CENIC
Connecting California

Tools and Techniques for MANRS Conformance

Christopher Bruton (he/him), Core Engineer at CENIC

APAN55, Kathmandu, Nepal

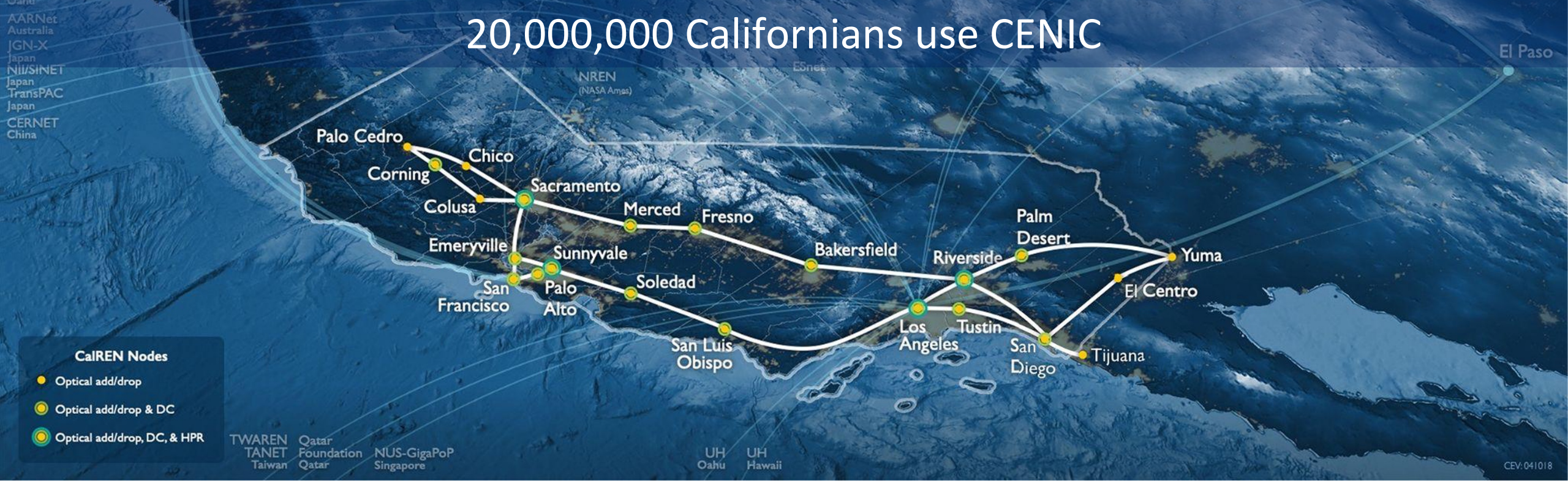
March 16, 2023

CENIC is a 501(c)(3) **with the mission to advance education and research statewide by providing the world-class network essential for innovation, collaboration, and economic growth.**

Charter Associates:

- California K-12 System
- California Community Colleges
- California State University System
- Stanford, Caltech, USC
- University of California System
- California Public Libraries
- Naval Postgraduate School

20,000,000 Californians use CENIC



- **8,000+ miles of optical fiber**
- **Members in all 58 counties connect via fiber-optic cable or leased circuits from telecom carriers**
- **Over 12,000 sites connect to CENIC**

- **A non-profit** chartered & governed by its members
- Collaborates with over **750 private sector partners and contributes > $100,000,000** to the CA Economy
- **24 plus years** of connecting California

MANRS: Mutually Agreed Norms for Routing Security

- CENIC recently became a MANRS Network Operator Participant in December 2022
- Participants commit to four actions:
  - Action 1: Filtering
  - Action 2: Anti-Spoofing (optional)
  - Action 3: Coordination
  - Action 4: Global Validation

MANRS

MANRS Observatory

Action 1: Prevent propagation of incorrect routing information

- **Generating prefix filters:**
  - We configure our customer-facing/CPE devices to drop all prefixes except those the customer is authorized to announce.
  - We use standardized templates for Junos and IOS-XR, to reduce the chance of errors by the implementing engineer.
- **Verifying ASNs and IP blocks:**
  - We check WHOIS data to verify that a customer is authorized to use the resources they intend to announce.

470_Junos_MX204_CPE_Inet-Conn_eBGP.txt 9.4 KB

```
policy-options {
    prefix-list {{ internet_connection.site_code }}-v4 {
        /* list all ipv4 prefixes to be accepted here */
        {{ prefix }};
    }
    prefix-list {{ internet_connection.site_code }}-v6 {
        /* list all ipv6 prefixes to be accepted here */
        {{ prefix }};
    }
    policy-statement {{ internet_connection.site_code }}-bgp-import-ddos {
```

-zsh ⌥⌘1

```
# whois.arin.net

ASNumber:       31
ASName:         CIT
ASHandle:       AS31
RegDate:        1984-09-21
Updated:        2003-08-07
Ref:            https://rdap.arin.net/registry/autnum/31


OrgName:        California Institute of Technology
OrgId:          CIT-4
Address:        1200 East California Boulevard
Address:        MS 1-10
City:           Pasadena
StateProv:      CA
PostalCode:     91125
Country:        US
RegDate:
Updated:        2022-05-02
Ref:            https://rdap.arin.net/registry/entity/CIT-4


OrgTechHandle: CI2-ORG-ARIN
OrgTechName:   Caltech Network Operations Center
OrgTechPhone:  +1-626-395-3500
OrgTechEmail:  noc@caltech.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/CI2-ORG-ARIN
```

How do we verify Action 1?

- **CIDR Report**
  - Gives an overview of the prefixes and ASNs we are announcing, and highlights bogons
  - IPv4: https://www.cidr-report.org/as2.0/
  - IPv6: https://www.cidr-report.org/v6/as2.0/

- **MANRS Observatory**
  - The MANRS observatory measures route leaks, misoriginations, hijacks, and bogons by us and our customers.

Bogus ASes Announced by this AS

Bogus AS		Announcing-AS	
AS22063	Announced by	AS2152	CSUNET-NW, US

MANRS Dashboard

OVERVIEW HISTORY DETAILS COMPARISON ABOUT

M1 - Route leak by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M1C - Route leak by a direct customer

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 (BGPStream) - Route misorigin by the AS

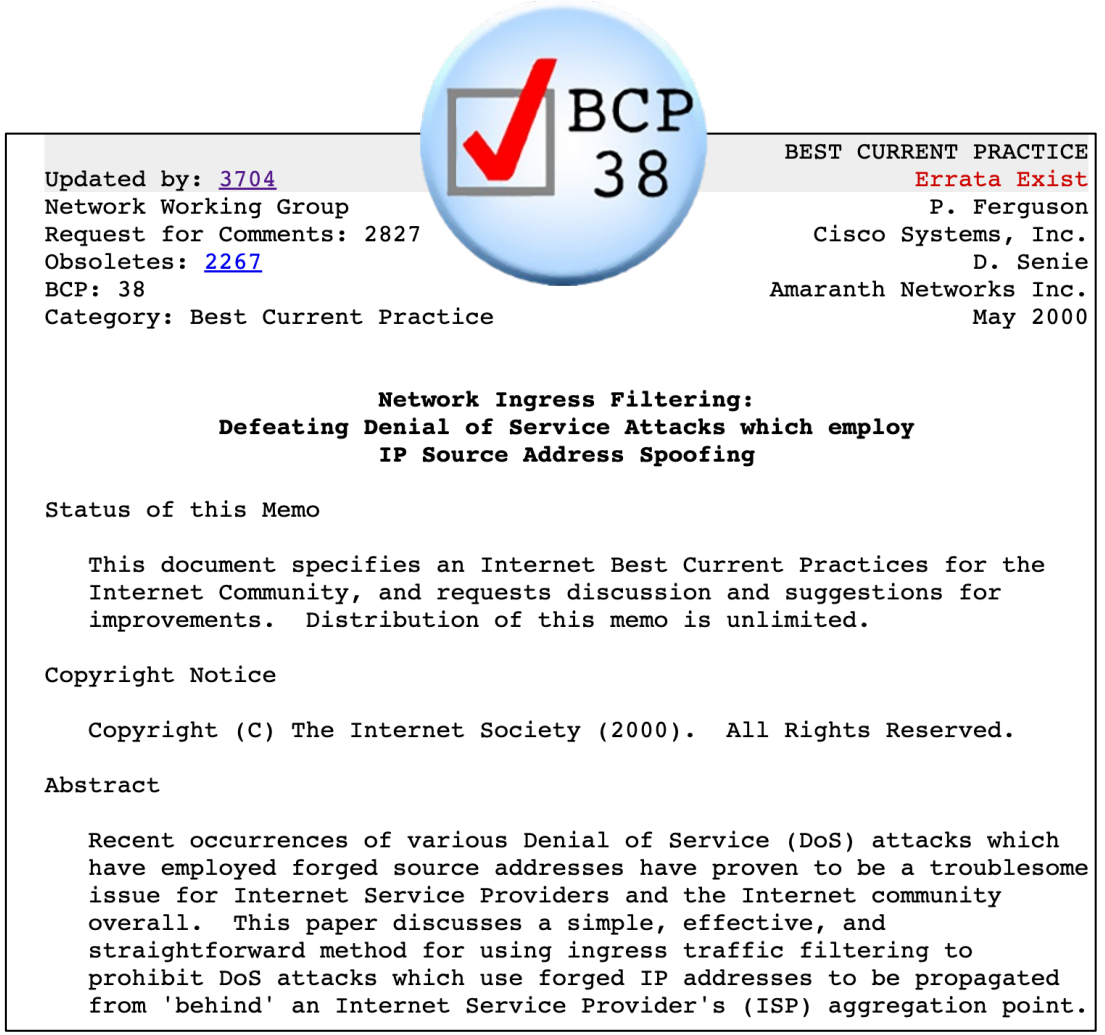
Absolute: **0.0** Normalized: **100%** Incident Count: **0**

M2 (GRIP) - Route misorigin by the AS

Absolute: **0.0** Normalized: **100%** Incident Count: **0**

Action 2: Prevent traffic with spoofed source IP addresses

- **Unicast Reverse Path Forwarding (uRPF)**
  - We implement uRPF loose mode in our standard router configurations.
  - Loose mode is not adequate to stop most spoofing—only certain bogon addresses
- **Source address filtering with ACLs**
  - We also add ACLs on our customer interfaces whenever feasible – these are typically added in conjunction with the prefix filters mentioned previously



BCP 38

BEST CURRENT PRACTICE
Errata Exist

Updated by: 3704
Network Working Group — P. Ferguson
Request for Comments: 2827 — Cisco Systems, Inc.
Obsoletes: 2267 — D. Senie
BCP: 38 — Amaranth Networks Inc.
Category: Best Current Practice — May 2000

Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

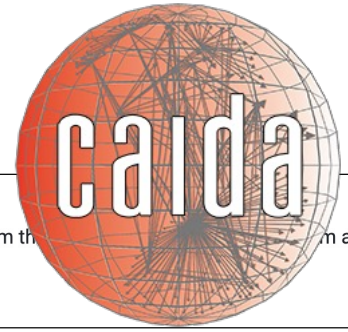
Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

How do we verify Action 2?

- **CAIDA Spoofer**
  - Spoofer client software runs from our own network and attempts to send traffic with spoofed source addresses
  - Results are sent to CAIDA and are publicly visible
  - Not a comprehensive spoofing detection system—requires active participation by networks.
  - **MANRS Action 2 requires CAIDA spoofer to be run from at least two network segments.**

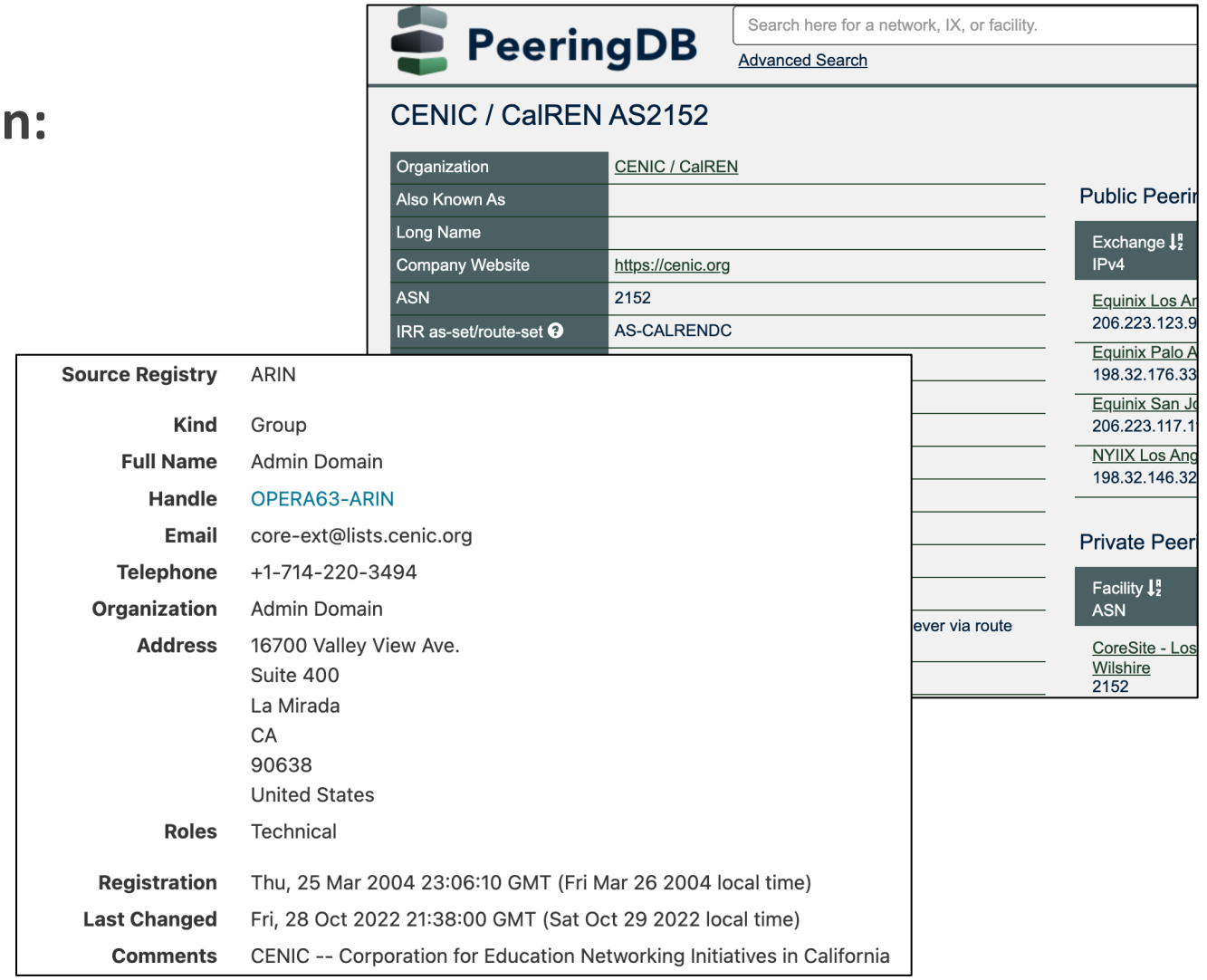


Spoof status key			
received	Spoofed packet was received.	✔	Pattern of tests from th…m allowing spo… to blocking it.
rewritten	Spoofed packet was received, but the source address was changed en route.		
blocked	Spoofed packet was not received, but unspoofed packet was.		
unknown	Neither spoofed nor unspoofed packet was received.		

Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj Spoof Prefix Len	Results
1542254	2023-03-13 13:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1538469	2023-03-06 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1534643	2023-02-27 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1530907	2023-02-20 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1526911	2023-02-13 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1522764	2023-02-06 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1518660	2023-01-30 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1512075	2023-01-16 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1507891	2023-01-09 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1503839	2023-01-02 14:00:01	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1500375	2022-12-26 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1496672	2022-12-19 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1492993	2022-12-12 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1486782	2022-11-28 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1482471	2022-11-21 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1479830	2022-11-16 22:17:14	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ blocked	/24	Report
1478360	2022-11-14 14:00:02	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ received	/8	Report
1475576	2022-11-09 21:47:11	207.62.80.x/24	2152 (CSUNET-NW)	usa (United States)	no	blocked	✔ received	/8	Report

Action 3: Facilitate global operational communication and coordination

- **We maintain updated contact info in:**
  - PeeringDB
  - ARIN (whois)
  - RADb



PeeringDB

Search here for a network, IX, or facility.

Advanced Search

CENIC / CalREN AS2152

Organization	CENIC / CalREN
Also Known As	
Long Name	
Company Website	https://cenic.org
ASN	2152
IRR as-set/route-set	AS-CALRENDC

Public Peerin

Exchange
IPv4

Equinix Los An
206.223.123.9

Equinix Palo A
198.32.176.33

Equinix San Jo
206.223.117.1

NYIIX Los Ang
198.32.146.32

Private Peer

Facility
ASN

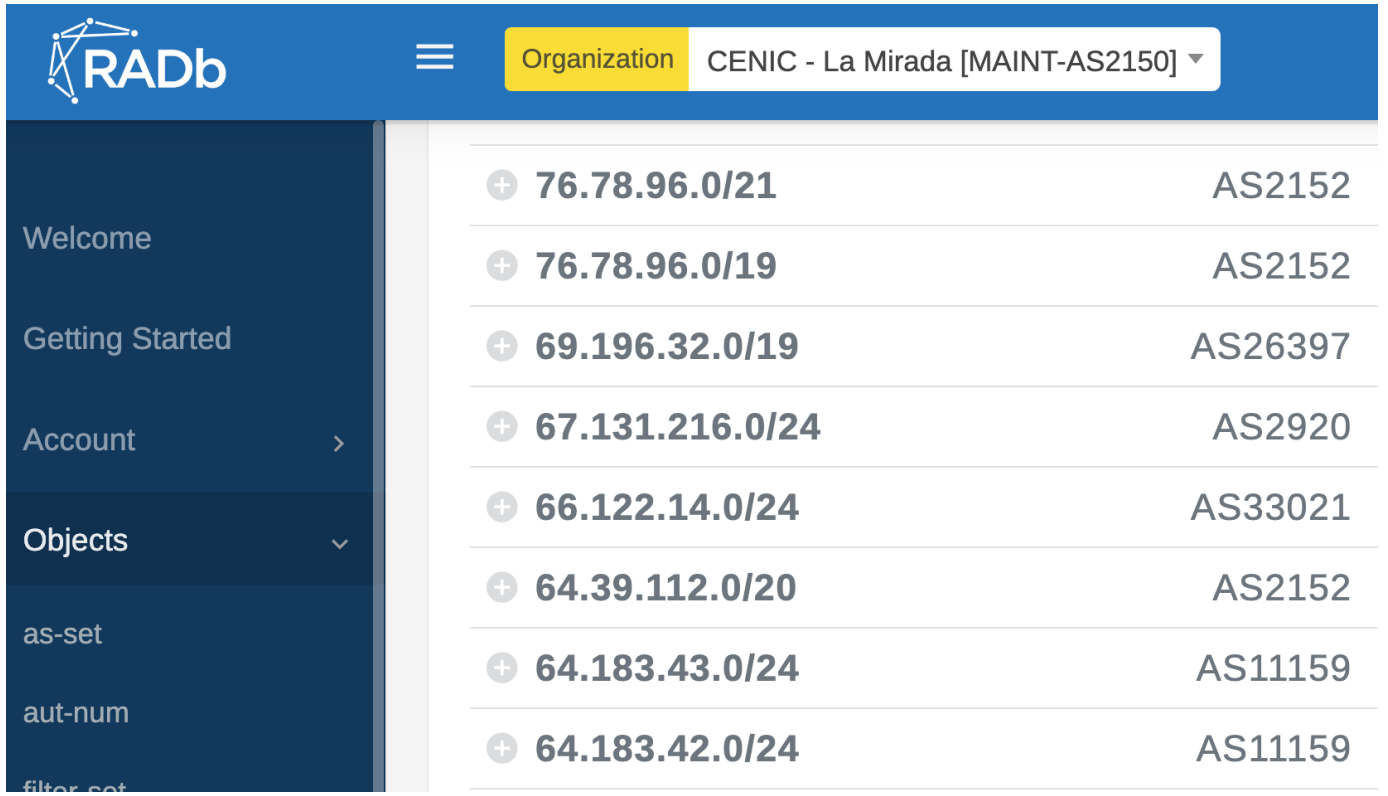
CoreSite - Los
Wilshire
2152

ever via route

Source Registry	ARIN
Kind	Group
Full Name	Admin Domain
Handle	OPERA63-ARIN
Email	core-ext@lists.cenic.org
Telephone	+1-714-220-3494
Organization	Admin Domain
Address	16700 Valley View Ave. Suite 400 La Mirada CA 90638 United States
Roles	Technical
Registration	Thu, 25 Mar 2004 23:06:10 GMT (Fri Mar 26 2004 local time)
Last Changed	Fri, 28 Oct 2022 21:38:00 GMT (Sat Oct 29 2022 local time)
Comments	CENIC -- Corporation for Education Networking Initiatives in California

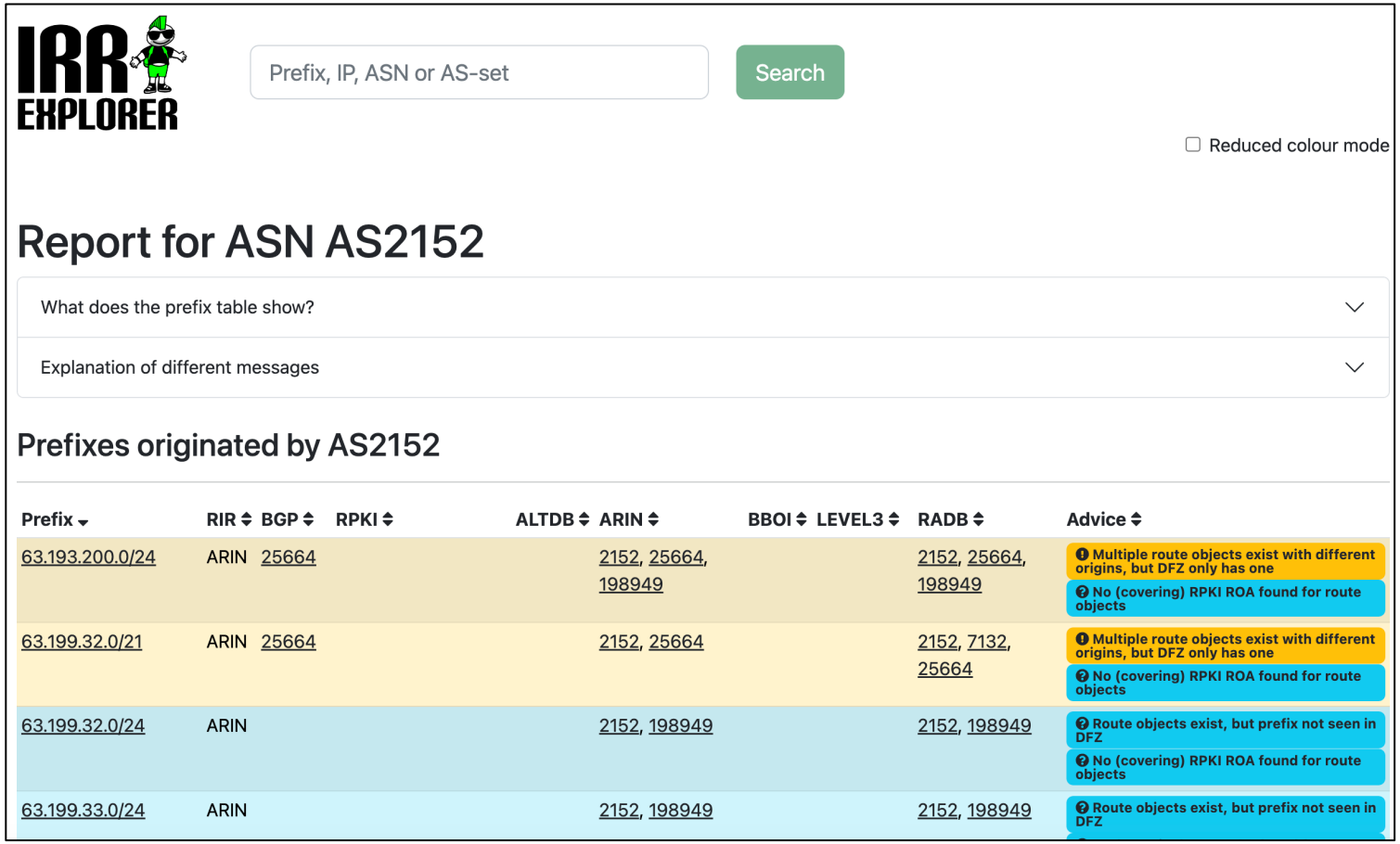
Action 4: Facilitate routing information on a global scale

- **We maintain updated IRR objects in RADb:**
  - route
  - route6
  - aut-num
  - as-set
- We proxy-register objects on behalf of customers that are unable/unwilling to do so
- We are still working on implementing RPKI and signing ROAs



How do we verify Action 4?

- **We frequently check our ASNs in NLNOG's IRR Explorer tool**
- https://irrexplorer.nlnog.net/
- Lists and compares the ASNs associated with each prefix in BGP, RPKI, and multiple IRRs.
- MANRS Observatory also detects obvious issues, but not as detailed and comprehensive.



We have lots of room for improvement…

- **Action 1 (prefix filtering):**
  - We do not yet generate filters from IRR data (e.g. with bgpq3)
  - We do not have a defined procedure to audit and update our filters after their initial creation
- **Action 2 (anti-spoofing):**
  - We should install the CAIDA spoofer client on many more network segments/source address ranges
  - We do not have a defined procedure to audit and update our ACLs after their creation
- **Action 3 (coordination):**
  - Our *de facto* ASNs 2152 and 2153 are still officially assigned to the CSU Chancellor's Office—we do not have full control over them in ARIN
- **Action 4 (global validation):**
  - We need to better define our internal procedures for updating RADB—our engineers sometimes forget to make these updates
  - We need to sign ROAs for our prefixes: this is in active planning

Thank You

Christopher Bruton (he/him)
Core Engineer at CENIC (AS 2152)
cbruton@cenic.org
https://www.linkedin.com/in/christopherbruton