Internet2 Community Exchange 2024

David Marble – CEO OSHEAN
Instrumentation and Automation in Today’s R&E Networks

IOHO

In OSHEAN’s Humble Opinion
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*
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
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
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
Automating Network Configuration

Devices

Automation Tools

GRNOC DB

GlobalNOC OS
- Monitoring
- Measurement
- Portals
- Notifications
- etc.

OSHEAN
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 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 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
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
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.
<table>
<thead>
<tr>
<th>No.</th>
<th>Event Type</th>
<th>Event Description</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Fri Feb 15 22:37:27 2024</td>
</tr>
<tr>
<td>2</td>
<td>commit</td>
<td>10000003005</td>
<td>Fri Feb 15 22:13:55 2024</td>
</tr>
<tr>
<td>3</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Thu Feb 15 20:02:08 2024</td>
</tr>
<tr>
<td>4</td>
<td>commit</td>
<td>10000003004</td>
<td>Thu Feb 15 19:31:16 2024</td>
</tr>
<tr>
<td>5</td>
<td>commit</td>
<td>10000003003</td>
<td>Thu Feb 15 19:18:22 2024</td>
</tr>
<tr>
<td>6</td>
<td>rebase</td>
<td>Commit database consolidation</td>
<td>Thu Feb 15 19:18:33 2024</td>
</tr>
<tr>
<td>7</td>
<td>commit</td>
<td>10000003002</td>
<td>Thu Feb 15 19:10:13 2024</td>
</tr>
<tr>
<td>8</td>
<td>commit</td>
<td>10000003001</td>
<td>Thu Feb 15 19:08:21 2024</td>
</tr>
<tr>
<td>9</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Thu Feb 15 19:07:05 2024</td>
</tr>
<tr>
<td>10</td>
<td>commit</td>
<td>10000003000</td>
<td>Thu Feb 15 18:54:20 2024</td>
</tr>
<tr>
<td>11</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Thu Feb 15 18:12:03 2024</td>
</tr>
<tr>
<td>12</td>
<td>commit</td>
<td>10000002999</td>
<td>Thu Feb 15 18:10:34 2024</td>
</tr>
<tr>
<td>13</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Thu Feb 15 18:31:59 2024</td>
</tr>
<tr>
<td>14</td>
<td>commit</td>
<td>10000002998</td>
<td>Thu Feb 15 14:23:07 2024</td>
</tr>
<tr>
<td>15</td>
<td>backup</td>
<td>Periodic ASCII backup</td>
<td>Tue Feb 13 13:15:23 2024</td>
</tr>
</tbody>
</table>

### Aggregate

- **Input**: 184 MB/s, 2.12 GB/s, 546 MB/s
- **Output**: 187 MB/s, 2.16 GB/s, 561 MB/s
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.”
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