Pacific Wave SDN/SDX

John Hess
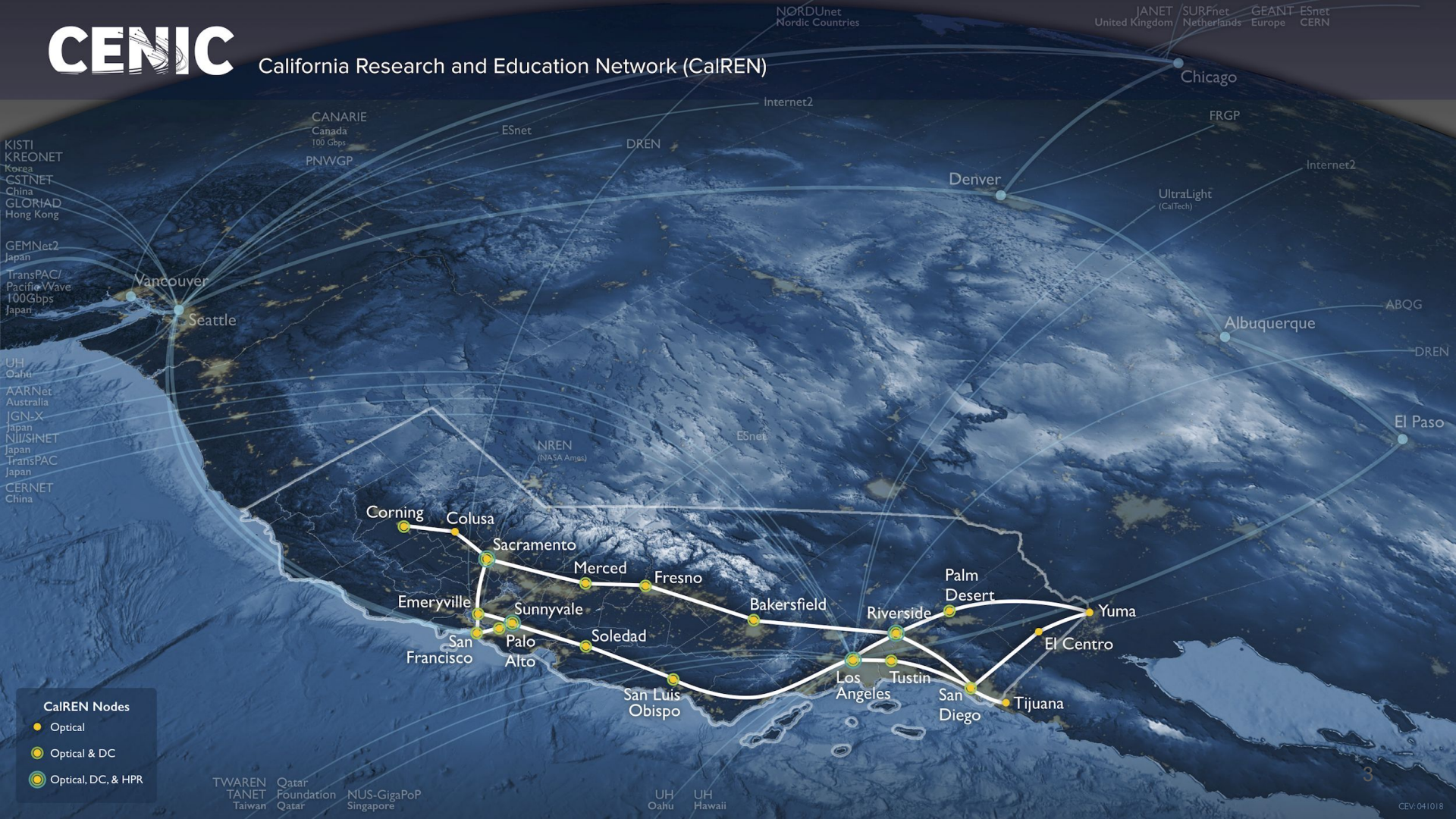*Network Engineer - Research Engagement*
CENIC - Pacific Wave

Agenda

- CENIC and Pacific Wave
- SDX Technologies and Services
- Routing Ecosystem
- Security for Routing and Infrastructure Services

Our community comprises universities, colleges, public schools and libraries, scientific organizations, cultural and performing arts institutions, university medical centers and their partners, and California cities.
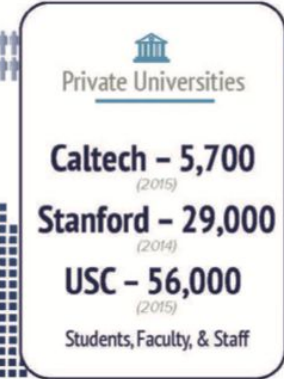
CENIC Associates like the Naval Postgraduate School, NASA Ames, Monterey Bay Aquarium Research Institute, University of San Diego, Community Hospital of the Monterey Peninsula, SFJAZZ, The Exploratorium, and many others, serve tens of thousands of Californians.

More than 11,000 institutions in all, and growing.

UC Campuses
436,700
Students, Faculty & Staff
(2014)

CA State Universities
467,000
Students, Faculty & Staff
(2015)

CA Community Colleges
2,189,000
Students, Faculty & Staff
(2015)

CENIC Community by the Numbers

Serving 20,000,000 Californians

CA K-12
6,727,000
Students, Teachers & Staff
(2015)

CA Libraries
129 Jurisdictions
160,000,000 visits
(2016)

Private Universities
Caltech – 5,700
(2015)
Stanford – 29,000
(2014)
USC – 56,000
(2015)
Students, Faculty, & Staff

Pacific Wave - International Peering Exchange

- A project CENIC and Pacific Northwest Gigapop (PNWGP), Pacific Wave was deployed as a geographically distributed peering facility in January 2004
- Open Exchange Points supporting both commercial and R&E peers
- Pacific Wave has been partially supported through three separate five-year National Science Foundation (NSF) grants supporting growth connectivity and innovation
- Currently serves 31 countries across the Pacific connecting to the Western USA
- Enables science-driven high-capacity data-centric projects, such as the Pacific Research Platform (PRP), enabling researchers to move data between collaborator sites, supercomputer centers, and campus Science DMZs without performance degradation
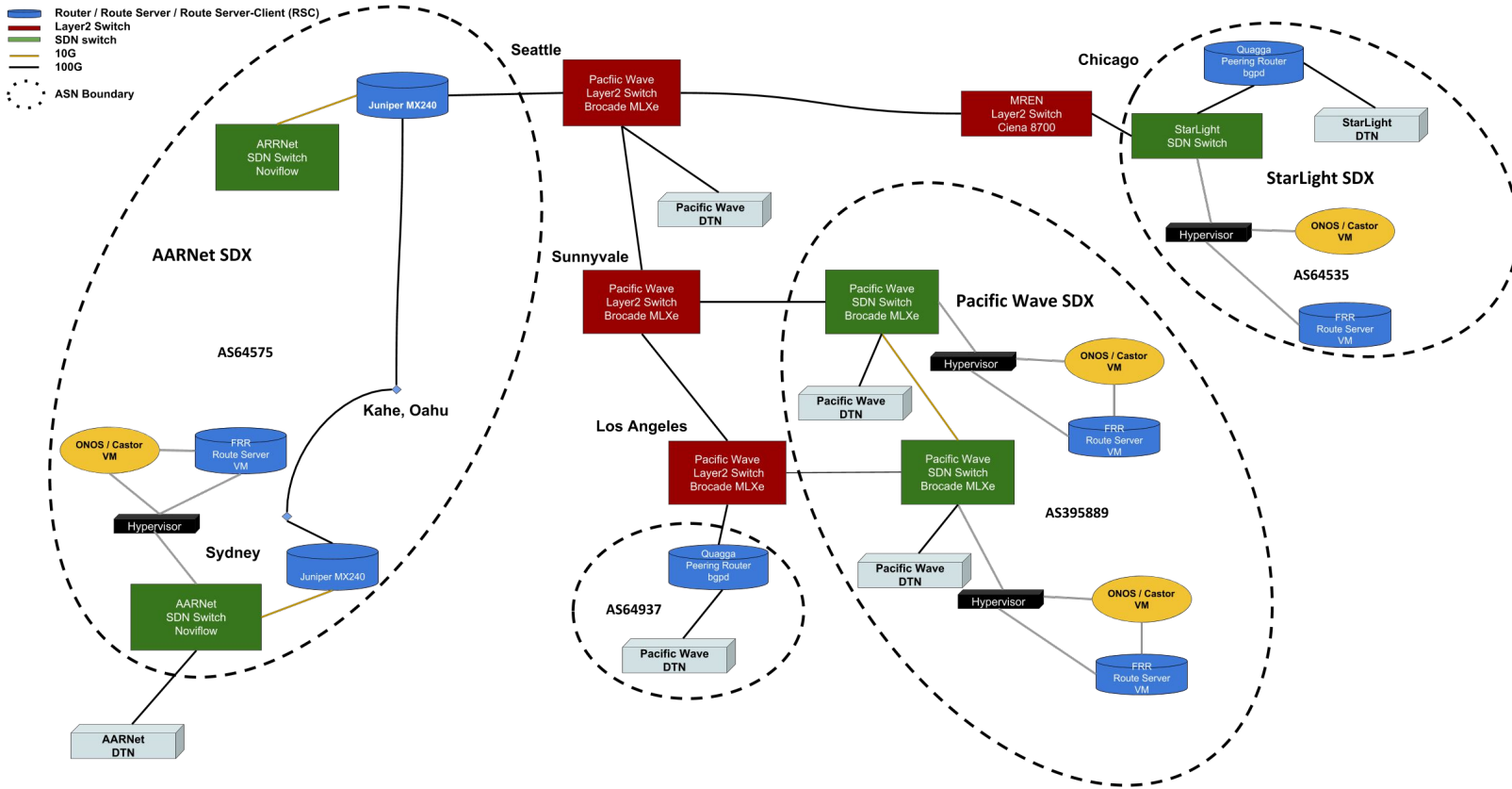
Agenda

- CENIC and Pacific Wave
- SDX Technologies and Services
- Routing Ecosystem
- Security for Routing and Infrastructure Services

AARNet - Pacific Wave - StarLight Inter-domain SDX Topology high-level v0.06.03A

Legend:
- Router / Route Server / Route Server-Client (RSC)
- Layer2 Switch
- SDN switch
- 10G
- 100G
- ASN Boundary

Seattle
Pacfiic Wave Layer2 Switch Brocade MLXe
Juniper MX240
ARRNet SDN Switch Noviflow
Pacific Wave DTN

Chicago
Quagga Peering Router bgpd
StarLight SDN Switch
StarLight DTN
MREN Layer2 Switch Ciena 8700
StarLight SDX
AS64535
Hypervisor
ONOS / Castor VM
FRR Route Server VM

AARNet SDX
AS64575
ONOS / Castor VM
FRR Route Server VM
Hypervisor
Kahe, Oahu
Sydney
Juniper MX240
AARNet SDN Switch Noviflow
AARNet DTN

Sunnyvale
Pacific Wave Layer2 Switch Brocade MLXe

Pacific Wave SDX
Pacific Wave SDN Switch Brocade MLXe
Hypervisor
ONOS / Castor VM
FRR Route Server VM
Pacific Wave DTN
AS395889

Los Angeles
Pacific Wave Layer2 Switch Brocade MLXe
Pacific Wave SDN Switch Brocade MLXe
Pacific Wave DTN
Hypervisor
ONOS / Castor VM
FRR Route Server VM
Quagga Peering Router bgpd
AS64937
Pacific Wave DTN

NOTE: this diagram represents a subset of sites, devices, and connections

V0.06.02A 20180306

GRP

Global Research Platform   September 18, 2019

CENIC   8
PACIFIC WAVE

PRPv2 BGP Pilot: route servers for control plane

http://pacificresearchplatform.org

Legend:
- PRPv2 BGP Peering Pilot Site
- PRP / AS395889 control plane
- Data Plane
- Pacific Wave
- CENIC CalREN HPR
- 1x100G

Chicago

MREN 8700

Starlight/ MREN

Seattle

Tokyo

icas-sttlwa01-03

NCSA

Oahu

rs01.sttlwa
Quagga / Juniper vMX
Route Server

Data Plane

PRP / AS395889

Sunnyvale

snvl2-pw-sw-1

rs01.snvaca
Quagga / Juniper vMX
Route Server

Control Plane

Los Angeles

losa2-pw-sw-1

El Paso

Hawaii

lax-hpr3

rs01.lsanca
Quagga / Juniper vMX
Route Server

SDSC

NOTE: this diagram represents a subset of sites, devices, and connections

V0.1.8
20170510

GRP

Global Research Platform   September 18, 2019

CENIC   9 PACIFIC WAVE
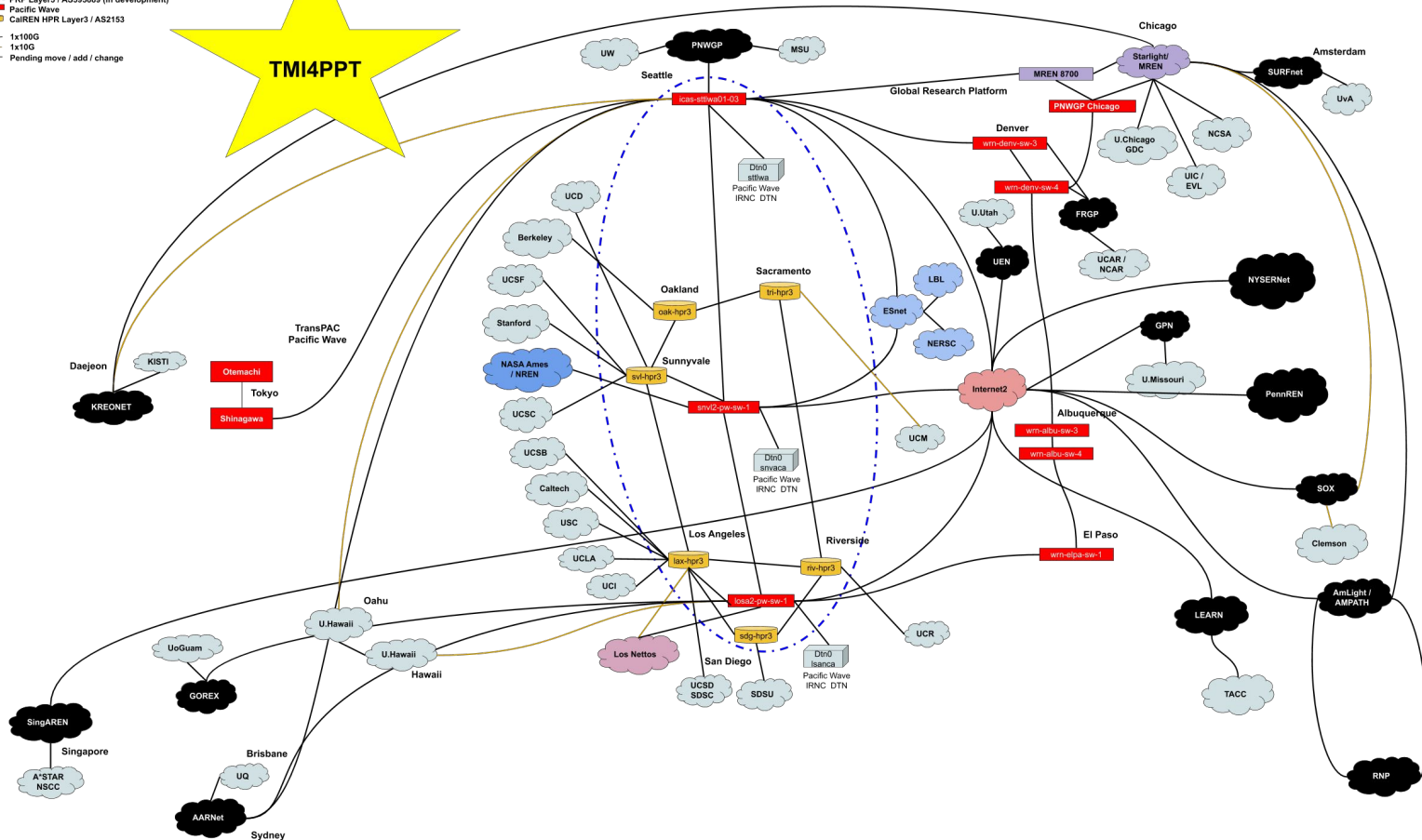
SDX Technologies and Services - Forward Looking

- Capacity

    - Core moving from N x 100Gbps to 200Gbps and toward 400Gbps

- Segment Routing: SR-MPLS vs SRv6

    - Who remembers source-based routing? Some workflows desire or require an explicit path.

    - SR may be implemented as a control-plane architecture to provide traffic engineering (TE) at the ingress router. TE policy to steer a packet through a specific set of nodes and links in the network.

    - SR-MPLS uses a label stack to describe the desired path through the network. Examine the label; do a lookup; pop the label; forward the packet. SR-MPLS requires some specific control-plane software, but does not impact ASICs ability to forward packets.

    - SRv6 uses a Segment Routing Header (SRH) embedded as a new header within an IPv6 packet to describe the desired path through the network. SRv6-capable routers will want (or need) new ASICs and/or programmable silicon (e.g. Juniper Penta). non-SRv6 capable routers ignore the SRH and forward the packet normally.

GRP

CENIC
PACIFIC WAVE
10

Pacific Research Platform
http://pacificresearchplatform.org

Global Research Platform   September 18, 2019

SDX Technologies and Services

- Orchestration

  - Dynamic circuit and services provisioning

    - AutoGOLE / NSI + MEICAN (RNP!); and, SENSE & Big Data Express

  - NFV, vCPE, IaaS

  - Containers: Docker, Singularity, OCI. Federated across cloud-providers, within-network, at member institutions

- Federated access to Infrastructure-attached resources

  - Inter-domain and inter-cluster: access to storage, CPU / GPU / TPU, FPGA

  - ICN / NDN -- hierarchical, caching of research data, e.g. LHC/HEP, genomics, weather. SANDIE: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1659403

Agenda

- CENIC and Pacific Wave
- SDX Technologies and Services
- Routing Ecosystem
- Security for Routing and Infrastructure Services

Routing Ecosystem

- IANA/ICANN
- Internet Routing Registries (IRRs) / Regional Internet Registries (RIRs)
  - http://www.irr.net/docs/list.html
  - American Registry for Internet Numbers (ARIN)
  - Merit's Routing Arbiter Database (RADb)
- Network Operators
- Internet Exchange Points (IXPs)
- Border Gateway Protocol
- Infrastructure Services and Tools

Agenda

- CENIC and Pacific Wave
- SDX Technologies and Services
- Routing Ecosystem
- Security for Routing and Infrastructure Services

15

Routing Security and Trust models

Mutually Agreed Norms for Routing Security (MANRS)

- https://www.manrs.org
- A global initiative, supported by the Internet Society, toward reducing the most common threats to the routing ecosystem
- MANRS actions for Network Operators / Internet Service Providers (ISPs)
  - Filtering -- Prevent propagation of incorrect routing information
  - IP source validation -- Prevent traffic with spoofed source IP addresses
  - Coordination -- Facilitate global operational communication and coordination between network operators
  - Global validation -- Facilitate validation of routing information on a global scale

Routing Security and Trust models

Mutually Agreed Norms for Routing Security (MANRS)

- MANRS actions for Internet eXchange Points (IXPs)
  - Prevent propagation of incorrect routing information
  - Promote MANRS to the IXP membership
  - Protect the peering platform
  - Facilitate global operational communication and coordination between network operators
  - Provide monitoring and debugging tools to the members

Routing Security and Trust models -- Implementation

Resource Public Key Infrastructure (RPKI)

- Resource certificates digitally verify that a resource has been assigned to a specific entity
- Route Origin Authorization (ROA) - a cryptographically-signed record that associate a BGP route announcement with the correct originating AS number
- Defined in RFC 6480 (An Infrastructure to Support Secure Internet Routing)
- Currently five RIRs (AFRINIC, APNIC, ARIN, LACNIC & RIPE) provide a method for members to take an IP/ASN pair and sign a ROA
- These five RIRs act as Trust Anchors (TAs) -- similar to Certificate Authorities (CAs) -- to validate ROAs

Routing Security and Trust models -- Implementation

RPKI high-level implementation elements

- Origin validation uses X.509 certificates with extensions specified in [RFC 3779](#)
- RPKI Cache server (RPKI Validator) synchronizes its local database with TAs
- RPKI Validator exports a simplified version of ROAs as Route Validation (RV) records
- An RV record is a (prefix, maximum length, origin AS) triple
- Router interacts with cache server to query the RV status for a given route
- Router implements Border Gateway Protocol (BGP) policy based on validation status indicated in the RV record for the route
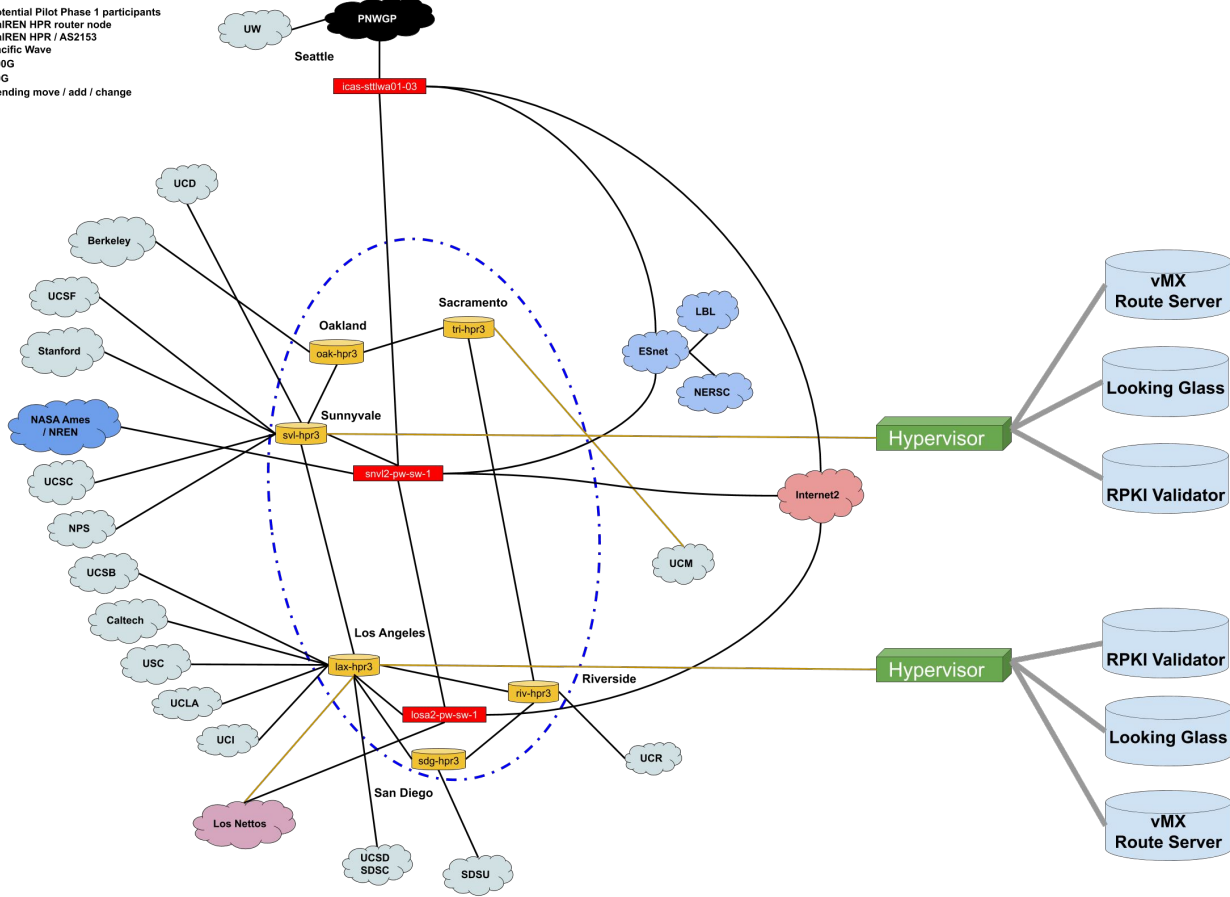
CENIC MANRS - RPKI regional pilot

- Pilot will focus on facilitating MANRS adoption and validation of routing information by implementing RPKI on a regional scale among CENIC and Pacific Wave research universities.

- The pilot is a collaborative effort involving contributors from CENIC, NSRC, ESnet, ARIN, as well as from the CENIC research university community.

- Phase One will focus on participation from California-based research institutions. We will also seek participation from Pacific Wave collaborators outside of California, including the University of Washington and its regional network, the PNWGP (Pacific NorthWest GigaPop).

- Results will be part of a public discussion at the 2020 CENIC Annual Conference

CENIC MANRS RPKI pilot - Phase 1 - v0.06

- RPKI Validator instances synchronize their local ROA database with the (RIRs) trust anchors

- Route Servers interact with RPKI Validators, using ROA validation status as a hook for determining BGP policy. Route Servers facilitate BGP policy for routing platforms which do not support for RPKI, and provide routing telemetry and other data to the Looking Glass instances

- Looking Glass instances provide monitoring and debugging tools to network operators and participants

NOTE: this diagram represents a subset of sites, devices, and connections

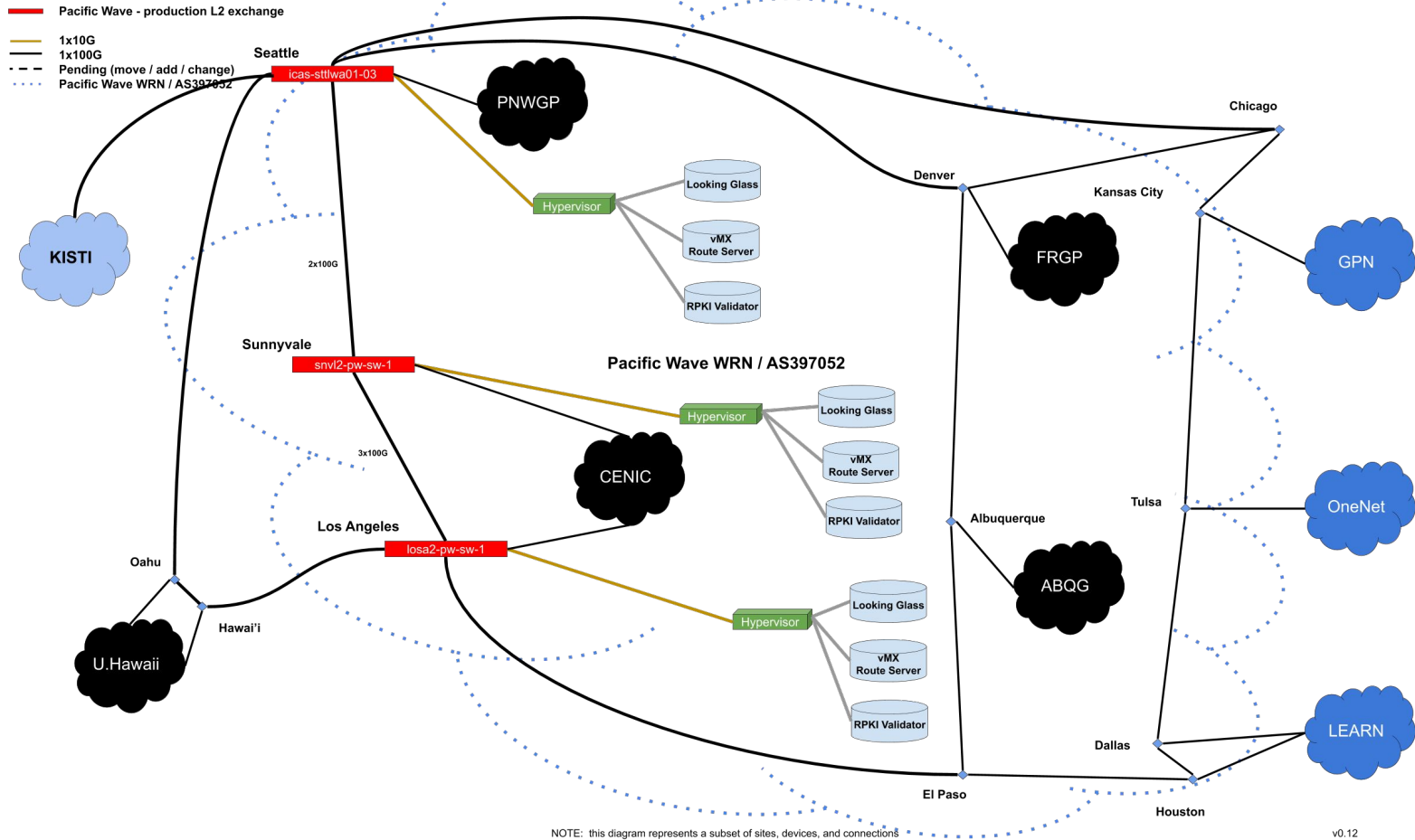Global Research Platform   September 18, 2019

CENIC MANRS - RPKI regional pilot

- Phase Two will seek to expand participation to include Western Regional Network members (University of Hawaii, Front Range Gigapop, New Mexico Gigapop), their respective research universities, as well as other key partners (Oregon Fiber Partnership, LEARN, OneNet, Great Plains Network, Nevada, and others) and their respective research universities. Phase Two will commence, based on the outcomes of Phase One, in the spring of 2020.

- Stretch Goals: Though this project will focus on implementing RPKI for route origin validation, we intend to investigate implementing complementary technologies for enhancing the security of core cyberinfrastructure functions. Examples include: filtering route announcements based on Internet Routing Registry (IRR) data; and, supporting Domain Name System Security Extension (DNSSEC).

CENIC   PACIFIC WAVE

Pacific Wave - Western Region Network: GXP Route-Servers with RPKI pilot - Phase 2 - v0.12

Legend:
- Pacific Wave - production L2 exchange
- 1x10G
- 1x100G
- Pending (move / add / change)
- Pacific Wave WRN / AS397052

Seattle — icas-sttlwa01-03

KISTI

PNWGP

Hypervisor
- Looking Glass
- vMX Route Server
- RPKI Validator

Chicago

Denver

Kansas City

FRGP

GPN

2x100G

Sunnyvale — snvl2-pw-sw-1

Pacific Wave WRN / AS397052

Hypervisor
- Looking Glass
- vMX Route Server
- RPKI Validator

CENIC

Tulsa

OneNet

3x100G

Albuquerque

ABQG

Los Angeles — losa2-pw-sw-1

Oahu

Hawai'i

U.Hawaii

Hypervisor
- Looking Glass
- vMX Route Server
- RPKI Validator

Dallas

LEARN

El Paso

Houston

NOTE: this diagram represents a subset of sites, devices, and connections

v0.12
20190918

GRP

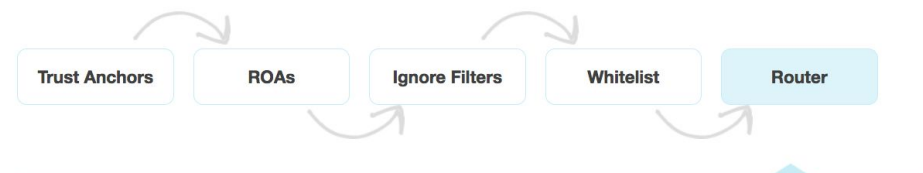CENIC   PACIFIC WAVE   23

Securing Infrastructure Services, and Tools

Considerations for Network Operators and IXPs (not an exhaustive list)

- DNS (Domain Name System):
  - DNSSEC (DNS Security)
    https://www.internetsociety.org/deploy360/dnssec/basics/
- BGP: Implement RPKI, then add BGPsec?
  - https://www.internetsociety.org/blog/2017/10/bgpsec-reality-now/
  - BGPsec is implemented via an optional non-transitive BGP path attribute called BGPsec_Path, that carries digital signatures produced by each autonomous system propagating the update message.
- BGP monitoring tools:
  - Artemis: https://www.inspire.edu.gr/artemis/
  - Looking Glass

CENIC MANRS - RPKI regional pilot

RPKI Validator | Home | Trust Anchors | ROAs | Ignore Filters | Whitelist | BGP Preview | Export and API | Router Sessions | ⚙

Quick Overview of BGP Origin Validation

Trust Anchors → ROAs → Ignore Filters → Whitelist → Router

RPKI/Router

You can configure your router to connect to this validator so that it can receive a full set of **Route Origin Attestations** (ROAs) based on all the ROAs that were validated, minus your ignore list entries, plus your own whitelist entries.

The RPKI to Router Protocol is standardised in RFC 6810 and several vendors have implemented support for this in their router Operating Systems.

Announcement Validation in the Router

Once your router receives the ROAs, it can use this information to determine the validity outcome of the origin AS in BGP announcements. To do this, your router will match an announcement to each attestation in this way:

Announcement has	an origin AS matching the attestation	an origin AS that differs from the attestation
a prefix matching the attestation	VALID	INVALID
a prefix that is more specific than the attestation	INVALID	INVALID

In all other cases, no conclusive decision can be made and the resulting status is 'UNKNOWN'

The final judgement on whether an announcement should be considered valid, invalid or unknown depends on **all** relevant attestations using the following reasoning:

At least one VALID	VALID
No VALIDS, at least one INVALID	INVALID
None of the above	UNKNOWN

```
root@lax-vmx0> show validation session
Session                        State   Flaps    Uptime #IPv4/IPv6 records
2607:f380:2:8030::20                   Up        0   17:21:23 56591/9933

root@lax-vmx0> show validation statistics
Total RV records: 66524
Total Replication RV records: 66524
  Prefix entries: 62340
  Origin-AS entries: 66524
Memory utilization: 12801844 bytes
....
root@lax-vmx0> show validation database
RV database for instance master

Prefix              Origin-AS Session              State   Mismatch
1.0.0.0/24-24        13335 2607:f380:2:8030::20     valid
1.1.1.0/24-24        13335 2607:f380:2:8030::20     valid
1.9.0.0/16-24        4788 2607:f380:2:8030::20      valid
1.9.12.0/24-24       65037 2607:f380:2:8030::20     valid
1.9.21.0/24-24       24514 2607:f380:2:8030::20     valid
1.9.23.0/24-24       65120 2607:f380:2:8030::20     valid
1.9.31.0/24-24       65077 2607:f380:2:8030::20     valid
1.9.65.0/24-24       24514 2607:f380:2:8030::20     valid
....
```

Routing Security and Trust models -- Participating

- ARIN's Operational Test and Evaluation Environment (OT&E):

  https://www.arin.net/resources/ote.html

  - Allows experimentation and research within ARIN's main services, including RPKI, without affecting production data
  - Available to organizations which have signed a Registration Services Agreement (RSA) as well as those organizations which have not signed a RSA
  - Example: test Route Authorization Requests (ROAs) can be created and validated without impacting production RPKI data
- RPKI cache server (Validator) application:
  - RIPE:https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
  - NLnet Labs Routinator: https://www.nlnetlabs.nl/projects/rpki/routinator/

GRP

CENIC   PACIFIC WAVE

Routing Security and trust models -- Participating

- Configuring Origin Validation for BGP:
  - Cisco:
    https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-xe-3s-book/irg-origin-as.pdf
  - Juniper:
    https://www.juniper.net/documentation/en_US/junos12.2/topics/topic-map/bgp-origin-as-validation.html
- Configure and Apply policies (implementation subjective to Network Operator)
  - Assign a local-preference to the RPKI validity attribute of the prefix
  - IETF standards discussions including setting local-preference to prefer valid over unknown, and valid and unknown over invalid
  - Apply extended community tags to signal ROA validity state to iBGP peers

Validated ROAs

Validated ROAs from APNIC RPKI Root, ARIN, AfriNIC RPKI Root, LACNIC RPKI Root, RIPE

Show 10 entries

ASN	Prefix	Maximum Length
0	209.24.0.0/24	24
42	74.80.64.0/18	24
42	204.61.208.0/21	24
42	2001:500:15::/48	48
42	74.63.16.0/20	24
42	2001:500:14::/48	48
42	204.61.216.0/23	23
42	206.220.228.0/22	24
42	2620:0:870::/45	48
87	129.79.0.0/16	16

First Previous 1 2 3 4 5 Next Last

RIPE NCC Copyright ©2009-2018 the Réseaux IP Européens Network Coordinatio

BGP Preview

This page provides a **preview** of the likely RPKI validity states your routers will associate with BGP announcements. This preview is based on:

- The RIPE NCC Route Collector information that was last updated 8 hours and 34 minutes ago.
- BGP announcements that are seen by 5 or more peers.
- The validation rules defined in RFC 6483.
- The validated ROAs found by this RPKI Validator after applying your filters and additional whitelist entries.

Please note that the BGP announcements your routers see may differ from the ones listed here.

Show 10 entries   Search: 15169

ASN	Prefix	Validity
15169	89.207.231.0/24	VALID
15169	104.132.34.0/24	VALID
15169	185.25.28.0/23	VALID
15169	2620:0:1000::/40	VALID
15169	2620:15c::/36	VALID
15169	2a00:79e0::/32	VALID
15169	8.8.4.0/24	UNKNOWN
15169	8.8.8.0/24	UNKNOWN

Global Research Platform   September 18, 2019

CENIC   PACIFIC WAVE   29

MANRS RPKI References

MANRS:

https://www.manrs.org/wp-content/uploads/sites/14/2018/10/Routing-Security-for-Policymakers-EN.pdf

https://www.manrs.org/isps/

https://www.manrs.org/ixps/manrs-actions-for-ixps/

RPKI:

https://blog.cloudflare.com/rpki/

http://www.sanog.org/resources/sanog30/SANOG30-Tutorial_rpsl-rpki-sanog30.pdf

https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources

https://www.arin.net/resources/rpki

https://tools.ietf.org/html/rfc8210

Tools: https://www.inspire.edu.gr/artemis/

GRP

CENIC

30
PACIFIC WAVE

Questions?

Extra Slides

CENIC MANRS RPKI Workshop - abstract

October 10-11, 2019 - CENIC offices La Mirada

Overview

Mutually Agreed Norms for Routing Security (MANRS) is an initiative, supported by the Internet Society, focused on reducing the most common threats to the global routing ecosystem through a variety of localized implementation methods. Resource Public Key Infrastructure (RPKI) is a technology that enables network operators to verify the integrity of routing information. This workshop is part of a CENIC-initiated pilot to facilitate MANRS adoption and implement a RPKI deployment on a regional scale among CENIC and Pacific Wave research universities. The MANRS RPKI pilot is a collaborative effort involving contributors from CENIC, NSRC, ESnet, and ARIN, as well as from the research university community.

In this workshop participants will learn about the global MANRS effort, how RPKI fits within the MANRS framework, the CENIC MANRS RPKI pilot, and the roles and services offered by ARIN as to support RPKI deployments. The workshop will offer hands-on lab exercises to model routing best practices, as well as creating Route Origin Authorization objects (ROAs) within ARIN's Operational Test & Evaluation Environment (OT&E).

Instructors:

Mark Kosters (MK), ARIN; Jon Worley (JW), ARIN; Philip Smith (PS), NSRC; Sana Bellamine (SB), CENIC; John Hess (JH), CENIC

CENIC MANRS RPKI Workshop - program

Thursday, October 10

9:00 - 10:30 Workshop Welcome (JH)

- CENIC MANRS RPKI Pilot overview
- Workshop Objectives & Goals
- Slack channel

10:30 - 10:45 Break

10:45 - 12:15 Session 1: Route Filtering - IRR and RPKI (SB)

- Campus aspects - BCP38 / Ingress Filtering, uRPF
- RPKI and DDoS mitigation services

12:15 - 13:15 Lunch

13:15 - 14:45 Session 2: Introduction to RPKI (MK)

- Lab 1.1 ARIN OT&E Online interface to setup RPKI and provision ROA (JW)

14:45 - 15:00 Break

15:00 - 16:30 Session 3: Install and use RIPE NCC Validator with ARIN OT&E

- Lab 1.2 Install RIPE NCC validator and use ARIN OT&E TAL (MK, JW)
- Lab 1.3 Validated results via RIPE NCC Validator (MK, JW)

16:30 - 17:00 Session 4: Day 1 debrief and review objectives for Day 2

17:00   Adjourn

Friday, October 11

9:00 - 10:30 Lab 2.1 MANRS elements for Network Operators (PS)

- Filtering; Anti-Spoofing; Coordination; and, Global Validation

10:30 - 10:45 Break

10:45 - 12:00 Lab 2.2 Setting up RPKI Validator with NRSC virtual environment (PS)

- Installing RPKI Validator Cache on NSRC virtual environment
- Configuring routers to use validator cache

12:00 - 1:00 Lunch

13:00 - 14:30 Lab 2.3 Exploring RPKI Validator with real global data (PS)

- Exploring validator on NSRC virtual environment, using real global data
- Using public RPKI tools - eg bgp.he.net, seacom looking glass, etc

14:30 - 15:00 Break

15:00 - 16:30 Session 3: Engineering Round-table, next steps for RPKI pilot deployment (ALL)

- Campus-specific use-cases, challenges
- Next steps in coordination toward deployment within pilot

16:30 - 17:00 Session 4: Workshop debrief and closing thoughts (ALL)

17:00   Adjourn