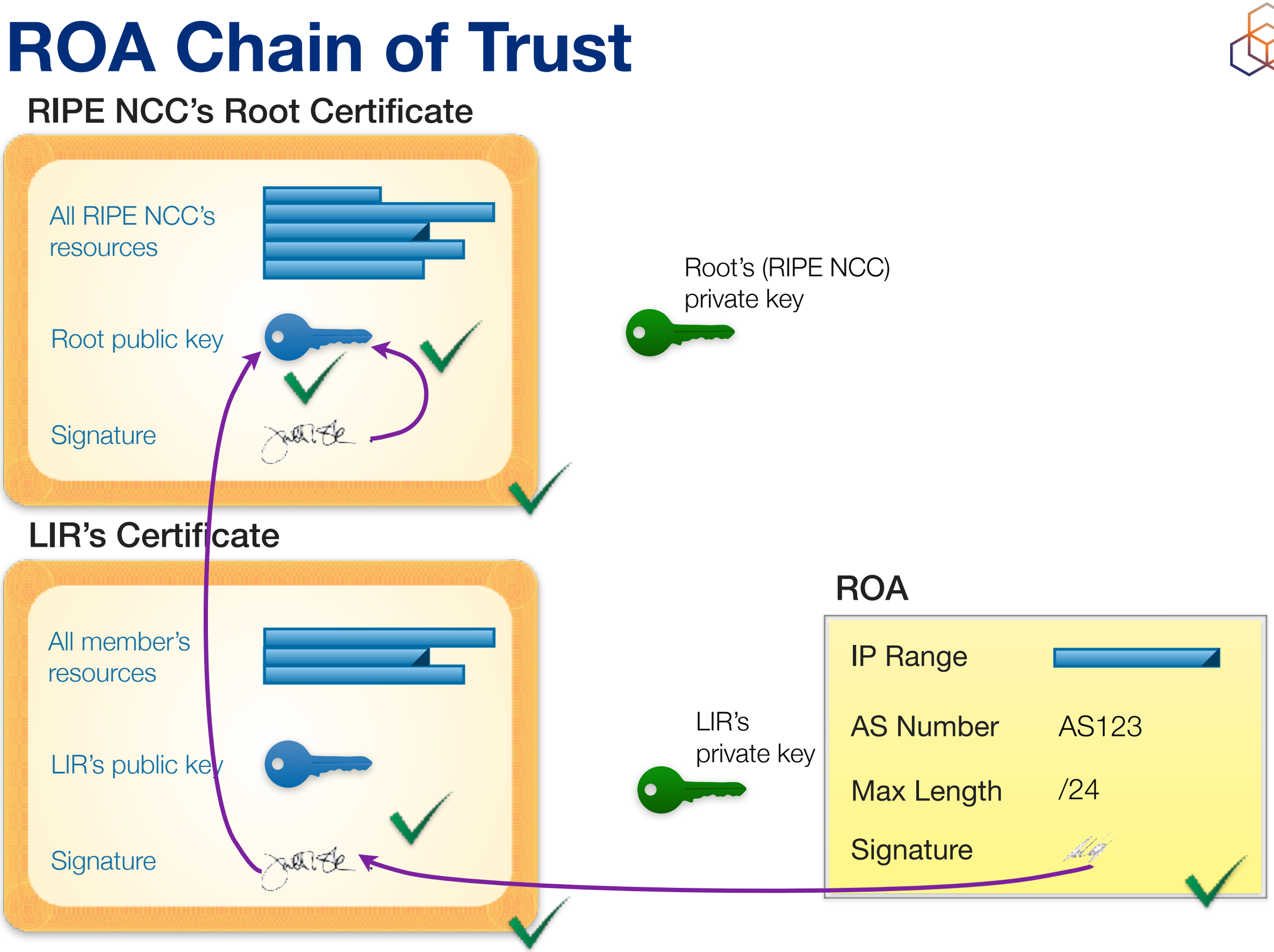
Why Publish Your Routing Policy?

- Some transit providers and IXPs (Internet Exchange Points) require it
  - They build their filters based on the Routing Registry
- Contributes to routing security and stability
  - Let people know about your intentions
- Can help in troubleshooting
  - Which parties are involved?

ROA (Route Origin Authorisation)

- LIRs can use their certificate to create a ROA for each of their resources (IP address ranges)
  - Signed by the root's private key
- ROA states
  - Address range
  - Which AS this is announced from (freely chosen)
  - Maximum length (freely chosen)
- You can have multiple ROAs for an IP range
- ROAs can overlap

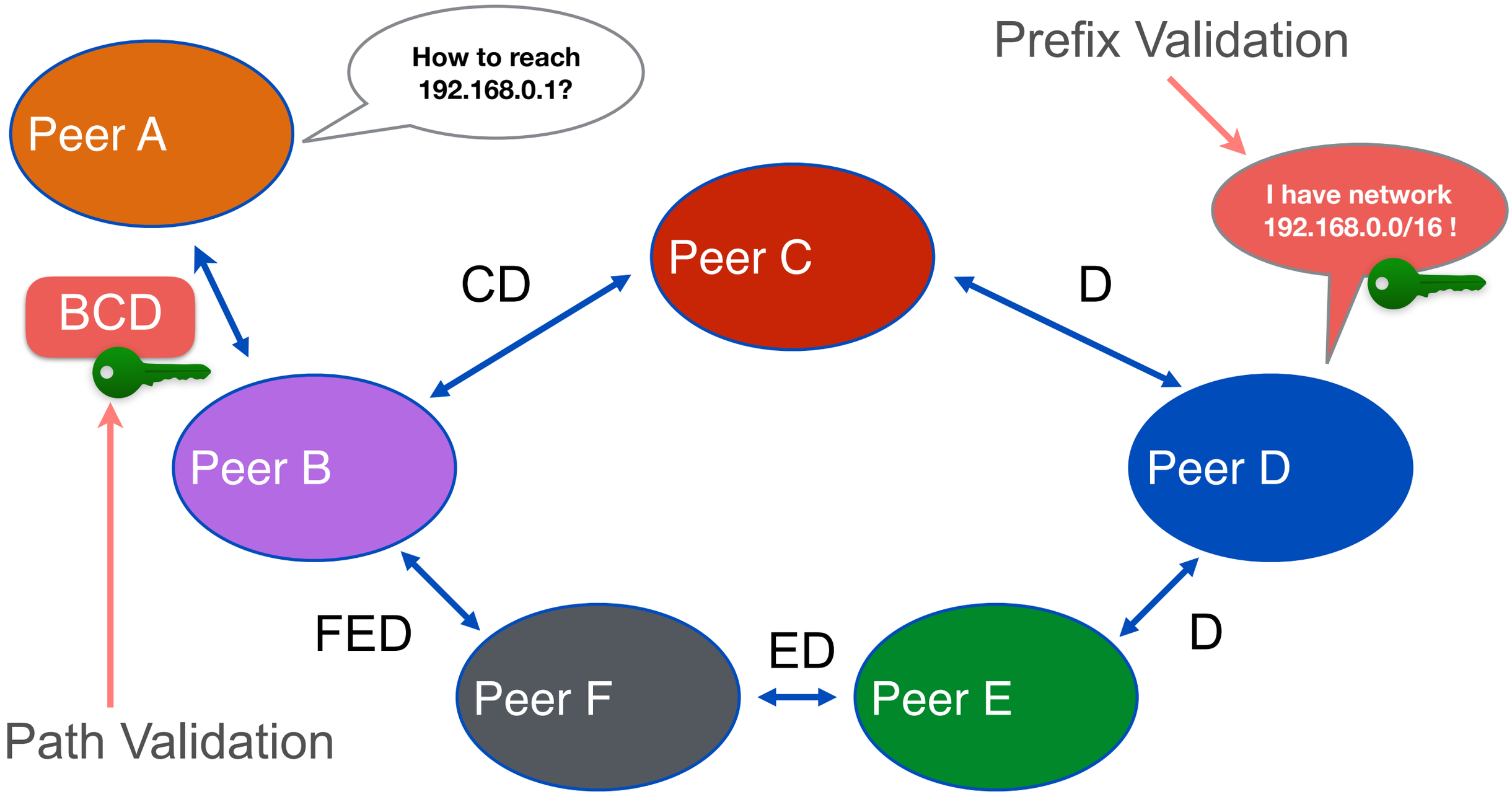
ROA Chain of Trust



BGPSEC Operations

- New, optional, transitive attribute, to carry digitally signed route info
- Support is negotiated between routers, non BGPSEC router will not be burdened by big UPDATE messages
- Data is never sent through non BGPSEC ASes, so secure paths exist only for contiguous sequences of ASes
- Incremental deployment is possible

BGPSEC


Peer A
How to reach
192.168.0.1?
Prefix Validation
I have network
192.168.0.0/16 !
BCD
CD
Peer C
D
Peer B
Peer D
FED
ED
D
Peer F
Peer E
Path Validation

3 - Anti-spoofing

- Implement source address validation
- Document your policy

Reverse Path Forwarding

- Called uRPF (Unicast Reverse Path Forwarding)
- Checks if an entry exists in the routing table before accepting the packet and forwarding it
- Two main modes
  - Loose
  - Strict

Strict and Loose RPF

- Strict
  - Checks if the entry is in the routing table
  - and the route points to the receiving interface
- Loose
  - Simply checks that an entry exists for the route in the routing table

4 - Filtering

- Define a clear routing policy
- Apply due diligence in checking your announcements and your customers’

Filtering Principles

- Filter as close to the edge as possible
- Filter as precisely as possible
- Filter both source and destination where possible

Bogons

- Routes you shouldn't see in the routing table
  - Private addresses
  - Non-allocated space
  - Reserved space (Future use, Multicast, etc.)
- You should have filters applied so that these routes are not advertised to or propagated through the Internet
- Team Cymru provides list or BGP feed
  - http://www.team-cymru.org/bogon-reference-bgp.html

Prefix-lists

- Prefix lists are lists of routes you want to accept or announce
- Easy to use but not highly scalable
- You can create them manually or automatically
  - With data from RIPE DB or other Internet Routing Registry
- Or using a tool
  - Level3 Filtergen
  - bgpq3
  - IRRexplorer

Building prefix lists with bgpq3

```
$ bgpq3 -4 -l AS64500-v4 AS64500:AS-ALL

no ip prefix-list AS64500-v4

ip prefix-list AS64500-v4 permit 203.0.113.0/24

ip prefix-list AS64500-v4 permit 192.0.2.0/24

ip prefix-list AS64500-v4 permit 198.51.100.0/24
```

Building prefix lists with bgpq3

```
$ bgpq3 -6 -l AS64500-v6 AS64500 AS64500:AS-CUSTOMERS

no ipv6 prefix-list AS64500-v6

ipv6 prefix-list AS64500-v6 permit 2001:db8:1000::/36

ipv6 prefix-list AS64500-v6 permit 2001:db8:1001::/48

ipv6 prefix-list AS64500-v6 permit 2001:db8:2002::/48
```

How to sign up

- Go to http://www.routingmanifesto.org/signup/
  - Provide the requested information

- Download the logo and use it

- Become an active MANRS participant

Questions

E-mail: mstucchi@ripe.net
Twitter: @stucchimax
Twitter: @TrainingRIPENCC

The End!

Край

Y Diwedd

Fí

Finis

النهاية

Соңы

Վերջ

Liðugt

Ende

Finvezh

Кінець

Konec

Kraj

Ënn

Fund

پایان

Kpaj

Lõpp

Beigas

Vége

Son

An Críoch

הסוף

Endir

Fine

Sfârşit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Tmiem

Koniec

Fim

Amaia

Loppu