

Internet2 Community Exchange 2024

David Marble – CEO OSHEAN

Luke Fowler – Exec. Director Network & Software Engineering at IU's GlobalNOC

IOHO

In OSHEAN's Humble Opinion

The background is a solid green color with several overlapping, semi-transparent, rounded rectangular shapes in a slightly lighter shade of green. These shapes are arranged in a pattern that suggests movement or a stylized architectural structure, with some shapes pointing towards the right and others towards the left.

OSHEAN View

Our World is Changing Rapidly

- ▶ The last few years have seen.....
 - ▶ 10G to 100G and 400G Transport
 - ▶ Elimination of MPLS
 - ▶ Now Segment Routing and eVPN
 - ▶ Much development in “above the net” services
 - ▶ Topology expansion to include smaller sites with wireless and SDWan
 - ▶ Big Uptick in Managed Security Services (managed Firewall)
 - ▶ Cloud Exchange functionality
 - ▶ Application specific handling of routes
 - ▶ Increased desire for metrics and reports of individual payloads
 - ▶ Developments of ML/AI for config and diagnostic automation

***The result is an increase in opportunity for the R&E community.....
with a corresponding increase in complexity and responsibility***

Who we are



OSHEAN strives to be a valued extension of our Member's digital infrastructure, IT staff and technical knowledge base. While providing an unparalleled fiber and IP virtual private infrastructure, we partner with our members to be the trusted source for expertise and service solutions in network, cybersecurity and cloud practices. Our goal is the continued development of a true member collaborative dedicated to the advancement of each Member's digital transformation journey.

- 501c3 Independent non-profit Rhode Island member organization
 - Higher Ed, K12, Library, Healthcare, Govt and other non-profits
- 700+ miles of fiber, 160 members, 275 Packet optical nodes, 16 DWDM core nodes
- Key services in network, security and cloud access
 - Recent years transition from transport (fiber) and IP to a services-centric model

Practice Development: IP Networking



Network Automation

- Service chains (i.e.DDoS)
- Diagnostic Automation
- Cloud network Layer2 access through AL2S with Insight

Analytics

- Leverage/pull analytics from the new NCS layer (Portal)
- Cloud route (end-to-end) Telemetry
- Visibility per Application
- Cisco FSO (Thousand Eyes) Investigation/PoC

100/400Gbps Transport & Circuit Services

- 100G Member Rings
- 400G Segments
- Segment Routing
- eVPN Site to Site; Site to Service

Expanded Content Networking

- Bulk ISP Resilience
- eGaming
- Expanded Peering points
- SaaS peers

Practice Development: Security



Expansion of Current Services

- DDoS Service to secondary non-OSHEAN circuits
- Drive Cisco Umbrella and Duo program; Secureworks VDR

Fortinet Security Service offering

- Hosted Firewall Svc stack
- Continue the development of the SDWan Service
- NAC service

New Services

- XDR Decision
- SoC Analysis
- Asset Systems

Security Information in the OSHEAN Portal

- Highest Level Crits
- Threat Feeds
- SSO to services

Practice Development: Cloud Access



Cloud Access Network Experts

- Optimized Routing; lowest latency; lowest cost
- Provisioning automation
- Telemetry to I2 Cloud Exchange

Cloud Security

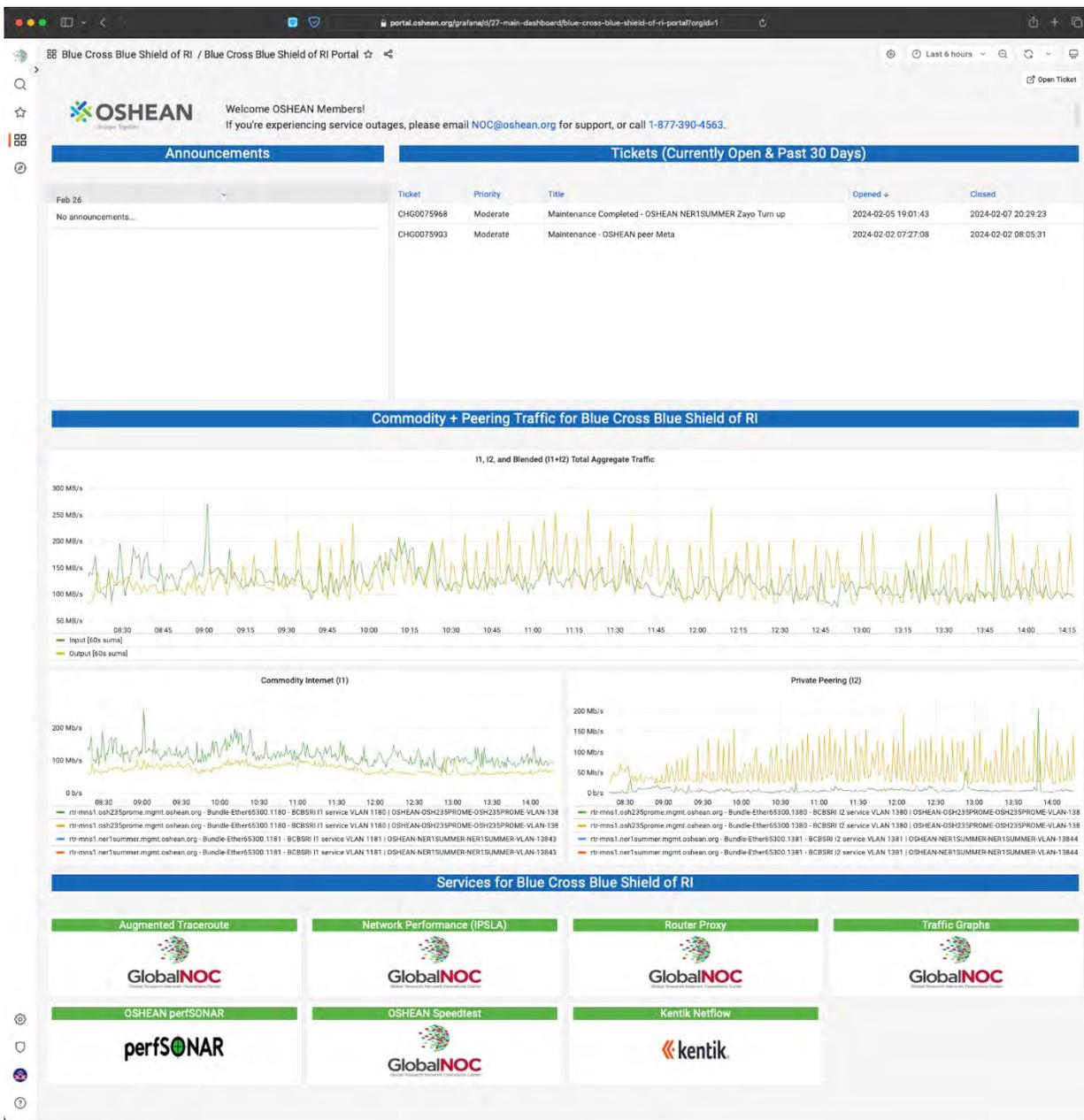
- Payload Encryption (MACSEC)MACsec in production (healthcare)

Cloud Management

- Cloud Services orchestration/mgmt. partnership (i.e Kion)
- CASB
- Expanded Portal Integration

The background is a solid green color with several overlapping, semi-transparent, rounded rectangular shapes in a slightly lighter shade of green. These shapes are arranged in a pattern that suggests movement or a stylized graphic design. The text "OSHEAN Services" is centered in the right half of the image.

OSHEAN Services

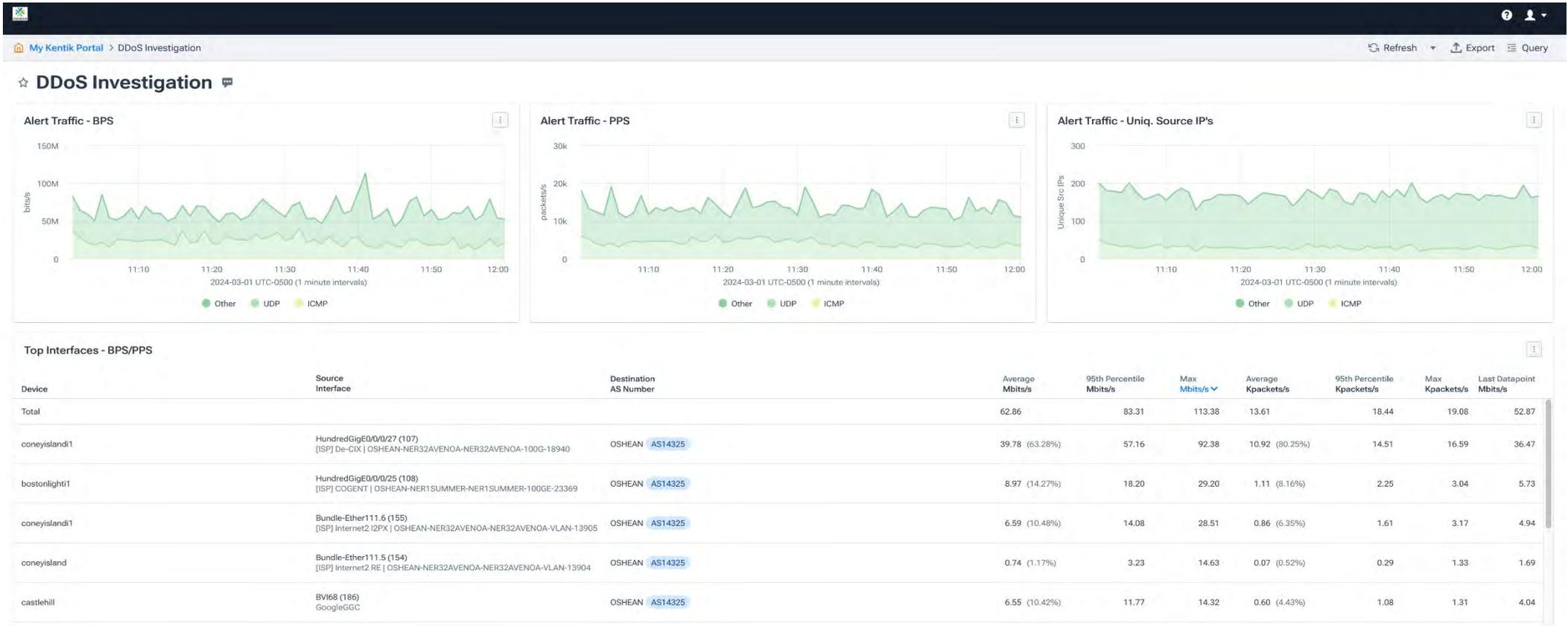


Member-facing Telemetry

OSHEAN portal provides a one-stop-shop for members to view network telemetry with views tailored to their services

Portal aggregates data from ticketing, time-series measurement, monitoring, and other data sources into a single view for members

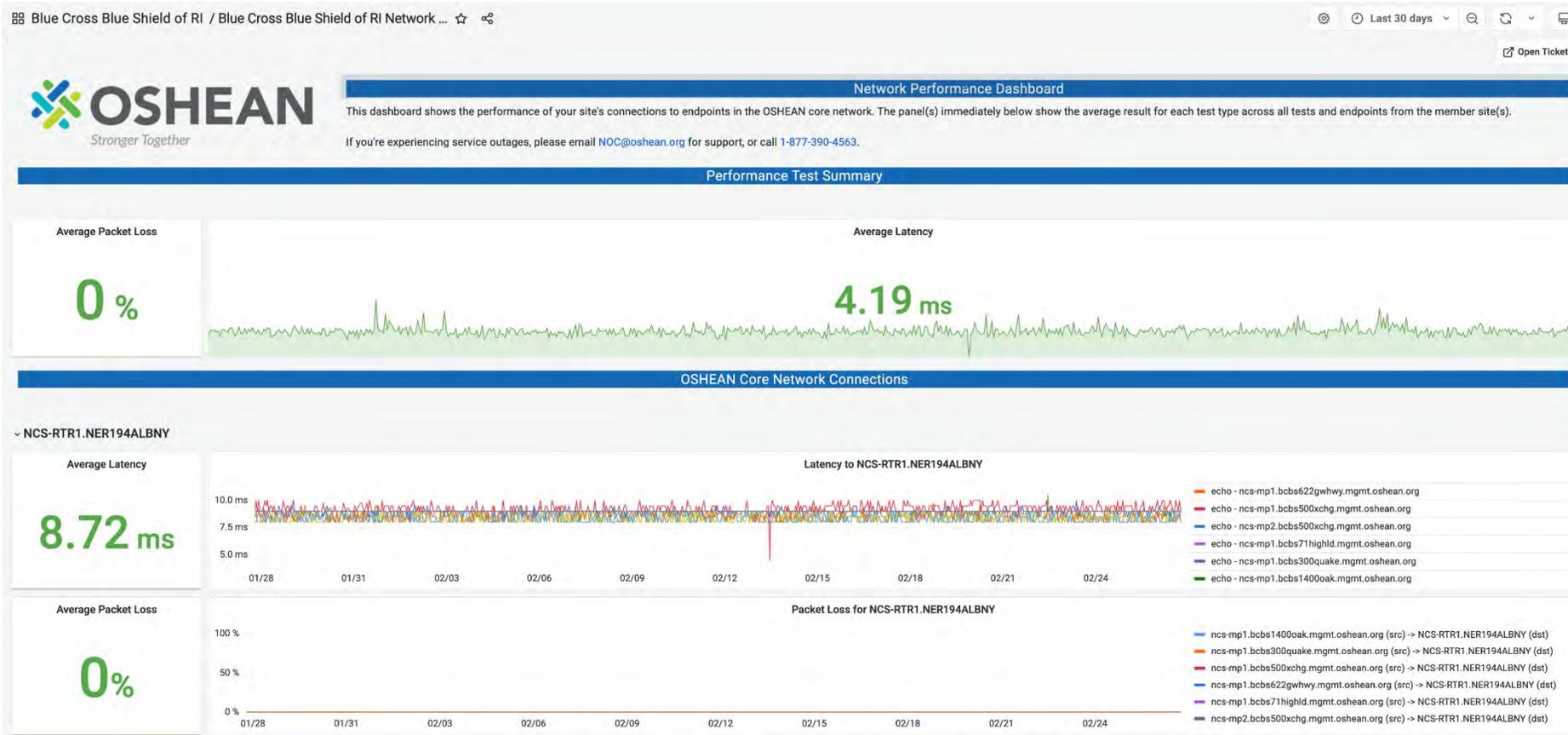
Eliminating the need to hunt through multiple systems to find the data you want – the portal puts it all right in front of you!



Member Security Service - DDoS

OSHEAN telemetry, automation and visibility provides reporting for members to view network telemetry data with views tailored to their individual payloads

In this instance, OSHEAN service chaining provides instant mitigation through telemetry with Kentik and scrubbing with Akamai. The Portal then provides diagnostic visibility to the member for subsequent analysis.

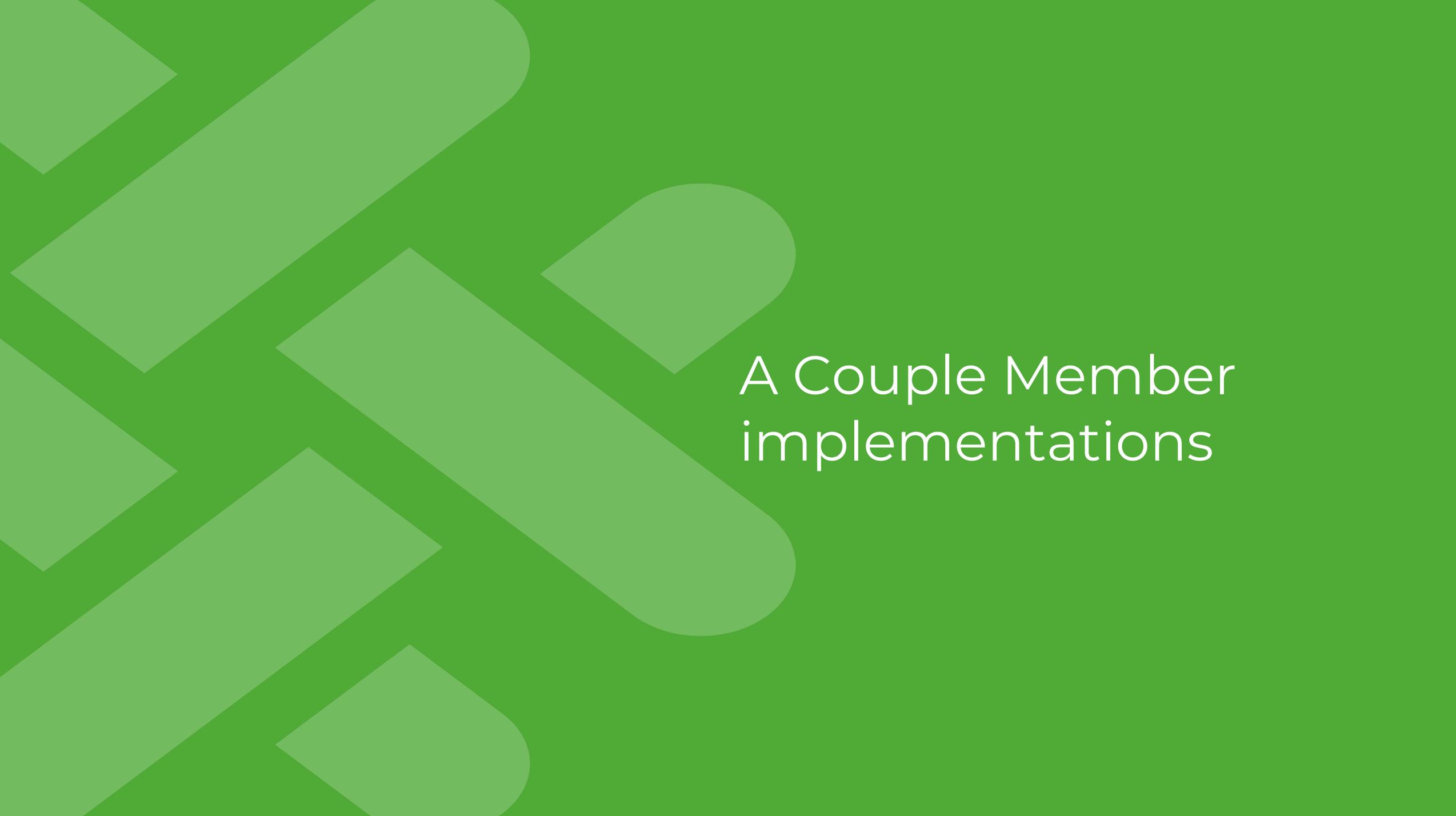


Member-facing Reporting - IP SLA

OSHEAN portal provides reporting for members to view network telemetry data with views tailored to their individual payloads

In this instance, OSHEAN provides visibility to IP SLA Protocol data to the edge of the OSHEAN Network (i.e. NYC)

Objective is to move the “edge” to the Cloud city by combining I2 data

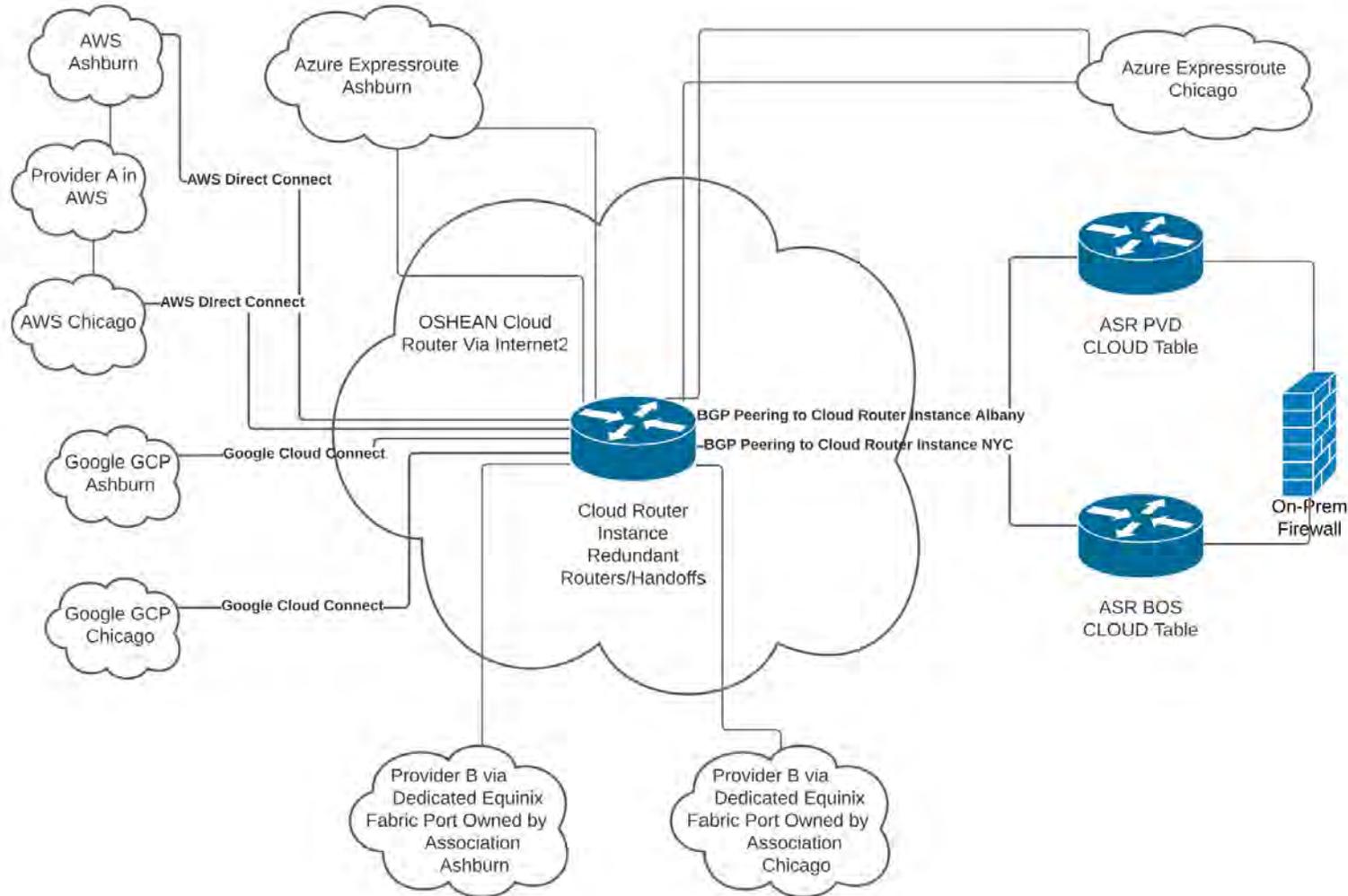


A Couple Member implementations

Member Cloud Migration

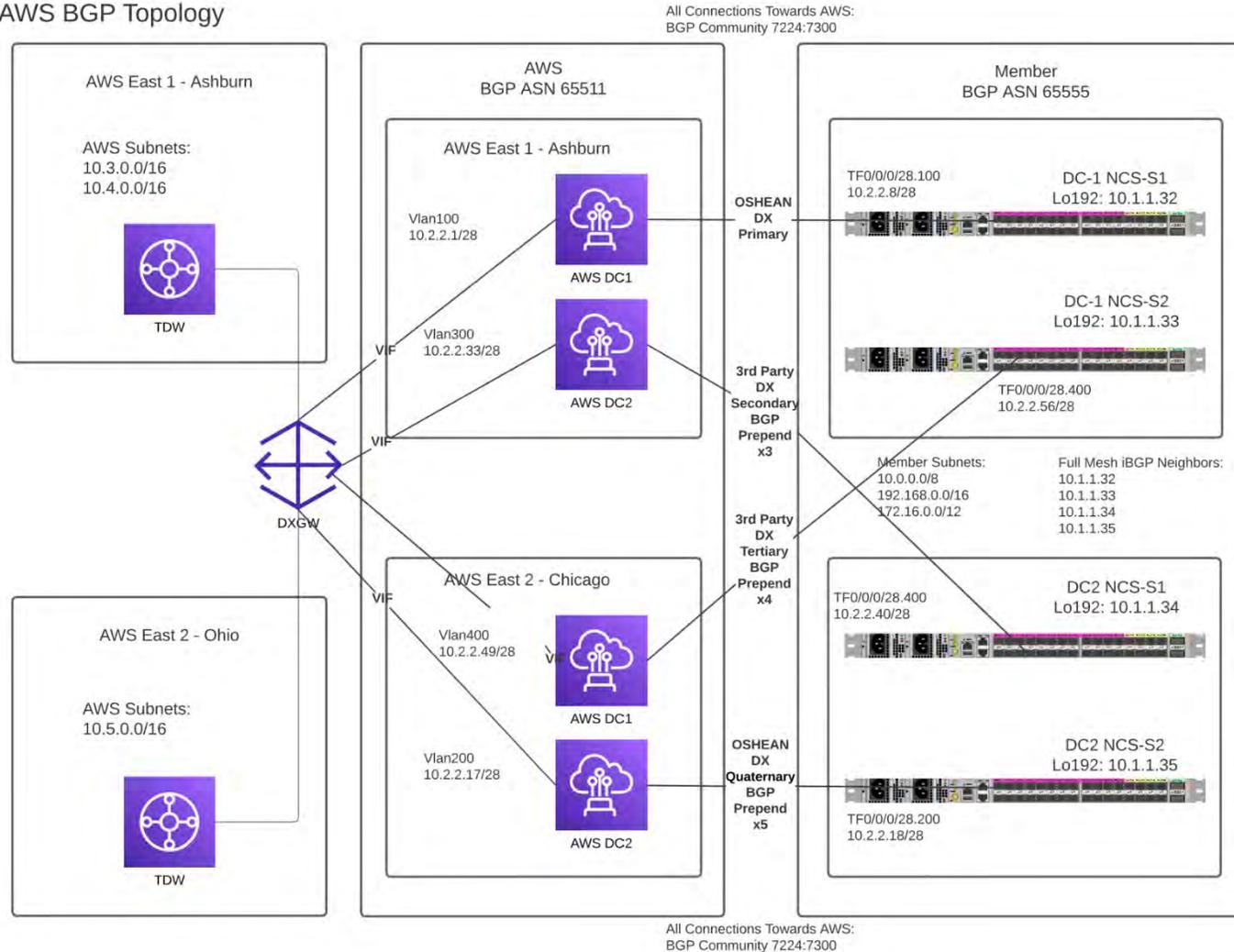
- ▶ OSHEAN member migrated their entire environment to the cloud over the last couple years.
 - ▶ All traffic transits OSHEAN and I2 fabric to Ashburn and Chicago
 - ▶ Utilizes each of the Big3, depending on app (10+ Cloud connect instances)
 - ▶ Fault tolerant, diverse city, topology
 - ▶ PVD data center is gone!

Integrated Cloud Exchange with I2



Integrated Cloud Exchange with I2

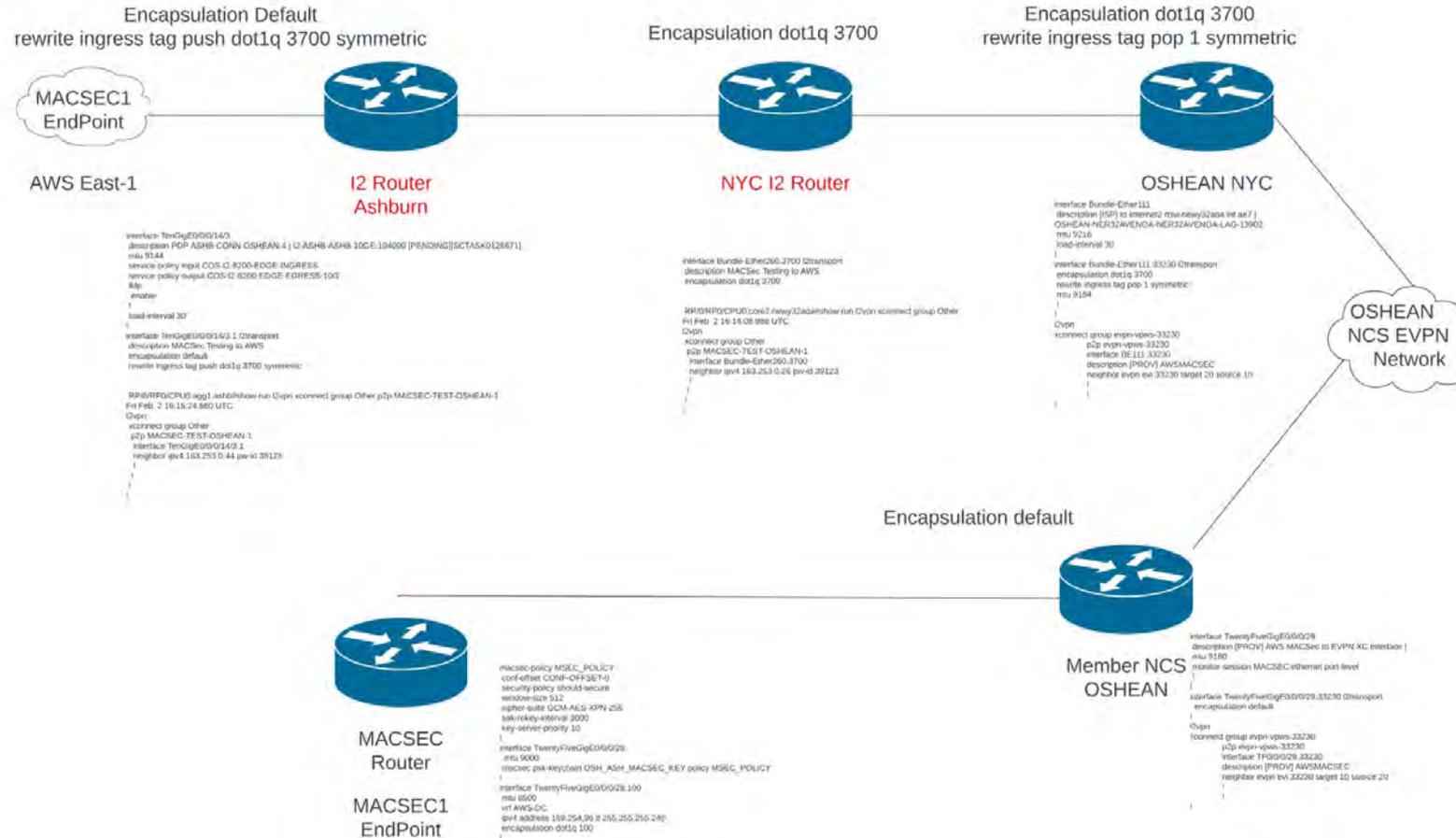
AWS BGP Topology

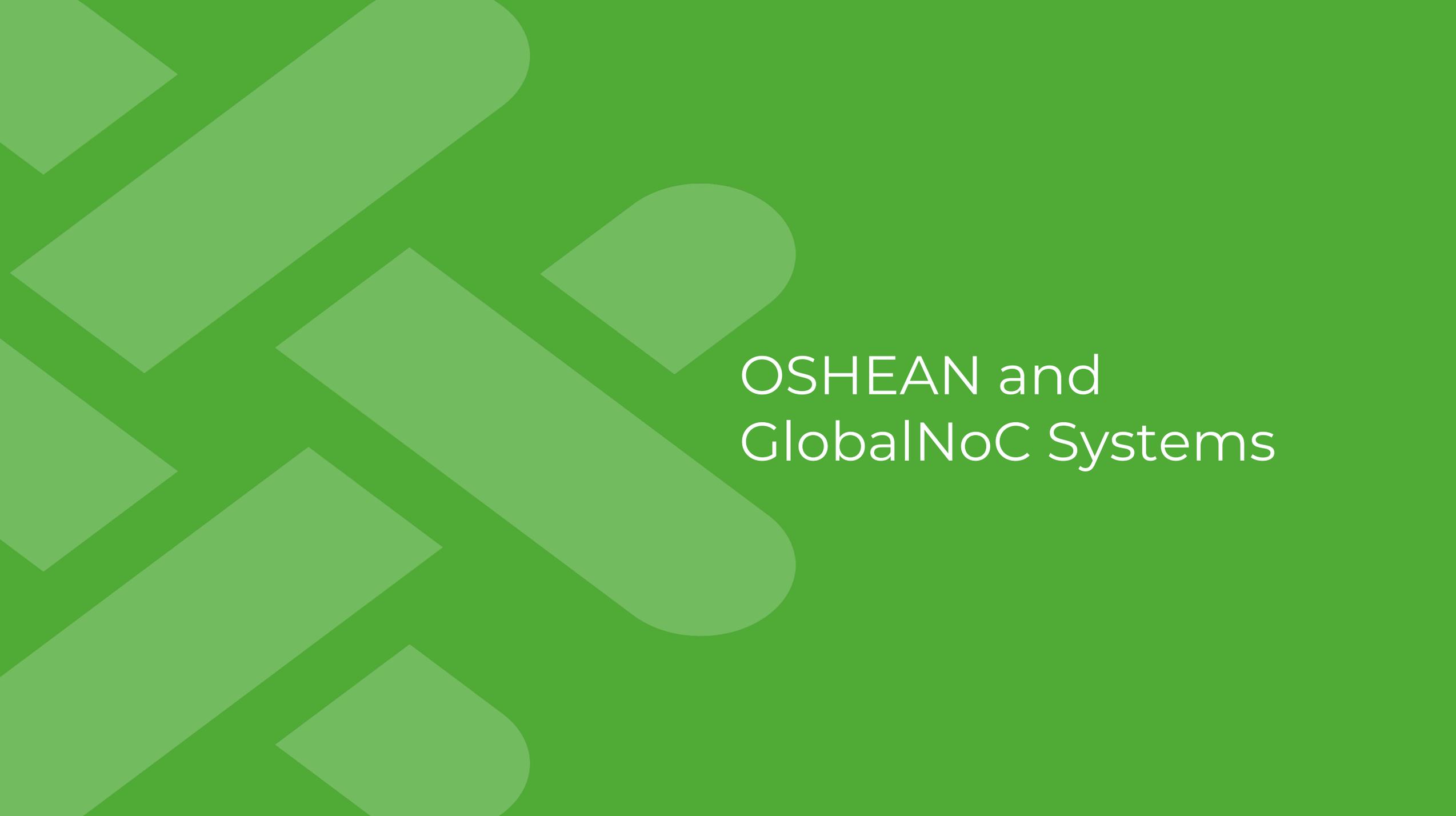


MACsec Encrypted Cloud Routes

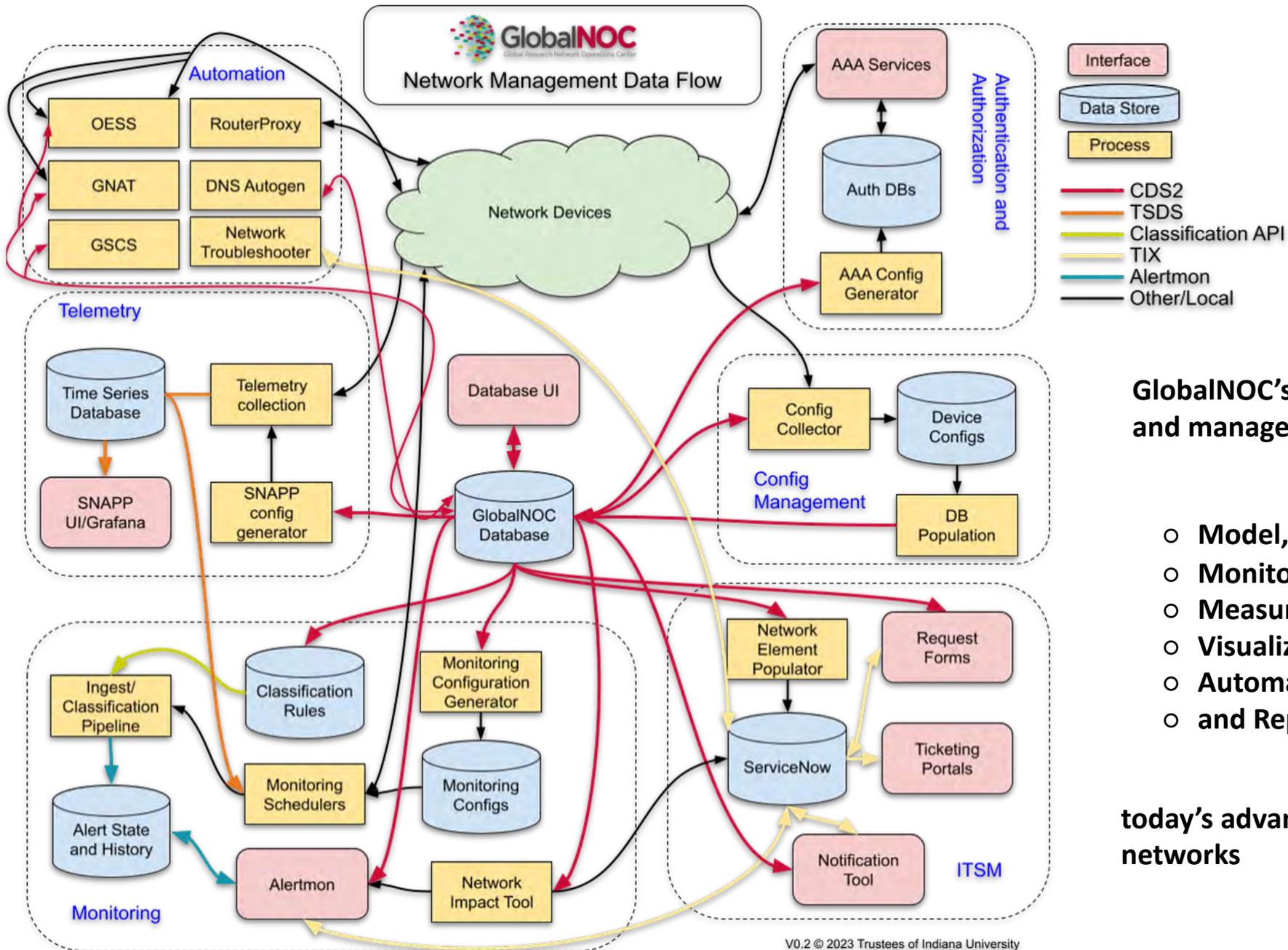
- ▶ OSHEAN has the first production MACsec routes in production through the I2 exchange for commercial (non-govt. traffic)
 - ▶ Layer 2 encryption through Internet2 RPI ports to AWS.
 - ▶ NCS at member site to AWS native receive.
 - ▶ Healthcare PHI application

MACsec Encrypted Cloud Routes





OSHEAN and GlobalNoC Systems



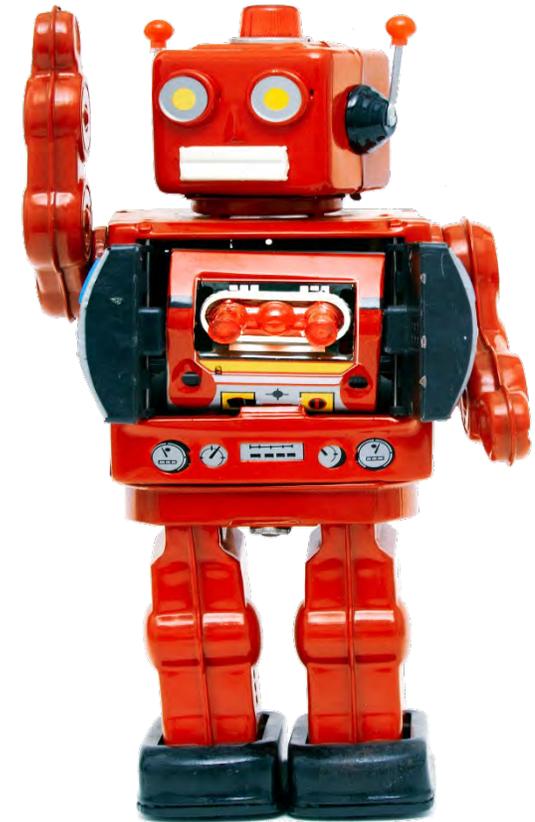
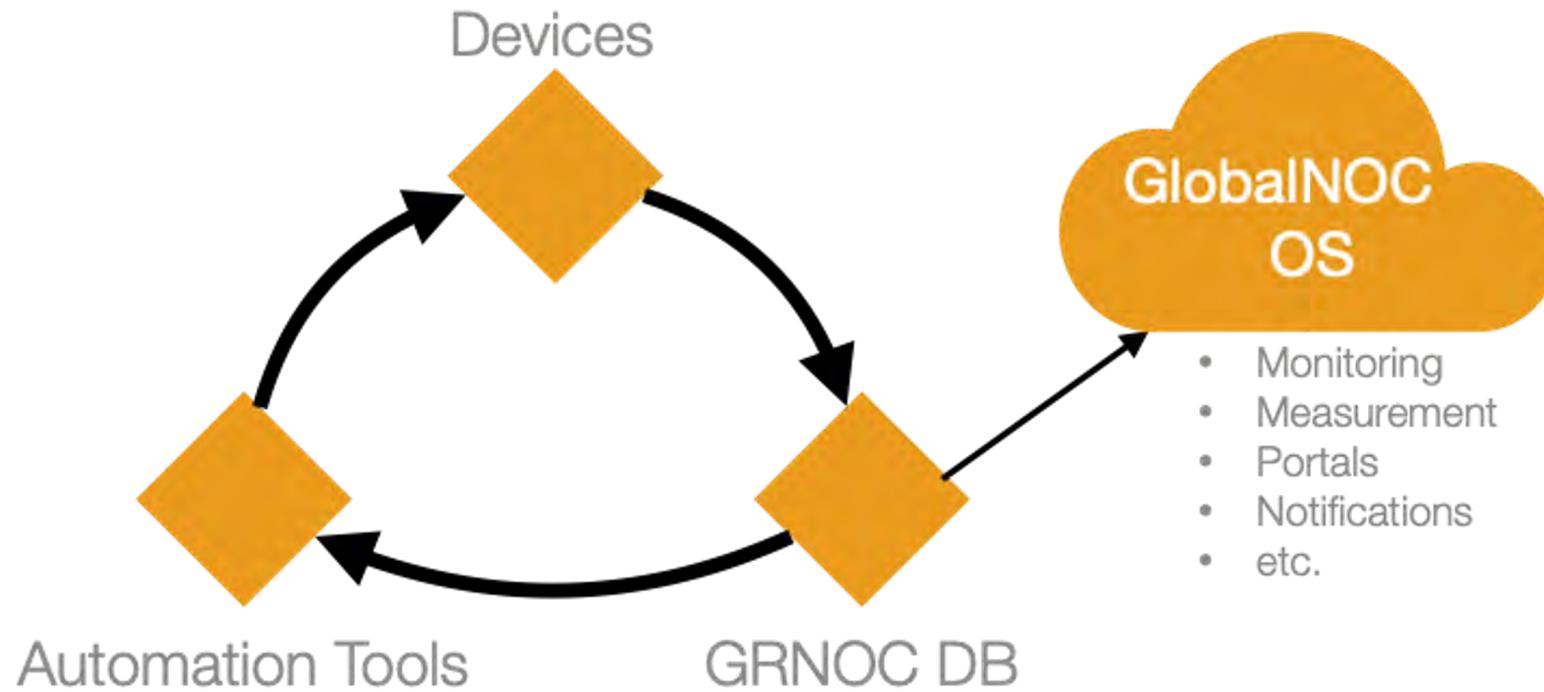
GlobalNOC's tools provide advanced telemetry and management functions in order to...

- Model,
- Monitor,
- Measure,
- Visualize,
- Automate & Control,
- and Report on

today's advanced Research and Education networks

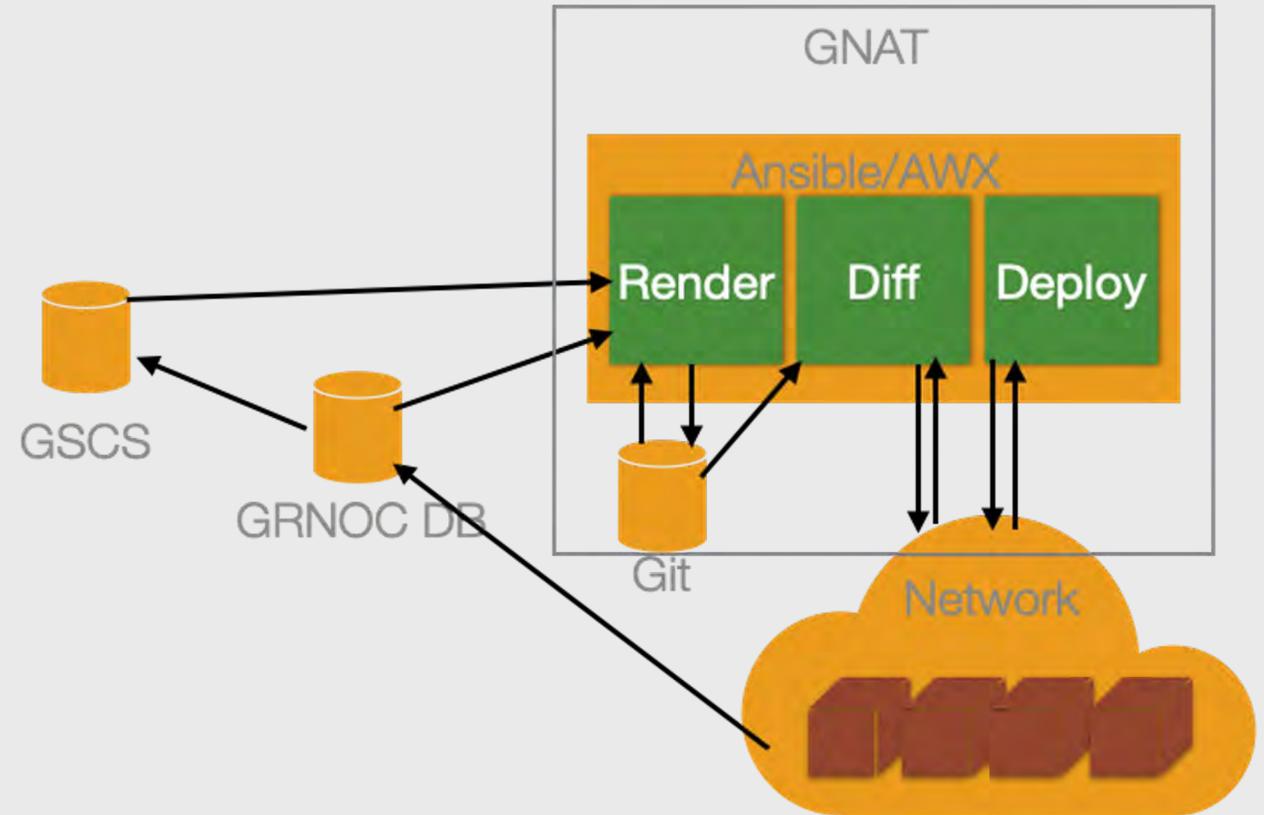
V0.2 © 2023 Trustees of Indiana University

Automating Network Configuration



◉ Integrated toolkit built on top of:

- Ansible / AWX
- Git / Github
- GlobalNOC Database
- Custom UIs for baseline automation and service configuration -- based on GNUI (what's this?)



GlobalNOC Home

Render and Diff Only Diff Diff and Deploy

Project: OSHEAN Branch: 3.0.4-test

Description: Deploying new ACLs in our 3.0.4 test branch

Submit

Device Selection Device Execution Order

Search:

Group by: device_type

Filter by: Add Filter

- iosxr
 - ncs-core1.nav400min.mgmt.oshean.org
 - ncs-core1.ner1summer.mgmt.oshean.org
 - ncs-core1.osh210benef.mgmt.oshean.org
 - ncs-core1.osh235prome.mgmt.oshean.org
 - ncs-core1.sto320washn.mgmt.oshean.org
 - ncs-core1.ton10beacha.mgmt.oshean.org
 - ncs-core1.uri1bairdhi.mgmt.oshean.org
 - ncs-core1.whe26emain.mgmt.oshean.org
 - ncs-core2.nav400min.mgmt.oshean.org
 - ncs-core2.ner1summer.mgmt.oshean.org
 - ncs-core2.osh210benef.mgmt.oshean.org
 - ncs-core2.osh235prome.mgmt.oshean.org
 - ncs-core2.sto320washn.mgmt.oshean.org
 - ncs-core2.ton10beacha.mgmt.oshean.org
 - ncs-core3.ner1summer.mgmt.oshean.org
 - ncs-core3.osh210benef.mgmt.oshean.org
 - ncs-core3.osh235prome.mgmt.oshean.org

GlobalNOC Network Automation Tool (GNAT) allows flexible baselining of network configurations and making large-scale changes across many network devices in a single automated workflow.

In this example, GNAT is being used to deploy new Access Control Lists across the OSHEAN network.

GlobalNOC Troubleshooter

Incidents

INC0165967

[View Ticket](#)

Alarm: ncs-mp1.cne101dudly.mgmt.oshean.org - BGP - 10.192.... History: Monday Feb 19 12:51 EST 2024

Critical
 ncs-mp1.cne101dudly.mgmt.oshean.org
 Since Mon Feb 19 12:15:11 EST 2024
 BGP to 10HEALTH2 is down (State: Last down time is within threshold of 30 minutes.),(CLEARED)

Ping Results
 Ping test with set sizes to verify MTU and to verify layer1 and layer2 connectivity to peer

Command	Results
ping vrf AWS-DC 10.192.0.33 count 10	Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/2 ms
ping vrf AWS-DC 10.192.0.33 count 10 size 1478	Success rate is 90 percent (9/10), round-trip min/avg/max = 1/1/2 ms
ping vrf AWS-DC 10.192.0.33 count 10 size 8975	Success rate is 90 percent (9/10), round-trip min/avg/max = 3/3/4 ms

Log messages
 Show the log matched on keywords 'BGP' and 10.192.0.33 Command: show logging | include 10.192.0.33 | include BGP

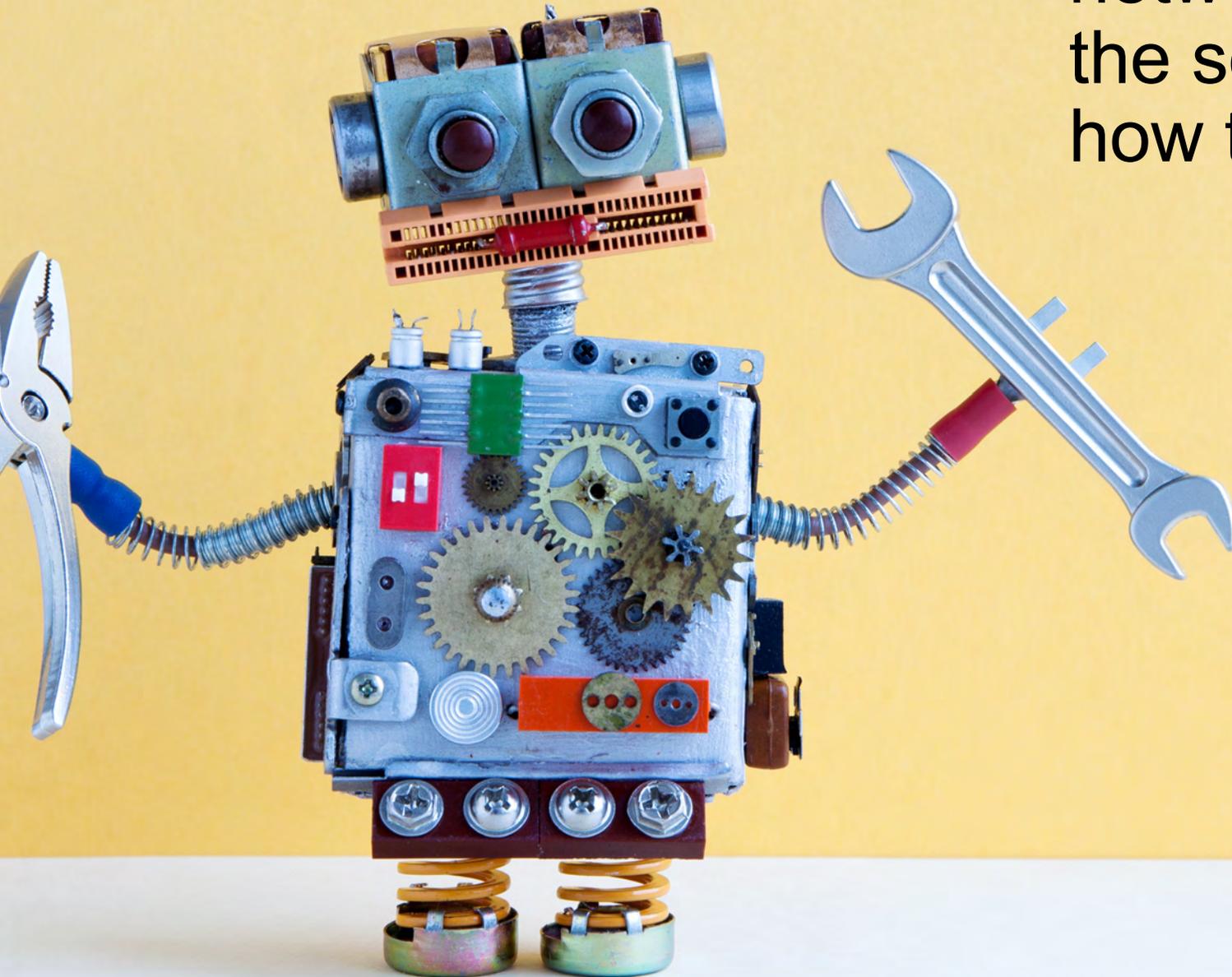
```

RP/0/RP0/CPU0:Feb 16 09:14:46.394 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Down - Peer closing down the session (VRF: AWS-DC) (AS: 400419)
RP/0/RP0/CPU0:Feb 16 09:15:12.599 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Up (VRF: AWS-DC) (AS: 400419)
RP/0/RP0/CPU0:Feb 17 16:45:38.856 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Down - Peer closing down the session (VRF: AWS-DC) (AS: 400419)
RP/0/RP0/CPU0:Feb 17 16:46:02.742 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Up (VRF: AWS-DC) (AS: 400419)
RP/0/RP0/CPU0:Feb 19 12:15:10.830 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Down - Peer closing down the session (VRF: AWS-DC) (AS: 400419)
RP/0/RP0/CPU0:Feb 19 12:15:36.262 EST: bgp[1085]: %ROUTING-BGP-5-ADJCHANGE : neighbor 10.192.0.33 Up (VRF: AWS-DC) (AS: 400419)
  
```

GlobalNOC Network Troubleshooter enables diagnostic automations for OSHEAN’s network infrastructure. The tool automates the early steps of event triage, formerly run manually by engineers, to reducing MTTR.

The troubleshooter is integrated with ServiceNow to automatically generate and populate trouble tickets.

Leveraging a telemetry-rich network to quickly determine the source of a problem and how to fix it!



Internet2 and Regional End-to-End Vision

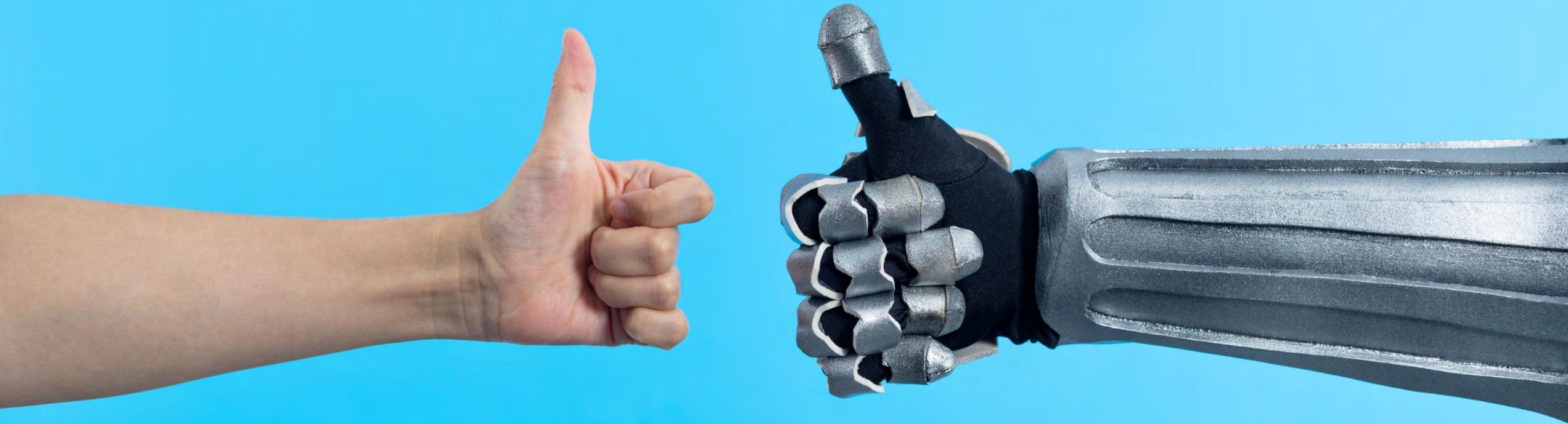
Visibility

Analytics

AI/ML Config.
and diagnostic
automation

Perimeter Reach
of Security

Robots and Humans working together to transform modern Research and Education Networks



The background is a solid green color with several overlapping, semi-transparent, rounded rectangular shapes in a lighter shade of green. These shapes are arranged in a pattern that suggests movement or a sequence of steps, with some shapes pointing towards the right and others pointing towards the left.

Backup Slides

How can we...

- Use automation to better support engineers working to resolve incidents on the networks we support?
- Get the right set of diagnostic data in front of engineers as quickly as possible
- Provide guided troubleshooting steps for a given incident type
- Provide options for engineers to initiate automated actions to remediate
- Provide support for completely automated remediation without human intervention

Service

View History

Name

OSHEAN-S20069

Nodes

+ ↕

Node Name

ncs-mp1.mid350emain.mgmt.oshean.org

Node ID

36561

openconfig
interfaces

Interface

+ ↕

Interface Name

GigabitEthernet0/0/0/10

Interface Tag

PROV

Sub-Interfaces

Sub-Interface

+ ↕

Rendered Config

Diff Deployed

View config for node:

Language:

ncs-mp1.mid350emain.mgmt.oshean.org

Source

group OSHEAN-S20069

```
interface GigabitEthernet0/0/0/10.3502 l2transport
interface GigabitEthernet0/0/0/10.3502 l2transport description [PROV][PROV] OSHEAN-S200
interface GigabitEthernet0/0/0/10.3502 l2transport encapsulation dot1q 3502
```

```
evpn evi description OSHEAN-S20069 | OSHEAN-NER1SUMMER-MID350EMAIN-EVPN-
evpn evi bgp
evpn evi advertise-mac
```

```
l2vpn bridge group bg- bridge-domain bd- description OSHEAN-S20069 | OSHEAN-NER1SUMMER-
l2vpn bridge group bg- bridge-domain bd- mtu 1518
l2vpn bridge group bg- bridge-domain bd- evi
```

```
l2vpn bridge group bg- bridge-domain bd- interface GigabitEthernet0/0/0/10.3502
```

end-group

GlobalNOC Service Configuration System (GSCS) automated service-level network configuration across your network.

In this example, GSCS is configuring a layer2 VPN service on the OSHEAN network.

BGP Route

Display the route to the BGP neighbor Command: show route vrf AWS-DC 10.192.0.33 detail

```
Routing entry for 10.192.0.33/32
Known via "ospf 99", distance 110, metric 3, type intra area
Installed Feb 9 15:54:51.134 for 1w2d
Routing Descriptor Blocks
10.192.0.30, from 10.192.0.6, via TenGigE0/0/0/14.192
Route metric is 3
Label: None
Tunnel ID: None
Binding Label: None
Extended communities count: 2
OSPF route-type:192:1:0x0
OSPF router-id:10.192.0.10
Path id:1 Path ref count:0
NHID:0xd(Ref:477)
NHID eid:0xffffffffffffff
MPLS eid:0x1281700000002
OSPF area: 192
10.192.0.25, from 10.192.0.6, via Bundle-Ether28091.192
Route metric is 3
Label: None
Tunnel ID: None
Binding Label: None
Extended communities count: 2
OSPF route-type:192:1:0x0
OSPF router-id:10.192.0.10
Path id:2 Path ref count:0
NHID:0xe(Ref:6)
NHID eid:0xffffffffffffff
MPLS eid:0x1282d00000002
OSPF area: 192
Route version is 0x5 (5)
Local Label: 0x675d (26461)
IP Precedence: Not Set
QoS Group ID: Not Set
Flow-tag: Not Set
Fwd-class: Not Set
Route Priority: RIB_PRIORITY_NON_RECURSIVE_MEDIUM (7) SVD Type RIB_SVD_TYPE_LOCAL
Download Priority 1, Download Version 658
No advertising protos.
```

Commit History

Show commit history to determine if any recent changes affected the BGP status Command: show configuration history last 15

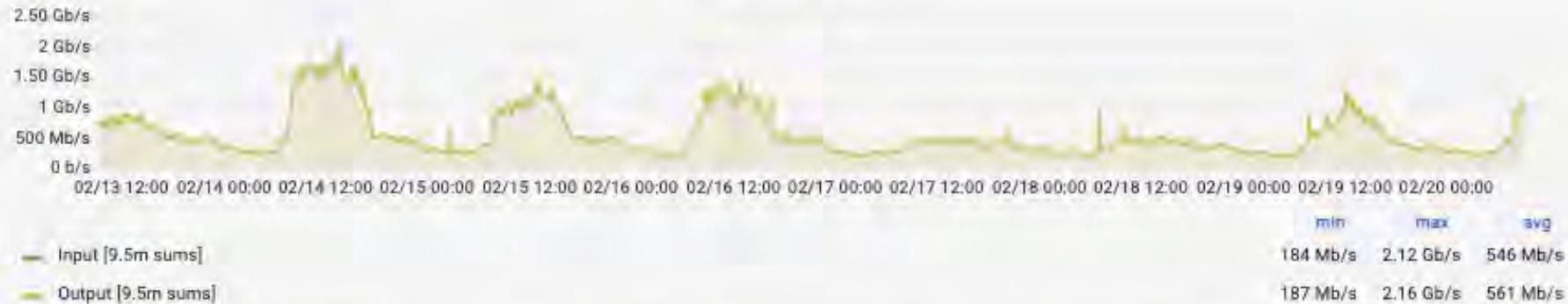
```
Sno. Event Info Time Stamp
-----
1 backup Periodic ASCII backup Fri Feb 16 22:37:27 2024
2 commit id 1000003005 Fri Feb 16 22:13:55 2024
3 backup Periodic ASCII backup Thu Feb 15 20:02:08 2024
4 commit id 1000003004 Thu Feb 15 19:31:16 2024
5 commit id 1000003003 Thu Feb 15 19:18:22 2024
6 rebase Commit database consolidation Thu Feb 15 19:10:33 2024
7 commit id 1000003002 Thu Feb 15 19:10:13 2024
8 commit id 1000003001 Thu Feb 15 19:08:21 2024
9 backup Periodic ASCII backup Thu Feb 15 19:07:05 2024
10 commit id 1000003000 Thu Feb 15 18:54:20 2024
11 backup Periodic ASCII backup Thu Feb 15 18:12:03 2024
12 commit id 1000002999 Thu Feb 15 18:10:54 2024
13 backup Periodic ASCII backup Thu Feb 15 14:31:59 2024
14 commit id 1000002998 Thu Feb 15 14:23:07 2024
15 backup Periodic ASCII backup Tue Feb 13 10:16:23 2024
```

Commit History

Show commit history to determine if any recent changes affected the BGP status Command: show configuration history last 15

```
Sno. Event Info Time Stamp
-----
1 backup Periodic ASCII backup Fri Feb 16 22:37:27 2024
2 commit id 1000003005 Fri Feb 16 22:13:55 2024
3 backup Periodic ASCII backup Thu Feb 15 20:02:08 2024
4 commit id 1000003004 Thu Feb 15 19:31:16 2024
5 commit id 1000003003 Thu Feb 15 19:18:22 2024
6 rebase Commit database consolidation Thu Feb 15 19:10:33 2024
7 commit id 1000003002 Thu Feb 15 19:10:13 2024
8 commit id 1000003001 Thu Feb 15 19:08:21 2024
9 backup Periodic ASCII backup Thu Feb 15 19:07:05 2024
10 commit id 1000003000 Thu Feb 15 18:54:20 2024
11 backup Periodic ASCII backup Thu Feb 15 18:12:03 2024
12 commit id 1000002999 Thu Feb 15 18:10:54 2024
13 backup Periodic ASCII backup Thu Feb 15 14:31:59 2024
14 commit id 1000002998 Thu Feb 15 14:23:07 2024
15 backup Periodic ASCII backup Tue Feb 13 10:16:23 2024
```

Aggregate

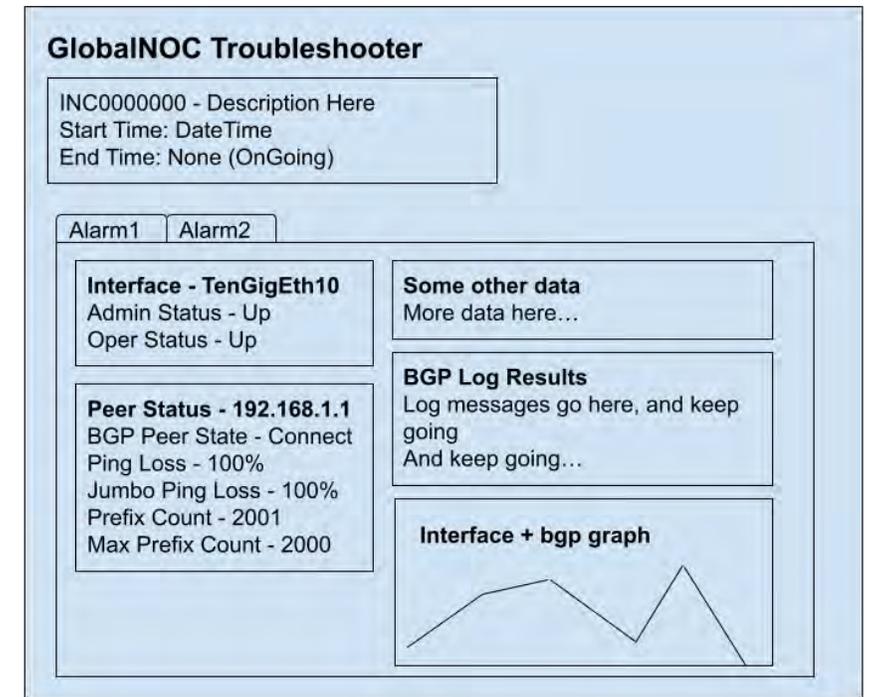
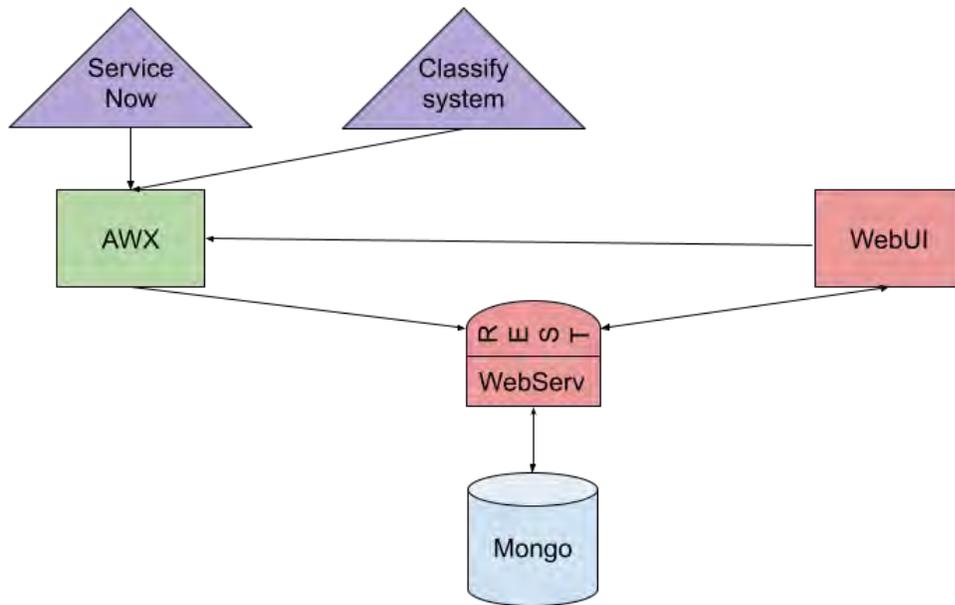


ncs-mp1.cne101dudly.mgmt.oshean.org - Bundle-Ether28091 - [SPAN9A][MBB] TO N...

ncs-mp1.cne101dudly.mgmt.oshean.org - Bundle-Ether28091.1 - [SPAN9A][MBB] TO ...

Incident-Specific Troubleshooting Dashboards





“The troubleshooting dashboard will require storage of data and page layout information and a way to fetch that data based on alarms associated with an Incident ticket. For each alarm in the ticket an **Ansible** playbook will be launched for the specific network and alarm-type. The playbook will fetch information and then write that information to a web-service (which stores the data in the database) for later usage by a **web UI**. The web UI will fetch the information from the web-service and then display the information to network engineers and service desk technicians working the incident..”

< ☰ INC0127546

- Preview Notifications
- Save
- Copy Incident
- Add to Visual Task Board
- Create Communication Record
- Create Child Incident
- Create Customer Service Ticket
- Create FSR
- Create Problem
- Create Request
- Open Network Troubleshooter
- Create Task
- Create Standard Change
- Refresh Impacted Services
- Metrics Timeline
- Export >



Launch Troubleshooter!



- **Run Books**
 - Providing the Service Desk and Engineers with written troubleshooting steps integrated with live data for troubleshooting each alarm type
- **Self Service Workflows**
 - Allowing Network Engineers to modify and create custom troubleshooter workflows on their own
- **Member/Portal Version of the Network Troubleshooter**
 - Enable a per-service version of the Troubleshooter to let members run the troubleshooter against services they use on the network