Monday (6/27/2022)
- 12:45 - 1:00 p.m. Welcome
- 1:00 - 1:45 p.m. Rural Broadband Initiatives, Dr. Michael Adelaine, CIO Emeritus and Professor Emeritus, South Dakota State University. Slides are attached.
- 1:45 - 2:30 p.m. Great Plains Network Research Platform, James Deaton, Executive Director of the Great Plains Network. Slides are attached.
- 2:30 - 3:00 p.m. Networking Break
- 3:00 - 3:45 p.m. Cyber Security, Kevin Hayes, CISSP, CISM, Chief Information Security Officer of the Merit Network. Slides are attached.
- 3:45 - 4:30 p.m. Microsoft 365 Panel, Paul Kern (Moderator) Network and Security Director at SD Board of Regents. Panelists: Kyle Gruhn, Director of IT Operations and Development, University of South Dakota; Lance Peterson, Chief Information Security Officer, University of South Dakota; Mavhu Chidaushe, IT Security Engineer, South Dakota State University; Tim Capps, IT Manager, Montana State University
- 4:30 – 5:15 p.m. Birds of a Feather (2nd floor mezzanine)
- Social hour at 6 p.m., followed by dinner at 7 p.m. (2nd floor mezzanine)

Tuesday (6/28/2022)
- 8:30 - 9:15 a.m. History of the NTNC, Marc Wallman, Vice President for Information Technology at North Dakota State University, Dr. Michael Adelaine. Slides are attached.
- 9:15 - 10:00 a.m. Annual meeting, future planning, and elections:
  ✓ Annual meeting location ideas: Jennifer Janecek-Hartman recommended a venue near Nueta Hidatsa Sahnish College, New Town, ND. The Steering Committee meeting will discuss this and other suggestions at its upcoming winter meeting.
  ✓ Elections: by unanimous agreement, Madhavi Marasinghe will serve as VP, Zach Rossmiller will serve as Secretary/Treasurer, and Marc Wallman will continue as President. Jennifer Janecek-Hartman was appointed as temporary Tribal College liaison, starting with the upcoming Steering Committee winter meeting, pending ratification as a member of the Executive Committee; Steering Committee meetings are open to all NTNC members and Tribal College representatives.
  ✓ Financial report (attached): Matt Riley stated that dues are $1,200 per institution per calendar year (U of Montana pays per fiscal year). We currently have $257,000 in our account. This year, we sponsored a WINS scholarship; additional sponsorships and financial support will be considered.
  ✓ A fellow program was proposed, to feature a historian duo, an elder statesman and a newer NTNC member, serving a one-year term documenting the NTNC history; in the meantime, everyone who has source documents will forward them to Marc, indicating whether a particular
At the upcoming Steering Committee, there will be discussion of potentially adding a historian position to the Executive Committee.

- **10:00 - 10:30 a.m. Networking Break**
- **10:30 - 11:15 a.m. NTNC state / TCUs Cyberinfrastructure Reports:**
  - Marc reviewed the NTNC & TCUs map; edits were recommended. See page 3.
  - South Dakota: rec’d funding via a CC** grant to build a statewide science DMZ. Completed a 100gig path from Aberdeen to Fargo.
  - AIHEC: just got funded with an EAGER proposal to build a CI Community of Practice for the TCUs, with 27 TCUs out of 35 committed to participate. Have been funded with a supplement to an existing award, in which NDSU’s Dane Skow is co-PI, for CI strategic planning, with 21 TCUs interested in participating. Looking for opportunities to collaborate for TCUs, including for TCUs joining Eduroam. Also looking for faculty collaborations, primarily on environmental monitoring in the ND area, and data science-related education in SD, as well as regional partnerships.
  - **Tribal colleges:**
    - Nebraska Indian Comm. College applied for a grant and have their own LT network.
    - Fond du Lac faced challenges during COVID and had to create laptop pools; the pandemic revealed digital disparity that was already in existence in tribal communities.
    - Cankdeska Cikana Comm. College applied for an FCC grant but had to withdraw. Internet connectivity is still the biggest issue there.
    - Nueta Hidatsa Sahnish College now has redundancy, cloud-based and on-site.
  - Nebraska: consolidated the U of NE wireless networking. Some projects are on hold due to equipment delivery delays.
  - Minnesota: U of MN working on an internet service to 100gig in Fargo. Started a project to centralize the firewall services group at the U of MN. Working on a unified communication strategy. Migrated to PCR for tele-management and billing. Evaluating a new wifi company.
  - North Dakota: UND is in the last leg of upgrading to 10gig. The student portal mobile app was published this week. NDSU has done a lot of network updates with CARES Act funds; switched 2/3 of the campus from Cisco to Aruba before the pandemic.
  - Montana: MSU has a new CIO. U of MT achieved R1 status earlier this year.
  - Wisconsin: there is a new University System president as of 6/1/22. During the pandemic, the U of WI system was upgraded to 100gigs to 4-year institutions and 30gigs to branch facilities. Still pursuing facilities-based networking. U of WI-Madison is running out of heating power facilities and are pushing off into private cloud facilities in the area and are in the process of investing in a research data center. Starting to consolidate IT across the System.
  - Illinois: there are underserved connectivity areas in the state, providing opportunities to assist. Collaborative opportunities are increasing at U of IL-Chicago; looking to do new HPC in the cloud.
  - PNWGP: looking at various upgrades. Working on fiber projects within Washington State.
  - Wyoming: U of WV is starting a school of computing. Working on meeting the criteria for cyber insurance.
- **11:15 - 11:30 a.m. Morning Wrap-up, Final Thoughts**
- **12 p.m. Meeting adjourned, safe travels!**
The Seven-Layer Cybersecurity Burrito

June 2022 NTNC Meeting

Kevin Hayes - CISO, Merit Network, Inc.
krhayes@merit.edu
Kevin Hayes

- Chief Information Security Officer
- 20 years in security industry for education and nonprofit
- Passion for cyber security education

CISSP – Information Systems Security Professional

CISM – Information Security Manager

GCIH, GCFA, GCCC, GCWN – SANS Incident Handling, Forensics Analysis, CIS Security Controls, Windows & PowerShell

CIHE, CPTE, CISSO – Mile2 Incident Handling, Penetration Testing, Security Officer
What We Can Do

Provide one-time and ongoing security assessments via our Community CISO services.

Our security assessments commonly utilize the CIS Critical Security Controls and the NIST Cybersecurity Framework.

Our experiences in the Michigan Cyber Range (MCR) directly inform us on practical attacks, tools, and techniques.

We practice what we preach with our integrated information security team.
# Example Cybersecurity Assessment

## Overall CIS Security Control Score

<table>
<thead>
<tr>
<th>Control Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic CIS Controls</strong></td>
<td>B-</td>
</tr>
<tr>
<td>Inventory &amp; Control of Hardware Assets</td>
<td>B+</td>
</tr>
<tr>
<td>Inventory and Control of Software Assets</td>
<td>B</td>
</tr>
<tr>
<td>Continuous Vulnerability Management</td>
<td>C-</td>
</tr>
<tr>
<td>Controlled Use of Administrative Privileges</td>
<td>C-</td>
</tr>
<tr>
<td>Secure Configuration for Hardware and Software</td>
<td>B</td>
</tr>
<tr>
<td>Maintenance, Monitoring and Analysis of Audit Logs</td>
<td>B</td>
</tr>
<tr>
<td><strong>Foundational CIS Controls</strong></td>
<td>B</td>
</tr>
<tr>
<td>Email and Web Browser Protections</td>
<td>B</td>
</tr>
<tr>
<td>Malware Defenses</td>
<td>A</td>
</tr>
<tr>
<td>Limitation and Control of Network Ports and Services</td>
<td>C-</td>
</tr>
<tr>
<td>Data Recovery Capabilities</td>
<td>A-</td>
</tr>
<tr>
<td>Secure Configuration for Network Devices</td>
<td>C-</td>
</tr>
<tr>
<td>Boundary Defense</td>
<td>A</td>
</tr>
<tr>
<td>Data Protection</td>
<td>B-</td>
</tr>
<tr>
<td>Controlled Access Based on the Need to Know</td>
<td>C-</td>
</tr>
<tr>
<td>Wireless Access Control</td>
<td>B+</td>
</tr>
<tr>
<td>Account Monitoring and Control</td>
<td>A</td>
</tr>
<tr>
<td><strong>Organizational CIS Controls</strong></td>
<td>C</td>
</tr>
<tr>
<td>Security Awareness and Training Program</td>
<td>C+</td>
</tr>
<tr>
<td>Application Software Security</td>
<td>B</td>
</tr>
<tr>
<td>Incident Response and Management</td>
<td>C-</td>
</tr>
<tr>
<td>Penetration Tests and Red Team Exercises</td>
<td>D-</td>
</tr>
</tbody>
</table>

## Control 2: Inventory and Control of Software Assets

<table>
<thead>
<tr>
<th>Grade</th>
<th>B</th>
</tr>
</thead>
</table>

**Synopsis**

The current environment for the ManageEngine product is also performing inventory of installed software packages on Windows platforms, and is able to enumerate package name and software version. Windows clients and servers are patched one to three weeks after Microsoft’s *Patch Tuesday* via a central WSUS server. Application software is typically limited and well known to IT staff. Non-Microsoft software is normally updated during regular OS refreshes. MDM product is actively managing applications on company-owned smartphones.

**Conclusion**

This control is being well performed, so long as the deployment of the ManageEngine software continues in earnest. Application whitelisting should be added to the security portfolio, especially with the heavy reliance on Microsoft server products.

**Recommendations**

1. Deploy AppLocker on all Windows systems, including any non-Domain Controller servers and workstations; this can begin with a policy where only signed code is permitted to run, with future enhancements permitting only approved vendors and applications. These protections will assist greatly in ensuring malicious code does not execute in the computing environment.

2. Continue with the deployment of the ManageEngine product and achieve 100% coverage for managed desktops and laptops.

3. Provide reports to management showing amount of out-of-date software in both client and server environments for consultation and signoff.
What Is The Cybersecurity Burrito?

A simple, layered approach to defend against what happens during typical ransomware and malware attacks.

Layers are critical because they will always be incomplete or they will fail.

Multiple layers buy you time to identify threats and discourage low-effort attackers.
A Typical Ransomware Attack

INITIAL ACCESS
Attacker looks for a way into the network

1. Exploit vulnerability
2. Email
3. Password guessing

VALID CREDENTIALS
Valid credentials

INTERNET-EXPOSED SERVICE
Internet-exposed service

COMMAND AND CONTROL
Command and control

LATERAL MOVEMENT
Lateral movement

PRIVILEGE ESCALATION
Privilege escalation

CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices

IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom

DATA EXFILTRATION
Data exfiltration

DESTROY BACKUPS
Destroy backups

ENCRYPT DATA
Encrypt data

Or Malicious Webpage
## Cyber Attack Continuum

<table>
<thead>
<tr>
<th>Opportunistic Attacks</th>
<th>Targeted Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Low Effort</td>
<td>- Higher effort</td>
</tr>
<tr>
<td>- Mass Scanning and Enumeration</td>
<td>- Slow and methodical Enumeration</td>
</tr>
<tr>
<td>- Relatively Automated</td>
<td>- Manual and deliberate</td>
</tr>
</tbody>
</table>

The attacker has no direct motivation to attack you in particular. The attacker really wants to attack you in particular and will invest time and effort.

These will take different strategies to combat.
The Attackers’ Achilles Heel

Attackers must succeed at each of these stages to be successful.

Disrupting them at any stage stops the entire attack.
We only need to break the attack chain at a single point, and a single time, in order to thwart bad actors.

Each element of a cyber attack has specific techniques, procedures, and indicators which can be detected and reported on.

In most cases, infrastructure used for cyber attacks is heavily reused.

Any attacker should only have one single shot to get through your defenses. The moment attackers are seen, they are toast.
Layer 1: Reconnaissance Protection

The first phase of any cyber attack is to learn about a target environment so that attacks can be more successful.

This can be simple and automated for unskilled attacks, and methodical and focused for targeted attacks.

There are easy defenses against both active and passive reconnaissance you can employ today.
Layer 1: Reconnaissance Protection

Use [https://shodan.io](https://shodan.io) and check your IP address space for any already existing reconnaissance.

Note down and block any undesired access.
Layer 1: Reconnaissance Protection

You can create a Shodan account **for free**. Or just log in using your Google or Windows account!

Once logged in, use the search filter **net**: followed by the CIDR notation of your subnet.

Full set of filters can be found at: [https://www.shodan.io/search/filters](https://www.shodan.io/search/filters)
Layer 1: Reconnaissance Protection

You can block TCP, UDP, and ICMP scans on your newer firewalls:

I have blocked scanners from the Internet extremely aggressively with no adverse results.

This will deter automated scans and frustrate dedicated attacks.
Today’s firewalls are well suited for scan and recon prevention.

Different vendors will have different variables and options to tune.

Not all vendors will have the same flexibility in configuration.

Log these events!

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto</td>
<td>Zone Protection Profiles</td>
</tr>
<tr>
<td>Juniper</td>
<td>Screens &amp; Flood Protection</td>
</tr>
<tr>
<td>Cisco</td>
<td>Intrusion Policies</td>
</tr>
<tr>
<td>Fortinet</td>
<td>DDoS Policy &amp; Portmap Signature</td>
</tr>
<tr>
<td>Watchguard</td>
<td>Packet Handling Options</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>IPS Protection / Host Port Scan</td>
</tr>
<tr>
<td>Sonicwall</td>
<td>Local Policy / Port Scanner</td>
</tr>
</tbody>
</table>
Layer 1: Reconnaissance Protection

You can also use **dynamic groups** to block ever-moving IP targets.

Block common scanners, Tor exit nodes, and other items from commercial or open source intelligence feeds.

Lists typically have IP addresses or domain names.

Blocking high-risk endpoints is minimal risk and very high gain.
Layer 1: Reconnaissance Protection

Create a firewall rule blocking traffic going to or from these groups.

Different vendors will make the population of these dynamic objects easier or harder than others.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Dynamic Object Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palo Alto</td>
<td>External Dynamic List</td>
</tr>
<tr>
<td>Juniper</td>
<td>Dynamic Address Group</td>
</tr>
<tr>
<td>Cisco</td>
<td>FTD Security Intelligence List</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Threat Feed</td>
</tr>
<tr>
<td>Watchguard</td>
<td>Blocked Site Import</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>Dynamic Objects</td>
</tr>
<tr>
<td>Sonicwall</td>
<td>Dynamic External Address Group (DEAG file)</td>
</tr>
</tbody>
</table>
Layer 1: Reconnaissance Protection

There are untold sources of places you can find Indicators of Compromise (IOCs) which can be used as part of your automatic threat blocking infrastructure:

Bad DNS Domains:
https://www.malwaredomainlist.com/
https://maldatabase.com/
https://ransomwaretracker.abuse.ch/
https://isc.sans.edu/threatfeed.html

Lists of Threat Feeds:
https://github.com/hslatman/awesome-threat-intelligence
https://threatfeeds.io/
Layer 2: Updates and Patches

Initial attacks are usually only a tiny toehold in your environment, and attackers will need to move laterally to find the “big fish”. Lateral movement is made extraordinarily easy when unpatched operating systems and applications are abound!
Layer 2: Updates and Patches

Unsupported operating systems will no longer receive security updates, however that does not stop researchers and attackers from finding new ways to exploit them.

If they cannot be removed, isolating them onto a VLAN may be acceptable for the short term.
Layer 2: Updates and Patches

Even if your border firewall is blocking everything, attacks can still succeed thanks to our users browsing the Internet.

Twelve updates for Chrome in 2022.

Google Releases Security Updates for Chrome

Original release date: April 28, 2022

Google has released Chrome version 101.0.4951.41 for Windows, Mac, and Linux. This version addresses vulnerabilities that an attacker could exploit to take control of an affected system.
Layer 2: Updates and Patches

Use WSUS, SCCM, Puppet, JAMF, Ninite, or your other favorite endpoint application to keep updates on schedule and uniform.

Attackers only need a single unpatched computer to proceed. Don’t give it to them!

Severe vulnerabilities in Dell firmware update driver found and fixed

Dell firmware update driver 2.3 can be exploited to gain kernel-level privilege.

JIM SALTER - 5/5/2021, 7:39 PM
Layer 2: Updates and Patches

You must keep a detailed inventory of all your network devices for this to work.

This includes all of those pesky non-managed devices, including phones, printers, projectors, media carts, smart devices, and IoT devices.

These devices have even worse security postures than Windows systems.
Layer 2: Updates and Patches

Software like LanSweeper or NetDisco can interrogate your network and find all of your devices. Even the silent ones!
Layer 2: Updates and Patches

Unlike managed systems, IoT devices will have their firmware updated much less often.

Do you feel comfortable all your unmanaged and IoT devices are getting regular updates?
Layer 3: Malware Protection / DNS

At this point, we are assuming that not only has reconnaissance been successfully performed, but that malicious code is being attempting to be executed on an endpoint.

This is due to the exploit of a vulnerability, either via an exposed Internet service or via client software and actions such as opening a file or visiting a vulnerable website.

Next steps are to stop the execution of malware, as well as detect the command and control capabilities using DNS protection.
Layer 3: Malware Protection / DNS

Microsoft has come a long way since the introduction of the Windows Operating System.

Many vendors have their own products, however being able to watch for activity and execution at the Operating System layer is a pretty good job for the operating system itself.

Windows Defender has a great integration and a pretty good catch rate when it comes to identified signatures and heuristic threats.

If you have nothing else, turn on Windows Defender on your managed desktops and servers, and remove the ability to disable the service.
Layer 3: Malware Protection / DNS

No matter your solution, monitor your respective console for alerts and act on every single one.

Tune your rules if necessary, but always respond.

You are already paying for the ability to see if threats are being detected!
Layer 3: Malware Protection / DNS

To protect unmanaged systems, we can watch DNS for abnormal requests. For the moment, this is a really good way in which you can detect many different versions of malware and ransomware on your network.

The Domain Name System (DNS) is used to translate between textual names and IP addresses.

Malware frequently uses DNS to communicate with its Command and Control (C2) infrastructure, either with static domain names or a Domain Generating Algorithm (DGA).
Layer 3: Malware Protection / DNS

Watching for malicious DNS traffic is easy and there are many options for both commercial and free services:

- CloudFlare / OpenDNS and CIS offer free services.
- Cisco Umbrella is a very powerful managed service.
- Firewalls may have DNS subscriptions which will intercept traffic not going through your DNS resolver server.
Layer 3: Malware Protection / DNS

**Malware Blocking Only**

Change your router DNS to:
- 1.1.1.2
- 1.0.0.2

**Malware and Adult Content Blocking Together**

Change your router DNS to:
- 1.1.1.3
- 1.0.0.3

---

**SLT Workstation**

Request for malicious domain www.badsite.com

**SLT DNS Server**

SLT DNS server passes message that requested domain does not exist, causing a break in malware functionality

Request for www.badsite.com passed to Akamai

**Akamai**

Akamai identifies domain as malicious. Responds back with “no listing exists”

**MS-ISAC and EJ-ISAC SOC**

Logs of blocked malicious domain requests sent to MS-ISAC and EJ-ISAC SOC

**MS-ISAC and EJ-ISAC SOC**

Provides regular reporting on blocked domains

https://1.1.1.1/family/

https://mdbr.cisecurity.org/
Layer 4: Privilege Escalation

Administrator rights can turn an annoying computer hack into a devastating one.

Attackers will search for elevated rights, whether they are for IT employees, regular employees, or even for the local computer account. Don’t give it to them!
Layer 4: Privilege Escalation

You need to make your regular computers and accounts look identical to everyone else at your organization.

If attackers run malware on your desktops, they should not be able to perform any important or elevated actions.

Instead, utilize separate accounts which have differing levels of access based on what you want to accomplish.

<table>
<thead>
<tr>
<th>Username</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>khrayes</td>
<td>Normal Domain Account</td>
</tr>
<tr>
<td>a_krhayes</td>
<td>Workstation Administration Account</td>
</tr>
<tr>
<td>s_krhayes</td>
<td>Server Administration Account</td>
</tr>
<tr>
<td>da_krhayes</td>
<td>Domain Administration Account</td>
</tr>
</tbody>
</table>
Layer 4: Privilege Escalation

That pesky local Administrator account is a huge problem if discovered by an attacker.

Use LAPS to randomize it and store it in an attribute on the Active Directory computer object; this is a documented GPO and AD Extensions by Microsoft and includes the periodic cycling of the local password.

Free utility available at:
Layer 4: Privilege Escalation

Default usernames and passwords will be tried in the first few moments of an attacker discovering an unmanaged or IoT device.

These credentials are commonly found in support documentation and are highly searchable on the Internet.
Layer 5: Host Based Firewalls

You will **not** have network firewalls between all of the hosts in your network, however you will still need to throw up roadblocks.

You need to assume that attacks will come from **inside your organization** if we have gotten this far into an attack.

While privileges have may or may not be escalated, an attacker will continue to use lateral movement to find a better toehold or beachhead inside your environment. **We need to stop that from happening!**
Layer 5: Host Based Firewalls

Write Windows Firewall Rules for every machine in your environment!

The **domain profile** applies to networks where the host system can authenticate to a domain controller.

The **private profile** is a user-assigned profile and is used to designate private or home networks.

The **default profile** is the public profile, which is used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.
Layer 5: Host Based Firewalls

For the best bang for your buck, **enable and scope** firewall rules for administrative services such as Remote Desktop, WMI, SMB, and Remote PowerShell.

Connections should come from **trusted** management networks and workstations.
Layer 5: Host Based Firewalls

When permitting server applications, utilize application-based rules; use `netstat` to identify the ports they are listening on and the name of the executable.

`netstat -abon` from an elevated prompt will provide this information.
Layer 5: Host Based Firewalls

Unmanaged devices will be the “wild west” when it comes to host-based firewalls.

You will have to check the configuration options of each device you have to see if there is an option to restrict access on a device level. **Use this where you can!**
Layer 6: Network-Based ACLs

Your servers and workstations can have easy host-based firewalls, but what can be done when that burrito layer falls flat?

Network router ACLs are the “budget firewall” that virtually everybody can use everywhere.

ACLs can be placed “in front of” network segments or VLANs, ensuring any traffic entering the VLAN must be permitted.
Layer 6: Network-Based ACLs

Remember those annoying IoT and other non-manageable devices back in Burrito Layer 2? This is the perfect place for them to be.

As you run asset scans, migrate these devices to dedicated VLANs and networks which are protected by these ACLs.

Ideally you will already be doing this during the onboarding of new devices, but network scans will catch anything which was missed.

Only permit access from actual required sources!
Layer 7: Multifactor Authentication

When all else fails, attackers will be using user credentials to gain elevation and migrate through your infrastructure.

Multifactor authentication grinds this to a halt, as now a step outside the control of the attackers is forced on to them.

This is extremely important in the case of public well-known services, specifically email and remote access VPN.
Layer 7: Multifactor Authentication

Google and Microsoft MFA are typically free addons for their basic services. Use them if you have nothing else!

Premium services such as Duo can link together multiple applications and services once you are ready.

It is impossible to prevent employees from reusing their work passwords elsewhere in their lives, but this then brings password management back under our control.
Bringing Together the Burrito

Seven Layers of Goodness:

1. Blocking Reconnaissance Attempts.
2. Preventing Exploitation with Aggressive Patching.
3. Antivirus Halts Malware Execution and DNS Discovers Unknowns.
4. System Processes Protected via Admin Password Control
5. Host-Based Firewalls Halt Side-to-Side Pivoting
6. Network ACLs Protect Pivoting Universally
7. MFA Protects Email and VPN Services
Lessons Learned

There are lots of things you can do to help secure your environment from cyber attacks, and **lots of resources** to help you along the way.

**Thinking** like a cyber criminal will let you focus your efforts into the most vital places first. You can always continue to expand from there.

Simple, quick wins described here will **discourage** all but the most motivated attackers.
The Seven-Layer Cybersecurity Burrito

June 2022 NTNC Meeting

Kevin Hayes - CISO, Merit Network, Inc.
krhayes@merit.edu
NTNC Financials

Through March 31, 2022

Current NTNC Balance: $ 257,502
NTNC Fund Balance and Revenue History

NTNC Fund Balance and Revenue: 2004-2022

- 2022 = $257,502
- 2022 = $27,600
Expenses During COVID

• This Meeting... guessing it will be relatively inexpensive

• WINS Scholarship...
  • $7,500 with a preference for an NTNC or tribal college attendee

.... That’s It really since 2019
GP ANRP
Developing a Regional Research Platform
June 27, 2022
A special thank you to James Deaton (@GreatPlainsNet) and Jim Stewart (@uennews) for their leadership in serving as the NGI NAOP working group chairs. We're also very appreciative of Bernie Gulachek (@UMNews) for hosting the NGI Community Architects' workshop. Thank you, Bernie!
The Great Plains Network (GPN) is a non-profit consortium aggregating networks through GigaPoP connections while advocating research on behalf of universities and community innovators across the Midwest and Great Plains who seek collaboration, cyberinfrastructure and support.

- Over two dozen universities
  - Across 9 states
  - 25 years of collaborating in research and education networking
Background

- Founded by researchers and for researchers
- Initially funded and started in 1997 by NSF EPSCoR
- One of the largest connectors for Internet2
- While the topology of the GPN physical network has changed over time, the GPN membership has grown because of a shared commitment to maintain an organization that sustains a collaborative and interdisciplinary focus among the membership.
Governance and Advisory Committees

- Executive Council (EC)
- Network Program Committee (NPC)
- Representative Council
- Cyberinfrastructure Program Committee (CIP)
- Network Technical Advisory Committee (NTAC)
  - Blue Ribbon Committee (BRC)
- Security Committee
Fun GPN/Internet2 Facts

- 1st to connect to Internet2 backbone @ 155Mbps
- 1st to upgrade to 2 x 10GE to Internet2
- 1st to have 3 x 100GE to Internet2
- All (okay, many) of Internet2’s best folks were previously dear members of GPN’s community
  - Rick Summerhill, Linda Roos, Dale Finkelson, Dana Brunson, Tim Middelkoop, James Harr…
Connected via 6 state networks and a RON

- ARE-ON
- KanREN
- MOREnet
- Network Nebraska
- OneNet
- SD-REED

- BOREAS
History of CI Sharing and Facilitation in the Region

ONEOCII
OneOklahoma Cyberinfrastructure Initiative
http://www.oneocii.okepscor.org/

ACI-REF Virtual Residency

ENCITE:
Enhancing Cyberinfrastructure by Training and Engagement
https://www.greatplains.net/archives/presentations/

GPN Cyberinfrastructure Program Committee (CIP)

THE CARPENTRIES
Universities in the Region Directly Impacted by CC* Grants

Black Hills State University  
Cameron University  
East Central Oklahoma University  
Fort Hays State University  
Kansas State University  
Langston University  
Northeastern State University  
Oklahoma State University  
Oral Roberts University  
Rogers State University  
South Dakota School of Mines and Technology  
South Dakota State University  

Southwestern Oklahoma State University  
University of Arkansas  
University of Arkansas at Pine Bluff  
University of Central Oklahoma  
University of Kansas  
University of Missouri-Columbia  
University of Missouri-Kansas City  
University of Nebraska-Lincoln  
University of Oklahoma Norman Campus  
University of South Dakota Main Campus  
University of Tulsa
GPN CC* Proposal Repository

GPN members continue to make past successful proposals available. Feel free to request access via this link.

Examples across many categories are available
Quilt CC* Proposal Development Corner

Username: Quilt-CC-Star
Password: 2020-Proposal

GPN members were speakers for 3 of the sessions
Non-profit organization that:

- Trains people in software development and data science skills for more effective work and career development
- Builds community and local capacity for teaching and learning these skills and perspectives
**Software Carpentry**
- Audience: researchers who need to program more effectively
- Domain independent
- Modular curriculum: three distinct sections, one optional

**Data Carpentry**
- Audience: researchers who are dealing with significant data
- Domain specific (ecology, genomics, GIS, others...)
- Full, two day curriculum centered around a single dataset

**Library Carpentry**
- Audience: People in library and information related roles
- Domain focus: Collections & information support (e.g.: museums & archives), LIS
- Modular curriculum centered around core objectives and lessons

*Flexible scheduling*
Quad Chart for:

**Challenge:**
Supporting computational and data-intensive research at under-resourced institutions in rural states is challenging.

- Sparse populations
- Fewer trained CI staff
- Smaller research output
- Less participation in national CI community.

**Broader Impact:**
- Drives CI development and adoption in EPSCoR States
- Enables advancements on campuses currently underserved by advanced CI
- Develops and disseminates CI best practices for an effective CyberTeam

**Approach:**
- Bring CI expertise directly to rural campuses.
- Cross-institutional distributed support team with 4 key foci:
  - Networking
  - System Administration
  - Security
  - Researcher Training and Outreach
- Leverages existing collaboration model of regional networks
- Pairs regional mentors with mentees and students
- Onsite campus engagement focused on enabling specific science workflows

**Great Plains CyberTeam**
Intentions

• Give a platform for women and minorities who utilize HPC resources
• Establish a support network, including allies
• Outreach to underserved institutions
• Increase visibility of advanced cyberinfrastructure professionals and researchers
Zoom meetings – second Wednesday of each month
12 noon – 1 pm Central

Current Leadership Team

Kate Adams, Great Plains Network
Boryana Koseva, children’s Mercy Hospital, Kansas City, MO
Kim Owen, North Dakota State University
Natasha Pavlovikj, Univ NE Lincoln
Christina Roberts, University of MO
To join the email list to receive notifications email Kim Owen [kim.owen@ndsu.edu]
CC* Compute: ARGO: The Great Plains Augmented Regional Gateway to the Open Science Grid

Expand GPNRP model
Train and develop local/regional researcher-facing staff
Deploy 18 HTC compute nodes across region, including gateways to local HPC resources
Augment CyberTeam CC* to train users, engage administration
The Great Plains Augmented Regional Gateway to the Open Science Grid

GP-ARGO creates a regional distributed Open Science Grid (OSG) Gateway led by the Great Plains Network (GPN) to support computational and data-intensive research across the region through the development of specialized CI resources, workforce training, and cross-support methodologies and agreements.
Resources contributed to the Open Science Grid

Core Hours Contributed
4,115,920

OSG Projects
86

Institutions Supported
62

Collaborating Campuses
- Arkansas State University
- Creighton University
- Dakota State University
- Emporia State University
- Kansas State University
- Langston University
- Oklahoma State University
- Oral Roberts University
- South Dakota School of Mines and Technology
- South Dakota State University
- Southeast Missouri State University
- University of Arkansas
- University of Arkansas for Medical Sciences
- University of Kansas
- University of South Dakota
- Wichita State University

OSG Project	Core Hours
---
Gravitational Physics	687,460
University of Michigan
ID: Michigan_Riles

Astronomy	567,078
American Museum of Natural History
ID: AMNH.astro

Astrophysics	492,679
University of Chicago
ID: spt.all

Nuclear Physics	428,105
Wayne State University
ID: WSU_3DHydro

Astronomy and Astrophysics	249,876
Rochester Institute of Technology
ID: CompBinFormMod

Bioinformatics	201,478
University of Pittsburgh
ID: BiomedInfo

Chemical Sciences	201,194
Carnegie-Mellon University
ID: TG-CHE200122

Chemistry	162,872
University of Chicago
Campuses and institutions that donate compute resources to the #OSPoo! make this all possible.

Thank you @Lancium @GreatPlainsNet @BrookhavenLab and many more for helping power the OSPool in the past month! We appreciate your contributions to open science!

Throughout the month of May, users leveraged 7.66 MILLION core hours on the OSPool to run 6.54 MILLION jobs!

That’s a lot of #OpenScience

Discover how May looked on the OSPool: bit.ly/3GCEFqq
Step back to FIONAs (high performance DTN)

- 11 purchased in the first wave with half funded by initiatives within states
  - 1 continues to show up on Internet2 maps as a thank you to GPN - one of the busiest OSG caches
- 8 more FIONAs have been purchased inspired by the design of the initial 11.
- Growing number are contributing to the Nautilus cluster
Share Computing Resources with Institutions in the State or the Region or Nationally

Infrastructure for Managing and Analyzing Big Data
Arkansas Research Platform (ARP)

- HPC/Cloud computing
- Petabyte scale storage
- Highbandwidth Networking
- Best practice tools for software development/ code management
- Provides support for all research themes
- DART requires a statewide infrastructure:
National Research Platform (NRP)

Partners and Collaborators

it²
CENIC
GPN
INTERNET²
KINBER
LEARN
nysernet
The Quilt
CITRIS
AND THE
BANATAO
INSTITUTE
Namespaces as a collaboration environment
https://pacificresearchplatform.org/nautilus/namespaces

600+ namespaces in the cluster
Participation in the PRP’s “Nautilus Hypercluster”

PRP’s “Nautilus Hypercluster” provides a platform where members of our community - whether they are researchers, research computing or research network operators can explore ideas atop of an infrastructure designed to be as akin to the major cloud providers to ultimately provide a mechanism to scale into (and out of) any of the major cloud providers.

With its caveats (of which we often discuss) it’s providing a path to rapidly innovate upon possibilities with minimal friction for those that are becoming familiar with industry-leading container orchestration systems.
Nautilus Compute

**General**
- Total GPUs: 543
- Used GPUs: 464
- Requested GPUs %: 85.5%
- Requested utilization: 39.4%
- Total utilization: 33.7%

**Requests**
Number of requested GPUs by namespace.
Nautilus Storage
CHASE-CI Nautilus 593 GPUs Distributed over US Networks--2022

- U SDakota: 9 GPUs over GPN
- UN-L: 16 GPUs over GPN
- UIC: 21 GPUs over MREN
- NYU: 12 GPUs over NYSERNet
- U Delaware: 12 GPUs over NYSERNet
- Clemson U: 21 GPUs over SCLR
- U New Mexico: 4 GPUs via Albuquerque GigaPoP
- FAMU: 8 GPUs over FLR
- UCI + UCR + UCM + UCSC: 99 GPUs over CENIC
- CSUSB + SDSU: 16 GPUs over CENIC
- UCSD: 371 GPUs over CENIC
- U Hawaii: 1 GPU over CENIC/PW
- U Guam: 1 GPU over CENIC/PW
- UC Davis + UCR + UCM + UCSC: 99 GPUs over CENIC
- U New Mexico via Albuquerque GigaPoP: 4 GPUs
- NYU: 12 GPUs over NYSERNet
- U Delaware: 12 GPUs over NYSERNet
- Clemson U: 21 GPUs over SCLR
- U New Mexico: 4 GPUs via Albuquerque GigaPoP
- FAMU: 8 GPUs over FLR
- UCI + UCR + UCM + UCSC: 99 GPUs over CENIC
- CSUSB + SDSU: 16 GPUs over CENIC
- UCSD: 371 GPUs over CENIC
- U Hawaii: 1 GPU over CENIC/PW
- U Guam: 1 GPU over CENIC/PW

Minority Serving Institutions

EPSCoR Institutions

Non-MSI Institutions
4.7 PB Nautilus Ceph Storage Over Networks—2022

UCR + UCSC + UCSB
727 TB over CENIC

UCSD + UCLA
901 TB over CENIC

UCS + Stanford
521 TB over CENIC

SDSU
109 TB over CENIC

NYU + NYSERNet
400 TB over NYSERNet

U Kansas
200 TB over GPN

U Oklahoma
200 TB over GPN

U Arkansas
200 TB over GPN

UIC
175 TB over MREN

UN-L
400 TB over GPN

FAMU + FIU
318 TB over FLR

U Delaware
200 TB over NYSERNet

U Guam
118 TB over CENIC/PW

U Hawaii
266 TB over CENIC/PW

EPSCoR Institutions

Minority Serving Institutions

Non-MSI Institutions

City Pair
State-to-State Pair
Inter-Connect Point

QUILT MEMBERS & AFFILIATES
100G Nautilus Nodes UCSD's IGROK/FIONAs and Internet2's OSG FIONAs--5/25/2022

Nautilus has 202 Nodes: 34@100G, 63@40G, 3@20G and 102@10G

CENIC 100G Ceph Nodes
1. ps-100g-scidmz-0.tools.ucla.net
2. k8s-nvme-01.sdsc.optiputer.net
3. k8s-usra-02.calit2.optiputer.net
4. stashcache.2.ucsd.edu
5. prp01.ifa.hawaii.edu

U Hawaii
100G UCSD FIONA over CENIC/PW

U Guam
100G-capable UCSD FIONA over CENIC/PW

PNWGP
200G IGROK over CENIC/PW

Sunnyvale
200G IGROK over CENIC/PW

LAX
100G I2 FIONA over I2

Sunnyvale OSG
200G IGROK over CENIC/PW

Sunnyvale
100G I2 FIONA over I2

Kansas City OSG
100G I2 FIONA over I2

UCSD
200G IGROK over CENIC/PW

Houston OSG
100G I2 FIONA over I2

AMPATH/FIU
100G UCSD FIONA over FLR

MREN 100G Data Transfer Nodes
1. dtn101.sl.startap.net
2. dtn108.sl.startap.net

StarLight
200G IGROK over CENIC/PW

StarLight OSG
100G I2 FIONA over I2

MANLAN OSG
100G I2 FIONA over I2

NYSERNet 100G Test Node
1. dtnnrp-s1.nysernet.org

GPN 100G Ceph Nodes:
1. fiona.offn.oscer.ou.edu
2. hcc-prp-c1312.unl.edu
3. nautilus1.hpc.uark.edu
4. sdsmt-fiona.sdsmt.edu

CENIC 100G Data Transfer Nodes
1. k8s-nvme-01.ultralight.org
2. 100g.ucsc.edu
3. siderea.ucsc.edu
4. k8s-epyc-01.sdsc.optiputer.net
5. k8s-igrok-01.calit2.optiputer.net
6. k8s-igrok-02.calit2.optiputer.net
7. k8s-igrok-03.calit2.optiputer.net
8. k8s-igrok-04.calit2.optiputer.net
9. k8s-igrok-05.calit2.optiputer.net
10. k8s-igrok-06.calit2.optiputer.net
11. k8s-igrok-07.calit2.optiputer.net

100G I2 FIONA over I2

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:

CENIC 100G Data Transfer Nodes

MREN 100G Data Transfer Nodes

Uawaii

U Guam

PNWGP

Sunnyvale OSG

Sunnyvale

Kansas City OSG

UCSD

AMPATH/FIU

MREN 100G Data Transfer Nodes

StarLight

StarLight OSG

MANLAN OSG

NYSERNet 100G Test Node

GPN 100G Ceph Nodes:
Custom JupyterHub Environments per University

- Rapidly deploy JupyterHub environments with customized environments for each research project, lab, or workshop
- Easily supported within Nautilus cluster on the domain of the university needing the resource
- Provides a less queue/time-limit heavy process for researchers to explore opportunities before migrating to campus research computing resources
- Basis of grant submission today
Jeremy Evert, Ph.D., Associate Professor, Computer Science Southwestern Oklahoma State University:

Having a web-based system greatly lowers the threshold for getting started with programming. It lets students with ChromeBooks and iPads start programming.

... a Jupyter Notebook means that even students with a Raspberry Pi can log-in and run a bigger job in a short time.
Deployed projects

Although you can run your own containers, there are several services and resources already deployed by cluster admins that you can use without creating those yourself.

❗ Most services require additional registration.

Computations

- JupyterHub (West Coast)
- JupyterHub (East Coast)
- WebODM (Web Open Drone Map): Drone Images stitching

Data sharing and collaboration tools

- EtherPad: notebooks
- GitLab: code and containers repository
- Jitsi: Video conferencing
- Nextcloud: File sharing
- Overleaf: LaTeX collaboration
- SyncThing: File sync (Contact us to set up)
- GitPod: shared development environment

Managed deployments for popular services

Network monitoring

- Traceroute tool
- PerfSONAR
Considerations

● Leverage PRP’s concept of “Potluck Supercomputing”
● Don’t lose campus identity! Use your domain name!
● Work around limits of InCommon participation
● Prioritize regional resources with “affinities”
● Reduce or eliminate time-constraints (friction) of other no-cost or commercial solutions
● Leverage a team of support already funded by NSF
● Be able to measure impact
GPN Server Progress

- Virtualized and migrated very dated servers (utilized scarce power needed for new perfSONAR servers)
- Migrated several services into OneNet hosted services and public clouds (DNS, mailing list)
- Establishing reference servers to leverage InCommon Services
- Proof-of-Concept testbed for GP-ARGO configurations
## GPNR perfSONAR Dashboard

<table>
<thead>
<tr>
<th>Network</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARE-ON Fayetteville, AR</td>
<td>Great Plains Network-Kansas City, MO</td>
</tr>
<tr>
<td>KU-Manhattan, KS</td>
<td>KU-Lawrence, KS</td>
</tr>
<tr>
<td>MOREnet-Kansas City, MO</td>
<td>MSU-Bozeman, ScienceDMZ</td>
</tr>
<tr>
<td>OneNet-Tulsa, OK</td>
<td>SDSU-Brookings, SD</td>
</tr>
<tr>
<td>UNL-Lincoln, NE</td>
<td>USD Vermillion Campus Edge</td>
</tr>
<tr>
<td>USD Vermillion Science DMZ</td>
<td>WSU-Wichita, KS</td>
</tr>
</tbody>
</table>

**Overview:**
- **ARE-ON Fayetteville, AR** connects to Kansas City, MO.
- **KU-Manhattan, KS** connects to Lawrence, KS.
- **MOREnet-Kansas City, MO** connects to Bozeman, ScienceDMZ.
- **OneNet-Tulsa, OK** connects to Brookings, SD.
- **UNL-Lincoln, NE** connects to USD Vermillion Campus Edge.
- **USD Vermillion Science DMZ** connects to Wichita, KS.
perfSONAR upgrades
(modeled after I2 Performance Assurance Service)

AgilityEdge Enterprise AMD ROME Server (Dell OEM)

1U Chassis with 10 x 2.5" Hot Plug NVMe Drive Bays
Single AMD 7402P, 24-core, 2.8GHz Processor
128GB of DDR4 3200MHZ ECC/REG Server Memory, (2 x 64GB in 16 DIMM slots)
BOSS Controller Card with 2 x 240GB M.2 Sticks (RAID 1)
1.6TB, NVMe, Mixed Use Express Flash, 2.5 SFF Drive, U.2, P4610 with Carrier C30, No RAID for NVME Chassis
Two 1GbE Ports via LOM Riser
One Broadcom 57416 Dual Port 10GbE SFP+ Network LOM Mezz Card
Mellanox ConnectX-5 Dual Port 40/100GbE QSFP28 Adapter
iDRAC9 Enterprise X5, Remote Access Controller
ReadyRails Sliding Rails Without Cable Management Arm
ReadyRails Static Rails for 2/4-post Racks
Dual, Hot Plug, Redundant Power Supply, 600W -48VDC
Two DC Power Cords for Dual, Hot Plug, Redundant Power Supply (1+1), 600W
Nautilus Ceph Storage Node
improves file access for Nautilus cluster in GPN region, adding 200+ TB in disk per node

AgilityStor 2U AMD Rome Server
Single AMD EPYC ROME 7402P, 24-core, 2.8GHz Processor
256GB DDR4 3200MHz ECC/REG Memory
Two 256GB Samsung 860 Pro SATA SSDs
One 1.6TB Samsung PM1735 HHHL PCIe 4.0 NVMe Card with PLP
Twelve WDC Ultrastar 18TB SAS ENT HDDs
Twelve 3.5" SATA Hot-swap Drive Bays, Two 2.5" SATA Hot-swap Drive Bays and
One Ultra-Fast M.2 with PCIe Gen3 x4 Interface
One Broadcom 9305-16i SAS HBA
Expansion Slots: Three x16 PCIe Gen4 (one populated by 200G adapter), Three x8
PCle Gen3/4 (two populated by SAS HBA and NVMe card) and One OCP 2.0 Gen3
x16 Mezzanine Expansion Slots
One ConnectX-6 Dx 200GbE Single-port QSFP28, Network Adapter
Two 1Gb/s LAN Ports (Intel I350-AM2)
One Dedicated Management Port
Aspeed AST2500 Remote Management Controller
One TPM 2.0 Module
Rail Kit
800W 80 PLUS Platinum Redundant Power Supply
Bandwidth Dashboard

The map shows the minimum, maximum, and average bandwidth utilization of the circuits and exchange points over the selected time period. The rows below the map show each of the links in more detail, including traffic rate and total volume transferred. A combined view of the average and maximum bandwidth utilization is shown at the bottom of the page. All times are displayed in browser local time.

Single Link Max A-Z
38.4 Gb/s

Single Link Max Z-A
56.3 Gb/s

Average Across All Links
9.56 Gb/s

Total Transferred
1.449 PB
<table>
<thead>
<tr>
<th>Org</th>
<th>Resource Name</th>
<th>CIDR</th>
<th>Organization</th>
<th>Discipline</th>
<th>Role</th>
<th>Country</th>
<th>Lat, Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>UN</td>
<td>UNL - Arvil Cloud</td>
<td>129.93.175.0/26</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Multiple</td>
<td>United States</td>
<td>41.2474, -96.0178</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - CMS Tier 2 Center - DTN and support nodes</td>
<td>129.93.239.128/26, 2600:9000:0:1101::/64</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>MPS.Physics.High Energy</td>
<td>Cluster</td>
<td>United States</td>
<td>40.8130, -96.7029</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - CMS Tier 2 Center - worker nodes</td>
<td>129.93.182.0/23, 2600:9000:0:1102::/64</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>MPS.Physics.High Energy</td>
<td>Compute</td>
<td>United States</td>
<td>40.8130, -96.7029</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - Crane HPC Cluster</td>
<td>129.93.227.64/26</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Cluster</td>
<td>United States</td>
<td>41.2474, -96.0178</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - HCC FIONA DTN</td>
<td>129.93.241.1/32, 2600:9000:0:1302::7ac:0b0a7/128</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Data Transfer</td>
<td>United States</td>
<td>40.8000, -96.6670</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - HCC IPv6 Resources</td>
<td>2600:9000:0:48</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Multiple</td>
<td>United States</td>
<td>40.8130, -96.7029</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - HCC Resources in Lincoln, NE</td>
<td>129.93.244.192/26, 2600:9000:0:1301::/64</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Cluster</td>
<td>United States</td>
<td>40.8000, -96.6670</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - perfSONAR</td>
<td>129.93.5.165/32, 2600:9000:8:392e:2baff:fe2b9050/128</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>CS.Network Testing and Monitoring</td>
<td>Network Testing</td>
<td>United States</td>
<td>40.8219, -96.6076</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - perfSONAR - HCC - bandwidth</td>
<td>129.93.183.249/32, 2600:9000:0:110:7a2bcbf5fe68a68c/128</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>CS.Network Testing and Monitoring</td>
<td>Network Testing</td>
<td>United States</td>
<td>40.8130, -96.7029</td>
</tr>
<tr>
<td>UN</td>
<td>UNL - Rhino HPC Cluster</td>
<td>129.93.241.16/28</td>
<td>University of Nebraska-Lincoln (UNL)</td>
<td>Multi-Science Facility</td>
<td>Cluster</td>
<td>United States</td>
<td>40.8221, -96.6980</td>
</tr>
</tbody>
</table>

11 records found
Social Network Analysis of Awards

- Reviewing data from NSF and NIH currently
- Text analysis to increase focus on projects with potential greater amounts of data movement
- Color of dots represent the state the PI or co-PI resides
- Lines represent common NSF awards between PIs, thickness represents number of awards between PIs
- As familiarity with the graphs grow, can visually identify interesting inter-institutional and/or interstate collaborations facilitating engagement opportunities
Social Network Analysis of Awards

Connecting network data such as ASNs to the institutions to help engage networkers

Interesting discoveries:
- Challenges of mapping co-PIs to their institutions and the networks that serve them
- Successfully identifying great collaborators

Developed and deployed initially in PRP’s Kubernetes environment now it is also in GPN’s
GlobalNOC Augmented Traceroute Report

Encouraged GlobalNOC Project

- Numerous networks already work with GlobalNOC
- Simplify sharing of metrics collected
- Simplify visualizing the metrics along the paths

KINBER
CEN
OSHEAN
OneNet
GPN
MCNC
NWAVE
Internet2, MANLAN, WIX
CAAREN
AREON
SOX
I-light
Indiana Gigapop
BTAA
Indiana University + its regional campuses
TransPAC
NEAAR
Ongoing & Upcoming

- Submitting CC* Regional Computing Proposal today!
- Routing Security (ROAs and RPKI)
- Greater InCommon adoption
- Weekly Research Platform discussions (Most Mondays at 11am)
- Great Plains Cyber Team engagements
- Continue collaboration with EPOC
- PEARC2022
- Exploring new opportunities working with FABRIC
Thank You

James Deaton
jed@greatplains.net
NTNC History
The NTNC was formed in 2003 by primarily representatives from Internet2 universities in the states of Washington, Idaho, Montana, North Dakota, South Dakota, Minnesota, and Wisconsin. The initial impetus was to pursue the development of a next generation network across a region that is currently served only by Internet2 infrastructure at the end points of Seattle and Chicago.

Source: Northern Tier Networking Development Planning Grant Proposal by Bonnie Neas, North Dakota State University and Ray Ford, University of Montana
Northern Tier Network (Virtual) 2005

Source NSF NT proposal 3/17/05
Simplified Timeline

- **ARPANET**
- **NSFNET**
  - National Science Foundation funds network backbone that connects research universities and national labs. (1985–1995)
- **Internet2**
  - National research and education network becomes member funded. Connects research universities and national laboratories.
- **NTNC**
  - NTNC formed circa 2003
  - NTNC planning grant from NSF circa 2005
- **US UCAN**
  - US UCAN Proposal from Internet2. Lots of engagement with NTNC members.
- **TCUs**
  - Purposely engagement with tribal colleges and universities
- **Everything Stops (COVID)**

Years:
- 1985
- 1990
- 1995
- 2000
- 2005
- 2010
- 2015
- 2020
- 2025
REGIONAL RESEARCH & EDUCATION NETWORKS IN THE UNITED STATES

QUILT MEMBERS & AFFILIATES

THE QUILT
Circa 2003
Circa 2003 w/ future points shown
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 31-February 1, 2019</td>
<td>Minneapolis, Minnesota</td>
<td>February 17-18, 2016</td>
<td>Iowa City, Iowa</td>
</tr>
<tr>
<td>February 1, 2019</td>
<td>Big Sky, Montana</td>
<td>February 17-18, 2016</td>
<td>Iowa City, Iowa</td>
</tr>
<tr>
<td>March 16, 2021</td>
<td>Chicago, Illinois</td>
<td>May 16-17, 2012</td>
<td>Anchorage, Alaska</td>
</tr>
<tr>
<td>December 5-6, 2017</td>
<td>Washington, DC</td>
<td>January 29-31, 2012</td>
<td>Bozeman, Montana</td>
</tr>
<tr>
<td>December 14, 2020</td>
<td>University of Montana</td>
<td>January 26-27, 2015</td>
<td>Deadwood, South Dakota</td>
</tr>
<tr>
<td>June 10-12, 2019</td>
<td>The Oxford Hotel</td>
<td>January 31-February 1, 2011</td>
<td>Omaha, Nebraska</td>
</tr>
<tr>
<td>July 10-12, 2019</td>
<td>Fargo, North Dakota</td>
<td>June 3-4, 2010</td>
<td>Missoula, Montana</td>
</tr>
</tbody>
</table>