National Oceanic and Atmospheric Administration (NOAA)
Office of the Chief Information Officer (OCIO)

N-Wave Service Catalog

Version 1.6 | Q3 2024

Email: nwave-communications@noaa.gov
Website: nwave.noaa.gov

Table of Contents

About N-Wave

N-Wave is the National Oceanic and Atmospheric Administration's (NOAA) network service provider and has been in operation since 2009. N-Wave's foundation relies on an extensive array of partnerships and relationships among NOAA, the Department of Commerce, other federal agencies and the academic and state research network communities. N-Wave's national network infrastructure extends across the contiguous U.S. to Alaska and Hawaii — reaching remote field sites, major campuses, data centers and supercomputing facilities. Combined with its scalable cloud solutions, robust catalog of enterprise managed services and advanced network operations, N-Wave supports all stakeholder missions with integrity, transparency and flexibility, and employs a unique partnership approach to provide the best customer experience.

What makes N-Wave unique?

- NOAA operated and managed national infrastructure, ensuring capacity, security and data delivery
  assurance
- Solid partnerships within the science, research and education (SR&E) community
- Trusted Internet Connection (TIC) services (X-Wave)
- Scalable cloud solutions
- Robust catalog of enterprise managed services
- Advanced network operations
- High value asset, authorized high Federal Information Security Modernization Act (FISMA) system, full network service provider

N-Wave works closely with its community of stakeholders and partners to ensure the network meets their needs today and in the future. From the brightest stars to the deepest oceans, N-Wave's operations support the important missions of its federal agency partners to provide vital public services, national and economic security, and to protect and serve the American people.

N-Wave Provided Services

N-Wave offers key technical services as described in the N-Wave Service Catalog. The N-Wave Service Level Agreement further defines the expected service performance, metrics and delivery. The following technical service areas are offered. Costs for specific services are provided upon receipt of an **N-Wave service request** with required additional customer information.

Enterprise Transport Services (Layer 0-3)
These services provide wide and metro area network connectivity to support the vast missions of stakeholders among NOAA, the Department of Commerce, other federal agencies and the academic and state research technical communities. N-Wave's NOAA owned and operated national network infrastructure extends across the contiguous U.S., Alaska and Hawaii - reaching remote field sites, major campuses, data centers, supercomputing facilities and the cloud.

Trusted Internet Connection Access Point (TICAP)
In collaboration with the NOAA Cyber Security Division, N-Wave is the network provider for Trusted Internet Connection (TIC) services across NOAA, with the ability to deliver these services to other bureaus in the Department of Commerce. TIC services leverage N-Wave Enterprise Transport and its public peering network infrastructure, X-Wave, to route traffic to and from the internet through Trusted Internet Connection Access Points (TICAPs).

Enterprise Network Services

There are four primary offerings included as part of network services, to include enterprise wireless, Managed Local Area Network (LAN), Enterprise Remote Access VPN (ERAV) and firewall.

- **Enterprise Wireless** - This service provides for data transport and access to the internet on WiFi-enabled devices. It also provides secure wireless internet access for employees that is wirelessly protected using FIPS 140-2 validated encryption. Employees must use a VPN to access internal networks while connected to WiFi. The service also provides temporary, unencrypted wireless access for sponsored guests and visitors.

- **Managed LAN** - This service is offered to provide full LAN management down to the access port for customers at large, medium, small and micro-sized sites. The service uses standardized hardware, software and network design models to reduce complexity, ensure compatibility among network components, simplify troubleshooting and improve security posture. N-Wave is able to build reliable, scalable and high-performance switching networks—without compromising network simplicity and ease of management. With the ability to securely converge multiple entities and services onto a single network infrastructure, N-Wave can also reduce labor, maintenance and equipment costs while improving the service for all.

- **ERAV** - This service is offered as a centralized solution that leverages N-Wave transport to provide remote access network connectivity to users on Government-Furnished Equipment (GFE) devices. ERAV allows users to obtain secure access to their organization's internal networks and resources while working from home or on travel and is fully compliant with NOAA VPN Policy.

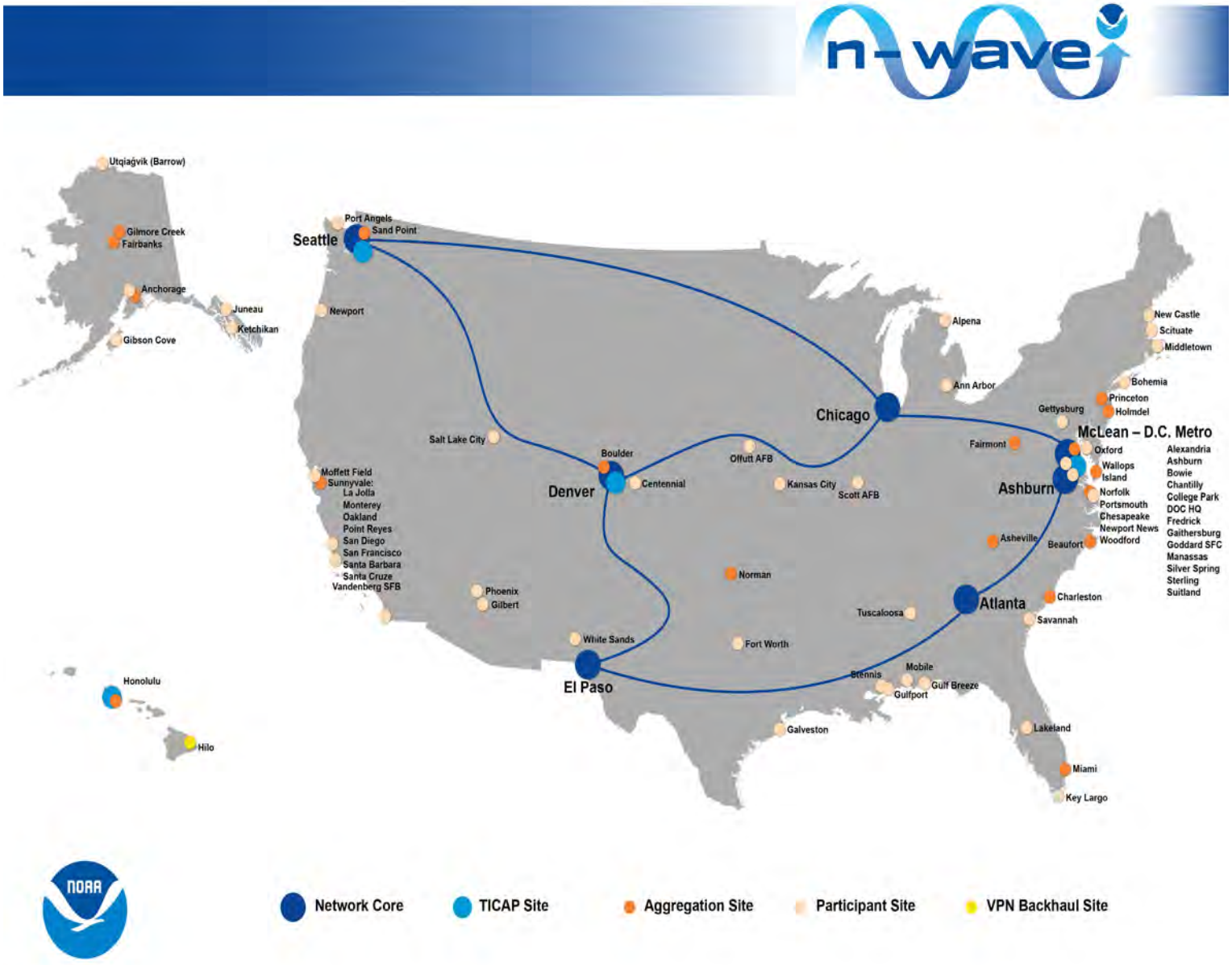
- **Enterprise Firewall** - This service provides a fully managed firewall solution that includes procurement, installation, configuration, monitoring, and management.

Enterprise Cloud Services

This service offers three solutions to support unique and complex cloud connectivity use cases. The service leverages N-Wave Enterprise Transport to connect customers' premise-based infrastructure to multiple cloud service providers, including Amazon Web Services, Google Cloud Platform, Microsoft Azure and Oracle Cloud Infrastructure.

N-Wave is committed to providing innovative, customer service driven engineering to support all transport capabilities and customer requirements through: network assessments (WAN/LAN); wireless network assessments; network design and strategy consulting; network deployment; and, special projects.

N-Wave Network Map



This map shows N-Wave's traffic across its vast network in the U.S. and to Alaska and Hawaii, including locations for the network core, Trusted Internet Connection Access Point (TICAP) sites, aggregation sites, participant sites and Virtual Private Network (VPN) backhaul sites. N-Wave continues to grow and expand its network.

N-Wave Subscribed Services

Enterprise Transport Services (Layer 0-3)		
Service Type	**N-Wave Role**	**Customer Role**
Co-Location	Provide racks for customer network assets (telcom, nondata) at the specified co-location facility.	• Define a program representative as Point of Contact (POC) for this service.
Layer 1: Lit and Dark Fiber Services	Provide annual procurement and tracking of lit and dark fiber services.	
Layer 1: Optical Lambda Transport over DWDM Gear – 10G/ 100G	In specific regions, N-Wave may be able to provide optical engineering solutions.	
Layer 2: Virtual Local Area Network (VLAN) Transport – 1G/10G/100G	N-Wave can provide private ethernet transport services, VLAN multi-point at 1G, 10G to 100G to support: • Wide area and metropolitan-area connectivity to NOAA campuses, laboratories, data centers and sites • Wide area and metropolitan-area transport for direct intra program connectivity. • Virtual Private LAN Service (VPLS) to provide ethernet-based multipoint to multipoint communication.	• Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Layer 3: Internet, Internal-External Routing 1G/10G/100G	N-Wave can provide private Layer 3 VPN multi-point IP routed services, Public Layer 3 transport to the NOAA TICAP (Internet, Internet2), NOAA-to-NOAA IP transit, 1G and 10G and up to 100G for R&E peering to support: • Wide area and metropolitan-area connectivity to NOAA campuses, laboratories, data centers and sites • Wide area and metropolitan-area transport for direct intra program connectivity. • Multiprotocol Label Switching (MPLS) allows for the creation of end-to-end circuits across any type of transport medium, using any protocol. • Both IPv4 and IPv6 transport. • Multicast communications. • Transport to NOAA TICAPs. • Internet and R&E providers. • Cloud services connectivity 1G VPN (any Cloud service provider). • Cloud broker connectivity service 2-10G (e.g., Azure, AWS, Google, Azure-AWS Gov, Oracle).	

Enterprise Transport Services (Layer 0-3)		
Service Type	**N-Wave Role**	**Customer Role**
Trusted Internet Connection Access Provider (TICAP)	• High bandwidth and availability • Redundant TICAP infrastructure at sites in the D.C. metro, Denver, Seattle and Honolulu • TICAP sites in the contiguous U.S. are capable of failover within and between sites • Dedicated infrastructure in Honolulu reduces latency for customers at Hawaii sites • X-Wave ensures symmetric traffic flow through each TICAP • Service is compliant with Office of Management and Budget TIC requirements • 24x7 Tier 1 support and expert troubleshooting from a centrally managed and geographically dispersed team of Tier 2 and 3 engineers • Robust configuration management, monitoring, alerting and diagnostic tools TIC customers can inherit the following controls through CSAM: • SC-7.c, SC-7(3), SC-7(4).a, SC-7(4).b, SC-7(4).d, SC-7(4).e – Boundary Protection	• Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Enterprise Network Services		
Service Type	**N-Wave Role**	**Customer Role**
Cable Plant	• Provide cable plant standards, training and mechanism for tracking cable assets.	• Help adhere to cable plant standards. • Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Managed Local Area Network (LAN)	• Provides network as a service. • Procure, install, configure, patch, scan and perform annual assessment and authorization on N-Wave managed network components. • Access layer is normal business hours with core layer 24/7.	• Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process. • Customer is responsible for patching end systems into switches.
Enterprise Wireless	• Design, deploy, manage and monitor the wireless network infrastructure within the campus. • Respond to Tier 2/3 system level issues from the campus. • Provide training for system administrators. • Normal business hours response.	• Report issues to their local Systems/IT administrator. • Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Local N-Wave Services Engineer	• Provide onsite tier 2/3 N-Wave network engineers for direct campus support of N-Wave services. • N-Wave engineers will prioritize efforts to N-Wave campus provided services and N-Wave enterprise services in use at the campus (e.g.wireless, VPN). • Normal business hours response. • Onsite engineers will provide hands and eyes for N-Wave equipment and troubleshooting of N-Wave services. • Interface with local POCs on an ongoing basis to provide the site with a more personalized experience.	• Verify and troubleshoot connectivity from end device to N-Wave device. • Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.

Enterprise Network Services		
Service Type	**N-Wave Role**	**Customer Role**
Enterprise Remote Access VPN (ERAV)	• Provide client remote access VPN services for access to internal network resources. • Normal business hours response.	• Designate VPN admin to be the POC for VPN group. • VPN admin will triage user issues and, when needed, submit tickets to N-Wave. N-Wave will only accept tickets from designated VPN administrators. • Users desktop support are responsible for maintaining VPN profiles and Anyconnect versions.
Firewall Services	• Provide firewalls as a service, including procurement, installation, configuration, monitoring and management. • 24x7x365 management, monitoring and response.	• Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process. • Customers need to ensure the request is approved by the customer change management process prior to submission to N-Wave. N-Wave will only accept changes from approved submitters. • Customers will be responsible for defining security rules.

Enterprise Cloud Services		
Service Type	**N-Wave Role**	**Customer Role**
Microsoft Azure Commercial Landing Zone	• N-Wave provides hub and spoke topology. • N-Wave manages the hub consisting of load balancers and firewalls. • Options for private and public peerings. TICAP compliant.	• Manage spokes. • Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Microsoft Azure Government Landing Zone	• N-Wave provides hub and spoke topology. • N-Wave manages the hub consisting of load balancers and firewalls. • Options for private and public peerings. TICAP compliant.	
Amazon Web Services (AWS) Landing Zone	• TBD – Service in development.	
Google Cloud Landing Zone		
1G VPN *(Any cloud service provider)*	• Options for private and public peerings. TICAP compliant.	• Define a program representative as Point of Contact (POC) for this service. • Designated Point of Contact (POC) will submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process.
Broker Connectivity Service 2-10G *(Azure, AWS, Google, Azure-AWS Gov, Oracle)*		

Value-Add Services for All N-Wave Stakeholder Customers

To provide exceptional service to its stakeholder customers, the following are direct value-added benefits included with N-Wave subscribed services:

Network Operations
N-Wave partners with the Global Network Operations Center (GlobalNOC) at Indiana University to provide highly available, world-class advanced network operations with an emphasis on professional and customer service driven interaction delivered across Tier 1, II and III levels of engineering service, advanced monitoring, measurement, visualization and analysis tool sets. This support is 24 x 7 and 365 days a year.

The Tier 1 service desk and Tier 2-3 engineering service types primarily support these operations. For the most efficient response with respect to network operations, stakeholder customers must designate a Point of Contact (POC) to submit trouble tickets to N-Wave and configuration change tickets via the N-Wave change management process. Cyber incidents localized to Federal Information Security Modernization Act (FISMA) users will be assigned to FISMA Information System Security Officer's via the NOAA Incident Response Reporting Application system.

Network operations is provided to all N-Wave customers who utilize transport, network and cloud services; however, the following services can be leveraged to customize individual Line Office or program needs:

- NOC Service Desk (Tier-1)
- Tier-2 engineering support
- Tier-3 engineering support
- Custom tool development and systems support
- Advanced network measurement and visualization service
- Customer Grafana dashboards

Security Controls
Security protections have always been built into N-Waves services. As an added value, N-Wave offers security controls for inheritance to its NOAA customers. FISMA of 2014 requires federal information systems to establish strategies for implementing required security controls within their system boundaries. When common service providers like N-Wave build controls into their services and then officially offer those controls for inheritance, customers can save time and expenses associated with establishing and documenting those safeguards on their own. For security controls, N-Wave provides both transport services (WAN/TICAP) and networking wireless (VPN) services as part of its security controls.

N-Wave's 24/7/365 Network Operations Center is provided in partnership with GlobalNOC at Indiana University

(Photo credit: GlobalNOC at Indiana University)

- **Transport Services (WAN/TICAP)** - N-Wave provides common controls for network availability and NOAA's Cyber Security Center (NCSC) with required logs, access to tools and other methods for initial triage of cyber incidents deemed sourced from the customer.

- **Networking Services Wireless (VPN)** - N-Wave provides common controls defined in the wireless service SLA and NOAA's NCSC with required logs, access to tools and other methods for initial triage of cyber incidents deemed sourced from wireless users.

How Customers Reach the N-Wave NOC

N-Wave's Network Operations Center can be reached 24 hours a day/7 days a week through the submission of an online service request form, by phone or email.

Submission of an N-Wave Request Form (3 options to select from):

1. **New Service Request** - Select if you need a service you do not currently have (i.e. new WAN connectivity, ERAV VPN Group, Managed LAN service inquiry, wireless service inquiry)

2. **Change in Service Request** - Select if you currently have a service and would like to modify or expand the service (i.e., add/remove/change ERAV group membership, change VLAN on a port, update prefix list)

3. **Request Support** - Select if you require assistance with an existing service (i.e., service outage, service degradation, service quality issues, routine maintenance)

By Phone: (812) 856-7477
By Email: nwave-noc@noaa.gov

scalability, reliability, security, robustness, strong partnerships with national networking infrastructures and advanced network operations

N-Wave Delivers Value

Service Level Agreement

Service levels are derived from historical data collected across various elements ranging from circuits and hardware to maintenance and engineering.

- **SLA** = Service Level Actual - based on historical data collection.
- **SLO** = Service Level Objective - target objective. This transitions to SLAs after a year of historical data is collected.

Enterprise Transport Services		
Service Element	**SLA or SLO**	**Service Response***
N-Wave Backbone	• SLA = 99.999%	• Tier 1-3 24x7x365
TICAP Services**		
Dual Core Connected Site (includes Cloud Transport)	• SLA = 99.99%	
Single Core Connected Site	• SLA = 99%	
Enterprise Cloud Transport VPN/Broker	• SLO = 99.99%	
Enterprise Network Services		
Dual Core Managed LAN Core Routing/Backbone	• SLA = 99.99%	• Tier 1-3 24x7x365
Single Core Managed LAN Core Routing/Backbone	• SLA = 99%	
Managed LAN Aggregation / Access Switching***	• SLA = 99.99%	• Tier 1, 24x7x365, Tier 2-3. 8x5xNBD
Enterprise Remote Access VPN (ERAV)***		
Wireless***		
Enterprise Cloud Services		
Landing zones all	• SLO = 99.9%	

*Refer to Appendix A - N-Wave NOC Response Time Agreement and Target Level of Service
**TICAP availability will be derived from a combination of network infrastructure resiliency coupled with TIC stack security component availability and stability
***8x5xNBD = Support during regular business hours M-F with support beginning the next business day for after hours or weekends. (Critical escalations will follow the defined procedure in Appendix A: N-Wave NOC Response Time Agreement and Target Level of Service)

From the Campus to the Cloud

N-Wave Provides Solutions

Through direct customer engagement, requirements gathering, and active monitoring, N-Wave continually seeks options to enhance deployed-in-place services, improve technology and capability of the current N-Wave network infrastructure.

N-Wave is also looking to the future with the design and engineering of the next generation of N-Wave infrastructure. At all levels, N-Wave collaborates and partners with NOAA, the research & education network community, commercial businesses and other federal agencies who are dedicated to exploring and implementing new and advanced networking technologies.

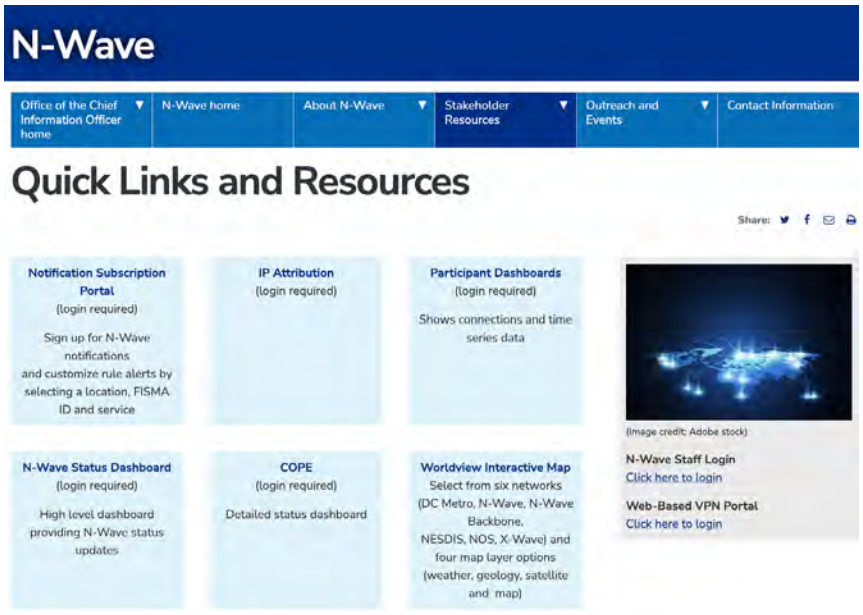
The N-Wave program embodies a culture of networking and all N-Wave customers benefit from the program's involvement in:

- Dedicated program support
- Direct customer requirement gathering sessions
- Diverse teams with strong science, research and engineering collaboration and robust advanced tools
- Performance capacity planning
- Recurring customer project and planning calls
- Stakeholders and science engagement summits
- Technology exchanges/community workshops
- Test beds and proof of concepts

N-Wave Resources and Tools

To access quick links and resources N-Wave dashboards and other resources and tools (login may be required), click **here**.

- Notification Subscription Portal
- IP Attribution
- Participant Dashboards
- N-Wave Status Dashboard
- COPE
- Worldview Interactive Map



Appendix A
N-Wave NOC Response Time Agreement and Target Level of Service

The N-Wave NOC is a contractual agreement and partnership between N-Wave and the Global Network Operations Center (GlobalNOC) at Indiana University.

Expected Service Desk Response Time – 15 Minutes

N-Wave NOC Service Desk is staffed 24 hours a day, seven days a week, all year long (24x7x365) and responds immediately to all incidents reported to the N-Wave NOC or when alarms are noticed on monitoring systems. Service Desk technicians will begin immediate problem assessment and analysis to identify the severity of the issue to include the following:

- Initial Problem Assessment
- Collect customer contact information
- Collect circuit, network device, customer/network impact information, service(s) affected information
- Check monitoring tools
- Reconcile scheduled maintenances
- Collect traceroute, ping, router information, ect.
- Create and assign trouble ticket to engineering
- Contact is assigned round-robin style through either the on-call engineer or Network Planning Team (NPT) engineer

NOTE: *Since critical issues require faster response times for notifying engineers, some of the information above may be added to the ticket after initial ticket assignment.*

Expected N-Wave NOC Engineer Response Times

Priority and severity impact level guidelines exist for how soon after a ticket has been created and assigned to an engineer that investigation must begin. All tickets are worked based on criticality, and ongoing major incidents may affect actual response times. See the chart on the next page for more detailed information.

N-Wave NOC Support - Customer Impact Guidelines (PRIORITY)

Customer Impact is a subjective scale of measure used to quantify the current impact of a problem or maintenance on the customer's operations, performance, and usability. Set in conjunction with the customer, it may change as the ticket progresses and is used for ticket escalation. Customer Impact seeks to answer, "How high of a priority is the problem/maintenance to the customer?"

Impact Level (Priority)	Investigation (Response Time)
• A problem or issue for which the customer needs immediate, undivided attention from NOC staff until resolved. • The customer is expected to be available immediately to commit full-time resources until the situation is resolved. • The NOC uses this by default when the network is monitored to have an outage of a non-redundant core network element.	**Critical (1) - 10 minutes**
• A problem or issue for which the customer needs resolution within one business day. • The customer is expected to commit resources to resolve the situation between the hours of 1300 and 0100 UTC (1200 and 0000 UTC when Daylight Saving Time is in effect). • The NOC uses this by default when the network is monitored to have an outage of a redundant core network element.	**High (2) - 1 hour**
• A problem or issue for which the customer does not need immediate resolution, but needs NOC attention within three business days. • The customer is expected to be available to provide information or assistance when available during normal business hours. • The NOC uses this by default when a customer connection or session is monitored to have a problem or outage. This is also used by default for maintenance which is both NOC initiated and customer impacting.	**Moderate (3) - 1 day**
• No impact to the customer's operations, performance and usability. • Non-urgent customer service requests. • Routine installation/provisioning tickets, non-customer impacting maintenance and customer initiated maintenance.	**Low (4) - 3 days**

N-Wave NOC Support - Network Impact Guidelines (SEVERITY)

Network Impact is an objective scale of measure used internally to quantify the highest level of impact to the network that occurred throughout the duration of a problem or maintenance. Network Impact seeks to answer, "How severe is the problem/maintenance to the network?"

Impact Level (Severity)	Investigation (Response Time)
• The network, a portion of the network, or a key network resource fails, causing an outage of service. • The network, a portion of the network, or a key network resource, is severely degraded rendering the network nearly unusable.	**Critical (1) - 10 minutes**
• The network, a portion of the network, or a key network resource, fails or is severely degraded, but service has not been affected due to redundant resources. • The network, a portion of the network, or a key network resource, is experiencing mild-to-moderate degradation, and service is affected. • Security requests and incidents.	**High (2) - 1 hour**
• Network problems or maintenances of limited scope that pose no risk to the network as a whole. • Direct connectivity to a single entity (peer, connector, lambda) has been lost.	**Moderate (3) - 1 day**
• No network impact.	**Low (4) - 3 days**

For more information about N-Wave, visit our website or contact us:

Email: nwave-communications@noaa.gov
Website: nwave.noaa.gov

Revised May 2024