ISSUE
08
November
2016

N-Wave News

NOAA N-Wave

N-Wave is a program and Enterprise Network that supports both operations and research, enabling NOAA's mission of science, stewardship and service through highly available, secure, high speed networking services.

Mission

N-Wave is committed to providing innovative networking capabilities with integrity, transparency, and flexibility, to enable NOAA's missions through the implementaton of:

- Quality, advanced high-speed connectivity both internally and externally to NOAA.
- Secure, private, flexible, hight-bandwith virtual circuit capabilities.
- Retention and recruitment of exceptional operations and engineering staff.

Our Vision

To provide a reliable, secure, and sustainable network resource for NOAA, which enables NOAA's mission of science, stewardship and service.

NOAA ENTERPRISE NETWORK

this issue

From the N-Wave Network Manager

As we close out the 2016 fiscal year, one word embodies the projects, efforts, and accomplishments this past year: partnerships. A hard drive to deliver all remaining Trusted Internet Connection (TIC) infrastructures was made possible through the solid relationship between N-Wave and the NOAA Cyber Security Center (NCSC). Acting NCSC Director Robert Hembrook provided N-Wave the support of his NCSC teams, [administrative and engineering] which ensured infrastructure and security services interoperability. Furthermore, TIC project manager Chi Kang brought together and led N-Wave team members, most notably John V. Parker and NCCS team members, for an outstanding performance on the Department of Homeland Security TIC audit and assessment which directly benefits the operational readiness, compliance and availability of TIC services. I greatly appreciate the talented staff across N-Wave and NCSC and the professional, collaborative partnership within the NOAA OCIO.

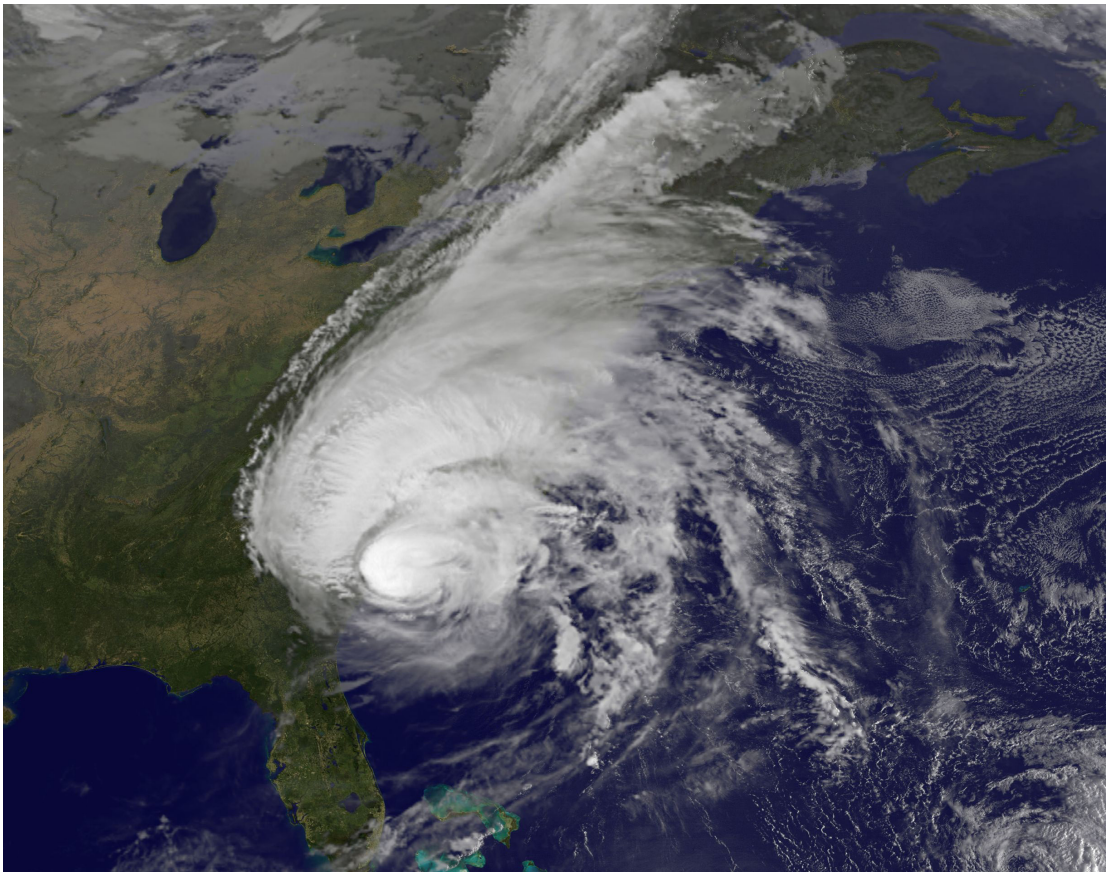
On October 12, 2016, the Indiana University Global Network Operations Center (GlobalNOC) hosted the NOAA CIO for a day of discussions covering High Performance Computing, International Science networks, and the wide range of network operations services provided to N-Wave. From right to left N-Wave program Manager Robert Sears and NOAA CIO Zach Goldstein present a plaque of appreciation for the GlobalNOC to Indiana University Vice President for IT and CIO Brad Wheeler.

From the N-Wave Network Manager - Cont.

From a TIC networking perspective, entire new infrastructures have been established NOAA-wide (Hawaii, Seattle, Denver, Dallas, DC Metro). This not only assists in TIC compliance but also delivers new highly available, reliable, high-speed transport services. A much-deserved thank you goes out to Jason Iannone, N-Wave engineer at the Indiana University GlobalNOC, who has done extensive work putting design to deployment for the X-Wave TICAP infrastructure. The interoperability of X-Wave, the TIC security service enclave, and N-Wave internal TIC aggregation points is a major engineering effort ensuring the most availability and enabling NOAA's mission.

Rounding out the TIC sites and services is NOAA's critical partnerships with Regional Optical Networks (RON) and the GlobalNOC. Leveraging the unique scientific, research, and education network infrastructures of the University of Hawaii, Pacific Northwest Gigapop in Seattle WA, Front Range GigaPop Boulder, (FRGP) CO, Lonestar Education And Research Network (LEARN) Dallas, TX, and the University of Maryland Mid-Atlantic Crossroads (MAX) in College Park MD, has allowed N-Wave to deploy the highly available TIC sites with increased Internet, Research and Science Network capacity along with innovative ways to peer with cloud providers and other provider services at a cost savings to NOAA. Operationalizing all these elements is the GlobalNOC, bringing the same outstanding customer service, and 24x7x365 network operations with unique, advanced tool sets for monitoring the health of these new infrastructures.

True partnerships are key to supporting NOAA's Mission Goals and Strategic Plan, whether it's via research with Cooperative Institutes or purposefully built scientific, research and education network infrastructures: all of these enable a community of excellence.



This image of Hurricane Matthew along the southeastern U.S. coast was taken by NOAA's GOES-East satellite on Oct. 8, 2016, at 7:45 a.m. EDT. Credit: NASA/NOAA GOES Project.

Update on NOAA's TICAPs and X-Wave

Since the last update in Spring of 2016, we completed the Denver and DC TICAPs; and now all five NOAA TICAP infrastructures are complete. X-Wave deployment is occurring while we prepare to move the entire agency toward TICAP 2.0 compliance. With all infrastructures up, the next two phases are underway: migrating NOAA campuses and sites to "bypass mode" in the new infrastructure for network stabilization and continued access to commodity Internet and R&E networks. The final phase is the migration to full inline TIC services. Hawaii is 100 percent complete, Seattle has completed network migration, and the Denver, Dallas, and DC metro are underway with network migration.

A quick refresher: X-Wave is a new NOAA network outside of the TICAP 2.0 security stack, for landing external partner connections and Internet Service Providers. It will provide an essential function of routing traffic in and out of the agency while preserving symmetry through the TICAP 2.0 firewalls. N-Wave will continue to function as the agency's intranet, routing traffic between NOAA participants while also routing NOAA to a TICAP when external connectivity is needed to reach non-NOAA sites.

In DC, the X-Wave connectivity has been fully tested and is passing actual NOAA traffic. The Geophysical Fluid Dynamics Laboritory (GFDL) in Princeton, NJ. was the first to transition to the new X-Wave infrastructure. GFDL uses X-Wave extensively since it moves large amounts of data to and from Oak Ridge National Laboratory which is outside the NOAA TIC boundary. Following GFDL will be other Eastern U.S. N-Wave participants, such as NCEI-NC, NOS and NWS. The Silver Spring, MD. area sites and OneNWSnet will transition by the end of this calendar year.

The Denver, CO. TICAP has been deployed across two different locations in downtown Denver. Boulder, CO. and central and mountain region participants will transition to X-Wave by the end of 2016.

After traffic has been transitioned to X-Wave, NOAA Cyber Security will begin implementing TICAP 2.0 services on to the traffic flowing in and out of the agency via X-Wave, including IDP, firewall, web content filtering, and monitoring.

Next, the N-Wave team and the NOAA Cyber Security Center will be planning for capacity augmentation and hardware refresh. The current TICAP security stack can function at 20 Gbps. Current projections show that NOAA requirements to the Internet (via X-Wave) will soon exceed that capacity. Fortunately, the installed hardware in the TICAP stack is capable of higher rates through the addition of more interfaces.

X-Wave and TICAP 2.0 represent an entirely new way for NOAA to interface with the public; it represents the largest change the agency has experienced since getting "on board" the Internet in the 1980s. As NOAA continues to provide data to the public and external partners, we must continue to plan and grow this essential capability to meet NOAA's important mission.

N-Wave Network and Performance Metrics

Welcome to the Fall 2016 edition of the network performance metrics discussion. As Figure 1 illustrates, N-Wave traffic levels slightly decreased after our last report (Jan 2016), but continue to average around 5-6 Petabytes per month.

The Research and Development High Performance Computing System (RDHPCS) and the Weather and Climate Operational Supercomputing System (WCOSS) continue to be high-volume users of the N-Wave network.

Oak Ridge National Labs (ORNL) provides computing cycles for the RDHPCS program, and large volumes of data are typically moved from ORNL to Fairmont and Princeton, NJ (GFDL). WCOSS continues to move large amounts of data from Reston, VA. and Orlando, FL. to the archive in Fairmont, WV. As shown in Figure 2.

N-Wave uses two methods for collecting network utilization information: Simple Network Management Protocols (SNMP) and IPFIX. SNMP [1] is a decades-old protocol that provides remote gathering and collection of router metrics such as "bytes transmitted per interface". IPFIX [2] looks deeper into traffic than SNMP and collects IP flow data as packets traverse our routers.

In addition to IPFIX traffic monitoring on routers, N-Wave is testing Juniper's WANDL IP/MPLSView software product. This application will allow us to go beyond monitoring the network with IPFIX or SNMP methods and expand into traffic management, engineering and capacity planning. For example, with WANDL, N-Wave can model network scenarios based on user data flow requirements, to ensure that there is adequate failover network capacity during a backbone circuit outage. WANDL will then suggest traffic engineering scenarios, such as either adding capacity or constraint-based routing of user traffic across the backbone, instead of simply using the shortest paths.

The N-Wave team is currently studying options for increasing capacity over the wide-area backbone. Today, the backbone utilizes 10 Gbps links between the four CONUS core nodes. Options for increasing capacity include multiple 10 Gbps links, as well as 40 or 100 Gbps links. These upgrades, as well as new routing technologies, will meet the growing demand of NOAA's networking needs for the next few years, and they will enable new services, such as Traffic Engineering and Software Defined Networking to N-Wave.

[1] https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
[2] IPFIX (IP Flow Information Export): see https://en.wikipedia.org/wiki/IP_Flow_Information_Export

N-Wave Traffic Levels

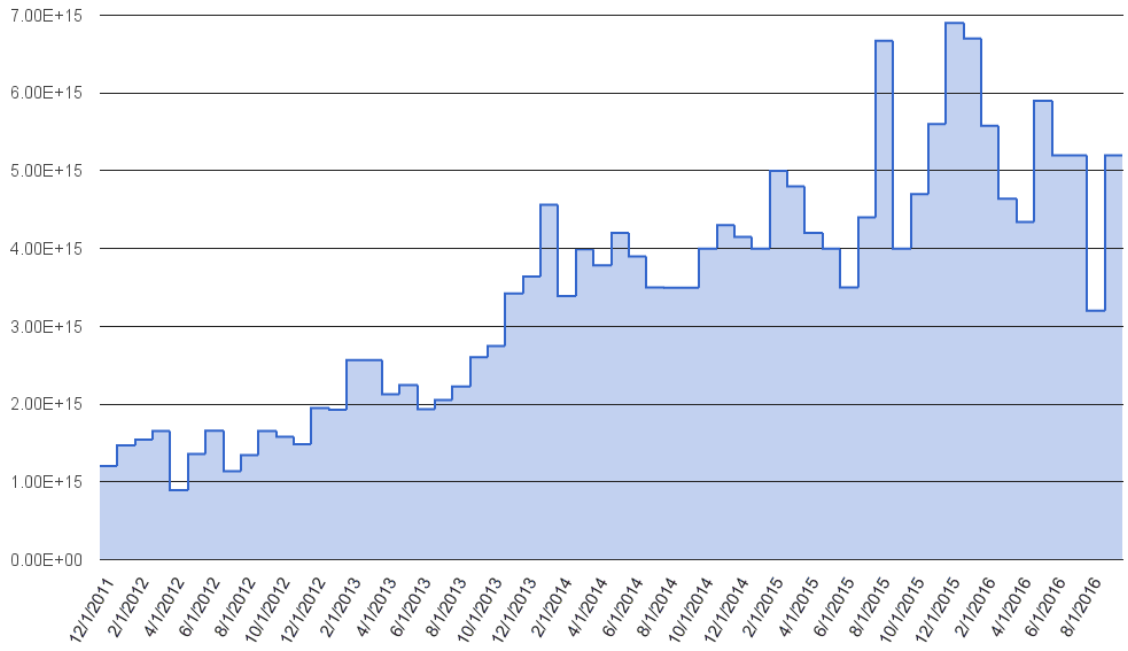
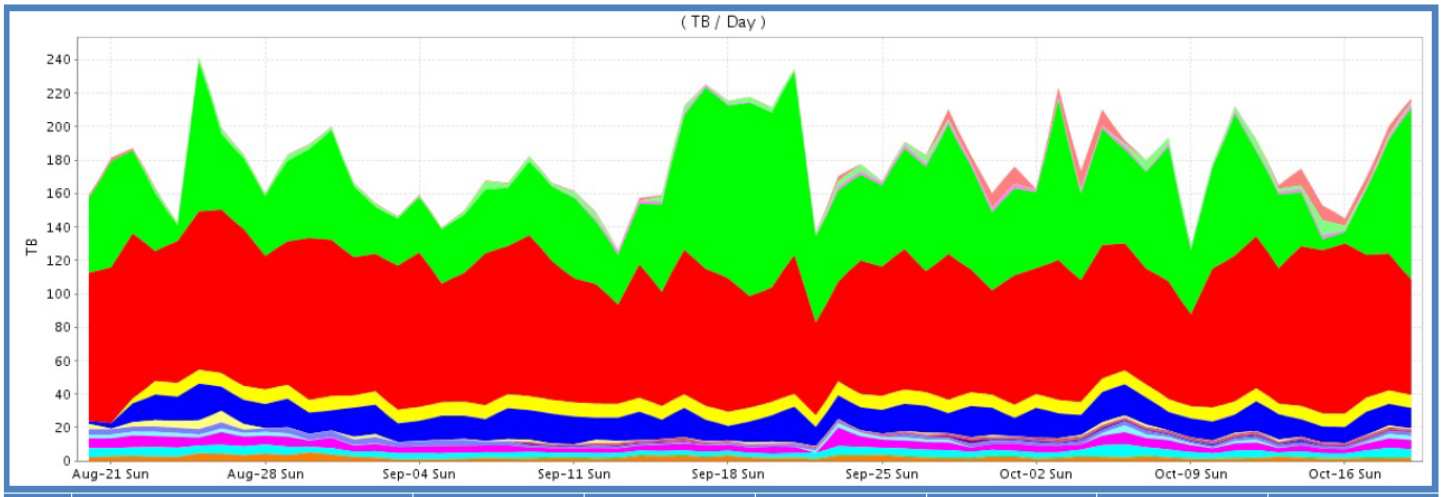


Figure 1: N-Wave total bytes transferred, by month. For reference, 5.00E+15 is equal to 5 Petabytes.

NOAA's GOES-R Satellite, due to launch in November 2016. N-Wave provides network connectivity to the GOES-R ground system. Credit: NASA/NOAA.

Volumes of Data Moving to Archives in Fairmont



No.	Destination CostCentre	TB sum	TB %	TB avg	TB max	G.Pkts sum	K.Flows sum
1	RDHPCS-FAIR	4,938.930	45.37%	80.966	101.783	620.590	6,629.165
2	RDHPCS-GFDL	3,326.692	30.56%	54.536	115.672	397.491	3,873.569
3	RDHPCS-BOULDER	855.198	7.86%	14.020	21.937	225.585	4,352.534
4	RDHPCS-CLPK	469.539	4.31%	7.697	8.667	60.359	61.828
5	CLASS-BOUL	271.154	2.49%	4.445	11.053	188.458	3,656.927
6	CLASS-ASHE	239.546	2.20%	3.927	7.596	171.317	3,567.439
7	Asheville	136.708	1.26%	2.241	5.105	211.180	25,116.597
8	WCOSS-RESTON	125.984	1.16%	2.065	10.863	101.467	4,307.151
9	WCOSS-ORLANDO	120.585	1.11%	1.977	8.957	75.040	3,655.249
10	Default	116.477	1.07%	1.909	3.803	134.723	10,484.825
11	ORNL	61.494	0.56%	1.008	6.857	141.398	2,955.527
12	STAR CLPK	60.087	0.55%	0.985	2.480	42.605	1,875.360
13	CLASS-SUIT	56.038	0.51%	0.919	4.148	68.282	4,055.937
14	GOES-R RBU	23.825	0.22%	0.391	0.870	33.100	1,606.892
15	GOES-R NSOF	23.719	0.22%	0.389	2.136	34.556	1,116.082
16	GOES-R WCDAS	22.470	0.21%	0.368	1.039	43.192	2,778.061
17	AWIPS	21.375	0.20%	0.350	0.628	16.548	3,778.018
18	GFDL	14.320	0.13%	0.235	1.478	10.701	1,352.880
19	ESPDS	2.193	0.02%	0.036	0.069	14.706	2,029.284
20	GOES-R HTEN	0.000	0.00%	0.000	0.000	0.000	0.001
	Total (20)	10,886.334	100.01%	178.464	241.541	2,591.298	87,253.326

Figure 2: N-Wave total daily bytes transferred, by project or program to archives in Fairmont. From August 22, to October 22, 2016.

Update on the Network Operation Center Integration Project

N-Wave NOC is partnering with other NOAA NOCs to create a single, integrated NOAA-wide NOC. The Integrated NOC (INOC) will function as a single point of contact for Tier 1 support. The expansion into the INOC will continue or expand the N-Wave NOC's 24x7x365 staffing model to the other NOCs and extend its active network monitoring, toolsets and measurement, Tier 1-3 support, and Change Management.

By working with other NOAA NOC operations and management teams, the N-Wave NOC has created a structured triage, response, and resolution plan of action for the various types of requests, scheduled maintenance, and unexpected outage network events. This procedural approach has allowed the INOC to provide custom support based on the specific requirements of each respective NOC, while maintaining a transparent and consistent customer facing resource for contact.

As of July, 2016, INOC has successfully moved into production status as the Tier 1 support for Boulder NOC. Incoming customer requests and reported issues are now being routed to the INOC Service Desk for triage and assignment to the Boulder NOC Engineering team for completion. Scheduled operations status calls with Boulder NOC engineering and operations have maintained open lines of communication and have increased the quality and accuracy of event processing as the INOC continues to make improvements to support procedures. The N-Wave NOC is currently working with the Silver Spring NOC through regularly scheduled operations conference calls and collaboration on support documents to develop the required procedures for integration with the INOC. Silver Spring NOC integration is expected to be completed mid-to-late November 2016.

The N-Wave Network Operations Center, Integrated Network Operation Center is available 24 hours a day, 365 days a year at 812-856-7477 and nwave-noc@noaa.gov.

Use this form to report a problem.

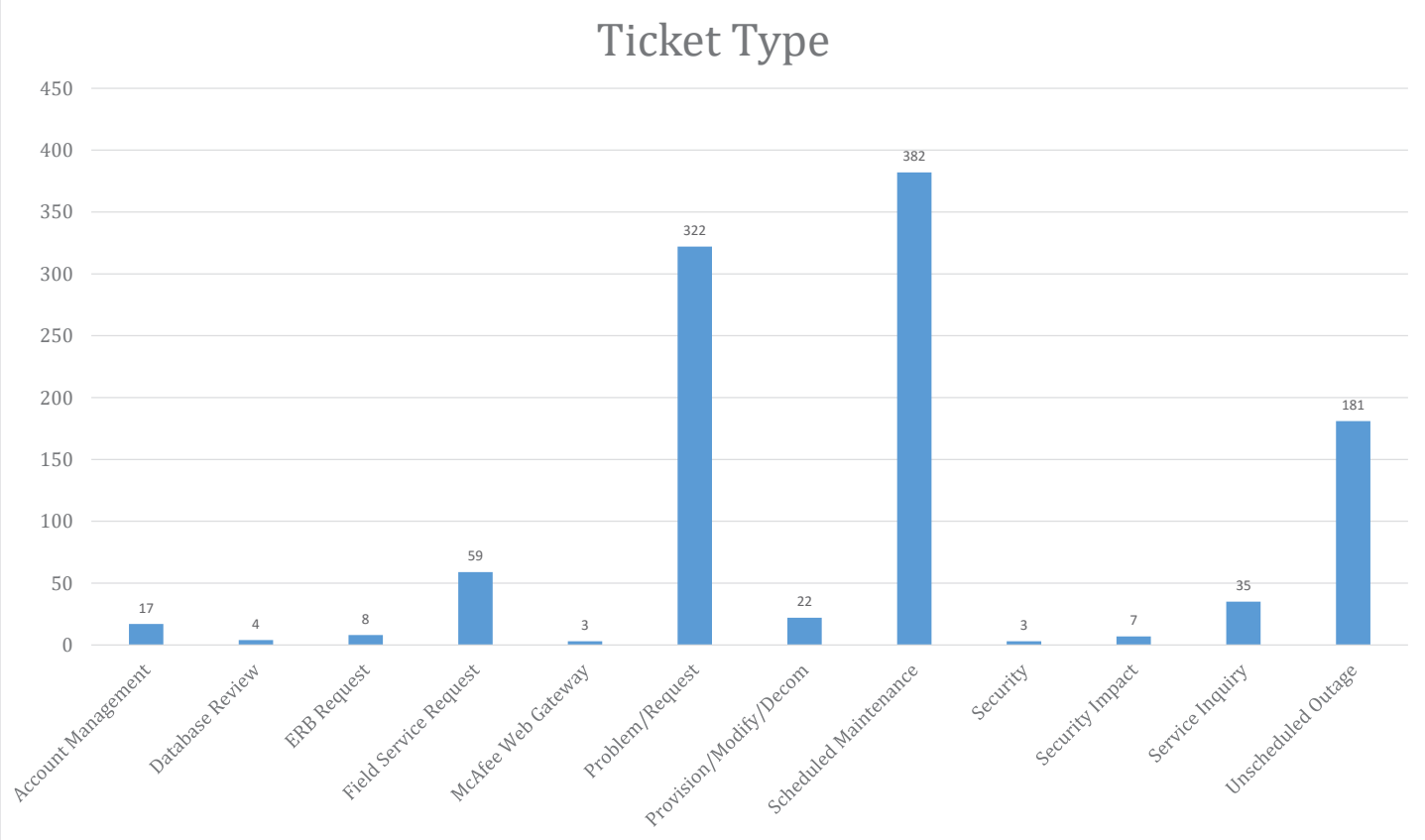
N-Wave NOC (GlobalNOC)

N-Wave NOC Tickets Report
March – August 2016

The N-Wave ticket report tracks the various ticket types used to support the N-Wave network. In this issue, we discuss one ticket type and its associated workflows: The McAfee Web Gateway Request Ticket.
N-Wave NOC works in cooperation with one NOAA Cyber Security Center to support the McAfee Web Gateways as one security component for NOAA-wide Trusted Internet Connections (TIC). McAfee Web Gateway blocks websites for two reasons, either malicious content or malware.

If a user attempts to access a website that has been blocked due to pre-determined content categories, they will receive a notification via a splash page. This splash page will describe the content and details of the block.

If a user suspects a website has been blocked in error, they can submit a re-categorization request. The user will be instructed, on the block splash page, to email nwave-noc@noaa.gov and attach a screenshot of the blocked page. The NOC will then create a McAfee Web Gateway Request ticket, attach the email details with the user contact info and screenshot, and assign it to NOAA Cyber Security for assessment. After the response from NOAA Cyber security, the NOC will contact the user with the update or resolution, and then close the request ticket as resolved.



NOAA-wide Network Performance Testing

Quite frequently, performance problems arise during the day-to-day operations of most wide- and local-area networks. These problems can be tough to pin down: sometimes they are related to circuit issues, other times they are application layer related. Firewalls and high-latency networks also cause problems that may require the tuning of either the firewall settings or end-host operating system.

To help identify and repair these problems, periodic network throughput and latency testing can provide a baseline of nominal network performance. This baseline is a reference for what the network can normally achieve in terms of end-to-end or segment-to-segment throughput. This information can help us isolate and diagnose problems and establish available levels of network performance.

The high-performance research and engineering network community has developed a suite of tools for measuring, recording, and displaying network performance. This suite, called perfSONAR, is free, open-source, and available to run on a Linux-based operating system or used from a bootable CD or USB stick. Development of perfSONAR started more than a decade ago and has involved many in the international research and educational networking community. Current development is being done by Internet2, GÉANT, Indiana University and the Department of Energy's Energy Sciences Network. More information is available on the perfSONAR website. [1]

PerfSONAR uses common UNIX tools, such as IPerf (for throughput testing with UDP and TCP), packet latency testing and scheduling/recording tools. The perfSONAR installation provides the system administrator with a web-based front-end for scheduling and setup of testing.

N-Wave has used perfSONAR since commissioning several years ago. PerfSONAR nodes live alongside all of the N-Wave core routers and on all edge routers. Mesh testing is set up to run hourly with throughput performance and latency measurements recorded and graphed for later inspection.

Currently, the N-Wave deployment is limited to only test to and from other N-Wave perfSONAR nodes. As the N-Wave team looks toward next-generation networking speeds beyond 10Gbps, we are planning on deploying a next-generation perfSONAR mesh that will not be limited to testing with only other N-Wave perfSONAR nodes. Other NOAA users will be able to test to N-Wave perfSONAR nodes on an ad-hoc or on a periodic, scheduled basis. Even non-NOAA users will be able to test, assuming security approval.

We would like to see other NOAA entities adopt perfSONAR and deploy test nodes throughout their networks or end systems. This will help reduce troubleshooting times across organizational and network boundaries.

If your program has any thoughts or interest in participating in a NOAA-wide perfSONAR deployment, please contact Robert Sears robert.sears@noaa.gov or David Hartzell david.hartzell@noaa.gov. We welcome collaborations that can benefit the whole agency.

1 http://www.perfsonar.net

Network Changes & New Participants

N-Wave engineers have completed the physical installations of all five NOAA Trusted Internet Connection Access Point (TICAP) infrastructures. The five TICAP locations—Hawaii, Seattle, Dallas, Denver and Washington DC—will allow NOAA to meet the OMB TIC 2.0 memorandum. There are three main phases in the overall project: installation of the infrastructures for networking and security services; campus and site network migration to the new infrastructures; and inline user (e.g., campus, sites, programs) migration with Inline TIC security components. The Hawaii TICAP is the first with all phases completed. The Seattle site has completed network migrations and is scheduled to complete in-line migration now through the end of FY17 Q2. DC has started migration, with Denver to follow. By FY17 Q3 network and inline migration will be completed across all TICAPs.

N-Wave recently worked with the National Ocean Service (NOS) to bring online a proof-of-concept VPN network to the Microsoft Azure Cloud Computing Platform. We are currently working on a similar proof-of-concept network to the Amazon Web Services cloud.

N-Wave has successfully completed core router hardware refreshes at two of the five core routing facilities. With this upgrade, NOAA will realize significant savings through lower operation and maintenance costs. The remaining core routers in Denver, Chicago, and Seattle are scheduled to be upgraded of FY17 Q1-Q2.

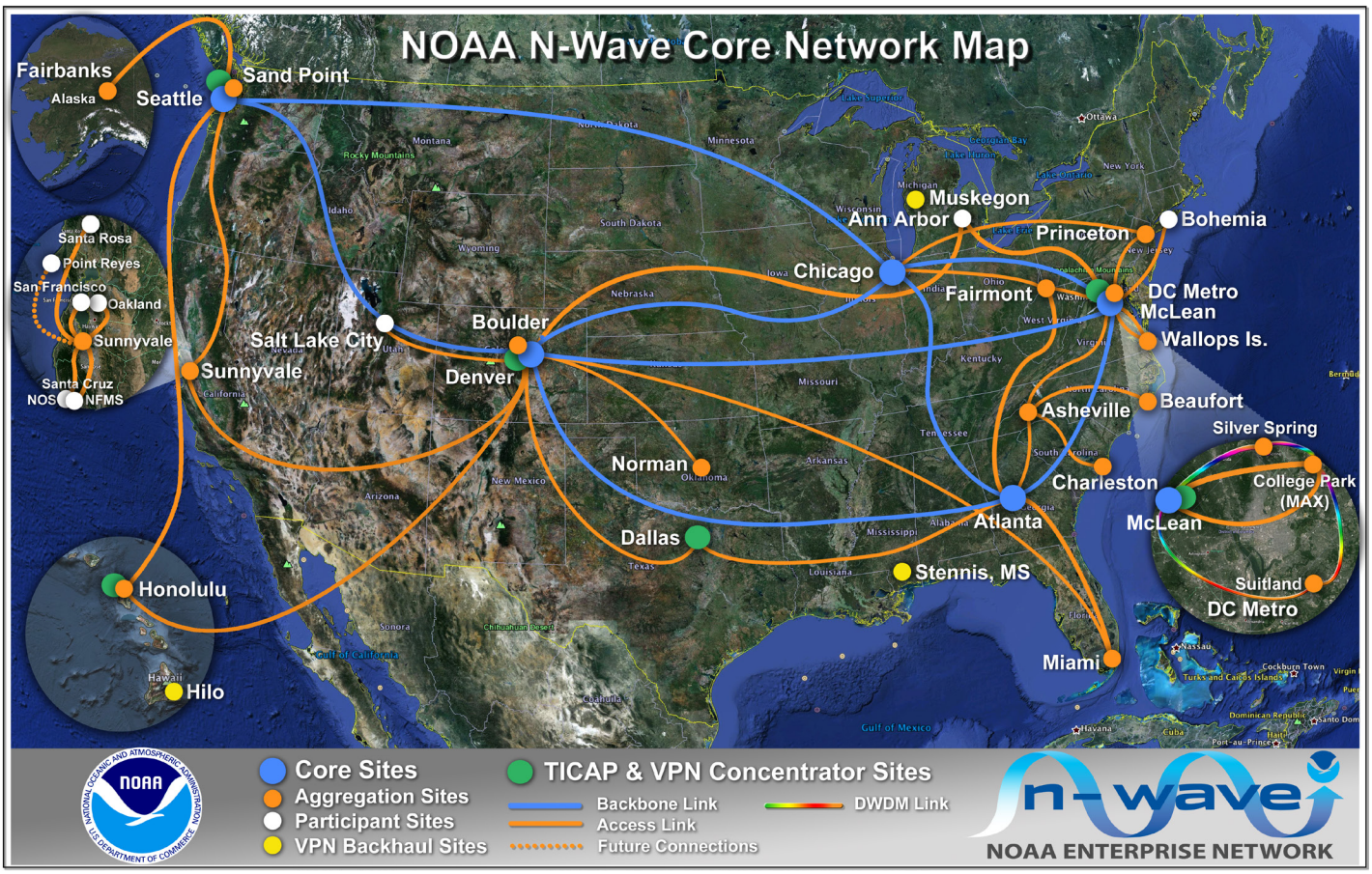
Five participant sites have been added in California, all connected to the N-Wave aggregation site put in earlier this year in Sunnyvale. One site is for NMFS in Santa Cruz, and the other four are for NOS in Santa Rosa, Oakland, San Francisco, and Santa Cruz.

WCDAS (Wallops Command and Data Acquisition System) at Wallops Island, VA, has migrated its Administrative LAN to N-Wave from its legacy commercial point-to-point DS3 circuit. The goal of the migration is to provide the Wallops facility with connectivity to various NOAA Enterprise systems (such as ECHMO, ArchSight, Secure Active Directory and others) that the NOAA CIO office is starting to provide at the enterprise level.

NESDIS has completed its initial roll-out of the WAN connectivity needed for the NESDIS Admin LAN implementation. In August, N-Wave provisioned connectivity for the final NESDIS Admin LAN site at STAR located on the NCWCP campus in College Park, MD.

An N-Wave Private VRF for sending data from DSCOVR (Deep Space Climate Observatory) at Fairbanks, AK. to SWPC (Space Weather Prediction Center) has been extended to include the WCDAS and NSOF sites, allowing those sites to communicate with both the SWPC primary processing site at Boulder, CO and the SWPC alternate processing site at College Park, MD.

NESDIS OSPO (Office of Satellite and Products Operation) has successfully migrated their legacy, low-bandwidth point-to-point T1 circuits for its legacy GOES satellite ground system between WCDAS (Wallops Island, VA) and NSOF (Suitland, MD) to N-Wave. The new N-Wave circuits provide OSPO with high-bandwidth throughput for their site-to-site communications at significant cost savings for the program. In the coming months, N-Wave and OSPO will complete the migration of their T1 circuits between Fairbanks, AK. and Suitland, MD. providing the program significant cost savings.



David Skaggs Research Center (DSRC), in Boulder, CO
Credit: Will von Dauster

Pilot Projects with Commercial Cloud Services

Commercial cloud offerings from companies like Amazon and Microsoft can offer compelling savings over in-house resources as well as with technology benefits for government agencies interested in moving applications and software development into the cloud. Extending any institution's infrastructure into the cloud requires careful planning to connect local resources to those being sent to this "hardware that lives somewhere else."

While generalized Internet connectivity can provide access into Amazon's AWS or Microsoft's Azure, there are many circumstances when a managed, encrypted tunnel, such as a Virtual Private Network (VPN), over the Internet is beneficial. Establishing this secure path could protect management traffic, sensitive data, end user traffic, or private business partner connectivity. Most providers of cloud or network services have established methods for this type of customer connectivity.

N-Wave is working on building TICAP-adjacent VPN services that will provide this connectivity as a generalized service for N-Wave customers. We have done a great deal of testing to ensure that route-based IPSec tunneling to cloud providers is seamless and reliable. These tunnels must support very high-speed encrypted connections over the Internet (in speeds up to 10 Gbps) and be able to scale. We will leverage advanced routing capabilities in order to integrate with the X-Wave architecture to accommodate shortest-path routing and redundancy/failover.

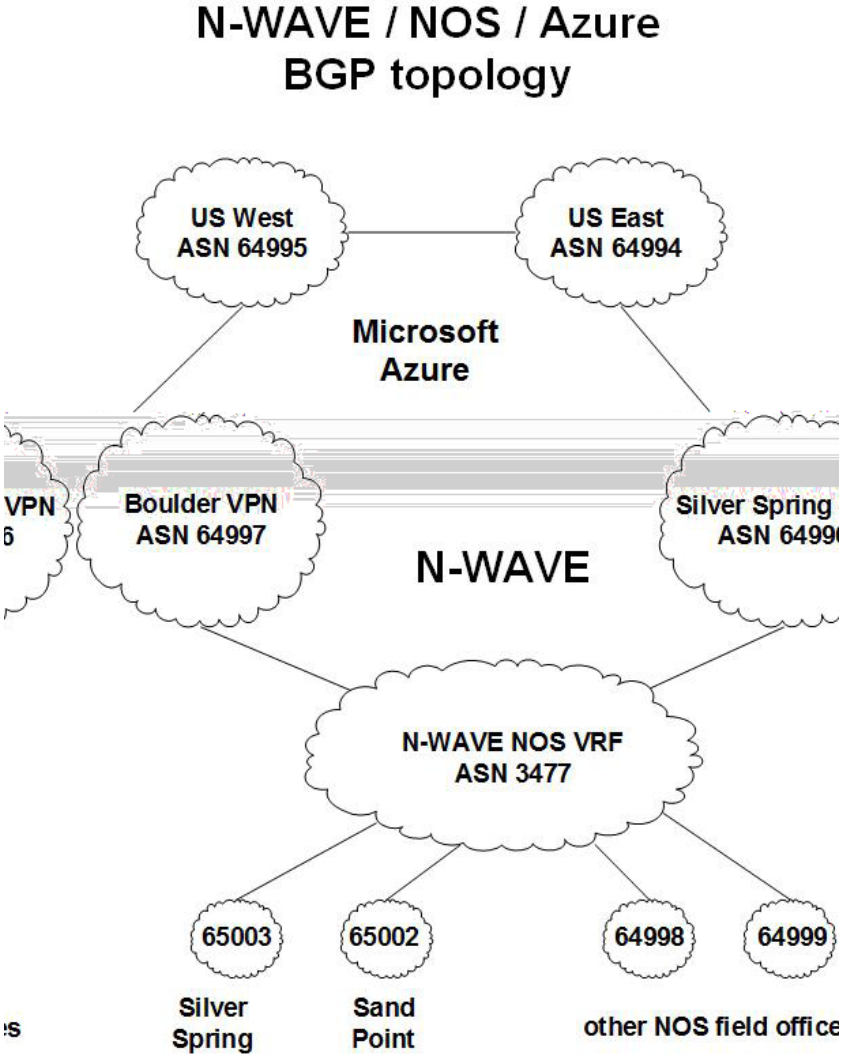
We are exploring the potential uses for this technology with two exercises. The first is a pair of pilot connections to Microsoft's Azure, being used by NOS for data center and private network extension. The second is a single testbed connection to CenturyLink for the Department of Homeland Security (DHS)-mandated Einstein DNS and mail inspection services. Small, limited scale hardware is being used for these projects that scales to an aggregate 200Mbps. Additionally, testing has begun with OCIO to explore connecting N-Wave to the Amazon Web Services (AWS) cloud.

NOS Pilot with Azure

NOS has a requirement to extend the NOS private network within N-Wave to Azure, with whom they had already chosen to partner. This data center extension does not require internet access from Azure and is confined to private IP addressing (addresses that cannot be "seen" in the Internet at large). As part of their requirements, NOS planned to build virtual machines in both the Azure US-West and US-East regions.

To meet their requirements, N-Wave deployed a pair of virtual routers on in-house Juniper SRX240 VPN devices in Boulder, CO. and Silver Spring, MD. Each SRX240 has a single route-based IPSec tunnel to an Azure region: from Silver Spring, MD. to US-East, and from Boulder, CO. to US-West. After setting up IPSec tunnels to the Azure interface, private autonomous system numbers (ASN) were assigned to the SRXs and Azure virtual networks, and the Internet's standard routing protocol, BGP, provided shortest-path routing based primarily on ASN path length. Within Azure, US-East and US-West have connectivity, but NOS is billed for this bandwidth so the preferred path is through N-Wave.

These pilot solutions provides secure, highly-available connectivity from N-Wave to Azure. In the event of device or circuit failure, the solution fails over transparently without user intervention. This solution is providing VPN services, not firewalling. Currently Azure provides these services at security-group and virtual machine level. In working with Azure, we learned that their user interfaces to these services are difficult to understand and use. One future benefit would be having a virtual firewall/VPN device in the Azure cloud that would be managed by N-Wave and provide visibility into both networks' protocols and session state. This would


N-WAVE / NOS / Azure
BGP topology
US West
ASN 64995
US East
ASN 64994
Microsoft
Azure
VPN
6
Boulder VPN
ASN 64997
Silver Spring
ASN 6499
N-WAVE
N-WAVE NOS VRF
ASN 3477
65003
65002
64998
64999
Silver
Spring
Sand
Point
other NOS field office
s

be highly beneficial for operational assurance and design flexibility. The OCIO-based testing that has begun with Amazon's AWS is using a virtual SRX device in the Amazon cloud to provide this functionality.

E3A Pilot

The second pilot is for the EINSTEIN 3 Accelerated (E3A) program. This Department of Homeland Security (DHS)-mandated program will protect NOAA from malicious traffic by providing additional inspection of Domain Name Service (DNS) and email traffic. The DNS inspection is accomplished by using IPSec tunnels to carry all DNS traffic from NOAA to a service-provider partner that matches DNS requests against a blacklist. While this solution is designed to provide resilience and "fails open" in event of a network or device failure, this is an impactful change for the agency's critical traffic. When DNS is broken, all other connectivity appears to be down. The "fails open" is designed to prevent loss of DNS service. For this reason, N-Wave wanted to characterize the IPSec tunnel we would be provisioning to our service provider partner prior to working in conjunction with the NOAA Cyber Security Center (NCSC) to set up the permanent solution.

A single tunnel was provisioned from the test Boulder SRX240 to the service provider, and BGP routing configured. Internally, a test DNS server was provisioned and local BNOC users pointed at that DNS server. For several weeks, the BNOC users have been using the E3A service with acceptable delays. Tests have included using the test malicious URLs, which generated the expected email alerts from the service provider.

We gained much experience from this pilot as well. We learned some fundamental things, such as generating the proper security certificates for sessions to our service provider; understanding their BGP advertisements and routing policies; and experimenting with session-state options for managing the VPN device. It was useful for us to understand the added latency in using DNS from Boulder to the service provider in Northern Virginia.

This pilot will greatly accelerate N-Wave's ability to support the production deployment. NCSC will be deploying new DNS servers in each of the TICAP stacks, which will have anycast addresses facing internal NOAA clients. This is expected to be operational in late 2016 or early 2017.

Conclusion

Ultimately, connectivity for all cloud-based services will be migrated to the more powerful and permanent SRX hardware living in multiple TICAP facilities. These firewalls are planned to support VPN connections to Amazon Web Services, Microsoft Azure, service providers for E3A connectivity, and untrusted connections to support mission and R&E traffic. Architectural planning for these services is in progress.

N-Wave is looking forward to offering generalized VPN services into cloud providers as an additional high-speed TICAP option.

SC16 November Conference

The supercomputing conference, SC16, will be held in Salt Lake City in November. This year's theme is "HPC Matters," whether in precision medicine, weather prediction, or structure design. Programmers, scientists, researchers and engineers are drawn each year to SC to meet with their peers. The conference includes tutorials, a technical program, workshops, participation by students in HPC fields and a technical exhibit with universities from around the world, government agencies, and vendors.

One of N-Wave's engineers, Matt Smith, is co-chair of the team designing the conference's supporting network, SCinet. The Architecture team has designed a system to bring between 3-4 Tbps of connectivity into the Salt Palace Convention Center using 100 Gbps circuits.

NOAA-related events at SC16:

- Two of N-Wave's major partners, Indiana University and Internet2, both have booths. Several of our RON partners are also research exhibitors.
- The StarLight booth will have multiple 100G connections and feature multiple demonstrations. One of the demos will use NOAA's environmental data via the Open Cloud Consortium, with which NOAA has an agreement.
- Corey Potvin of the National Severe Storms Laboratory will be presenting in the Scientific Visualization & Data Analytics Showcase.

NOAA ENTERPRISE NETWORK

For more information contact:
NOAA N-Wave Program
http://noc.nwave.noaa.gov
Office of the chief Information Officer
http://cio.noaa.gov
Robert Sears, Network Manager
Holly Palm, Design and Layout
Karin Vergoth, Editor

U. S. Department of Commerce, NOAA
325 Broadway, NWAVE
DSRC - GB306
Boulder, CO 80305-3337