THE NETWORK OPERATIONS CENTER (NOC): HOW NOCS WORK

In ITIC's 11th annual Hourly Cost of Downtime Survey, published in 2020, 40% of enterprise respondents estimated that an hour's downtime cost their organizations $1-5 million dollars in lost revenue, end user productivity, and remedial action by IT administrators.

And that $1-5 million does not consider legal fees, fines, or penalties.

From a user perspective, uptime and performance are key determinants of service quality. That's why service providers require high levels of visibility on components, configurations, and dependencies that can indicate service status and issues.

The Network Operations Center (NOC) is one such capability that organizations can deploy in order to support this need.

What is the NOC?

Short for network operations center, the NOC (pronounced "knock") refers to a centralized location where 24/7 monitoring and management of events affecting technology services and infrastructure takes place.

This location can be managed by you—the direct service provider—or to an outsourced third party.

NOCs were first originated in the late 1970s by telecommunication service providers (thus the 'network' name) for displaying the status of switches, routing, and circuits.

Today's NOC is not only restricted to monitoring networking equipment (e.g. routers, switches, servers), but also cloud, power, environmental, and service aspects such as:

- Transactions
- Traffic
- User patterns

Here, the term 'operations' refers to the delivery and support of:

- Live services
- Services about to be deployed

So, it's not so much about the development side of things, though the NOC might monitor the overall development environment since it is a "live service" for developers.
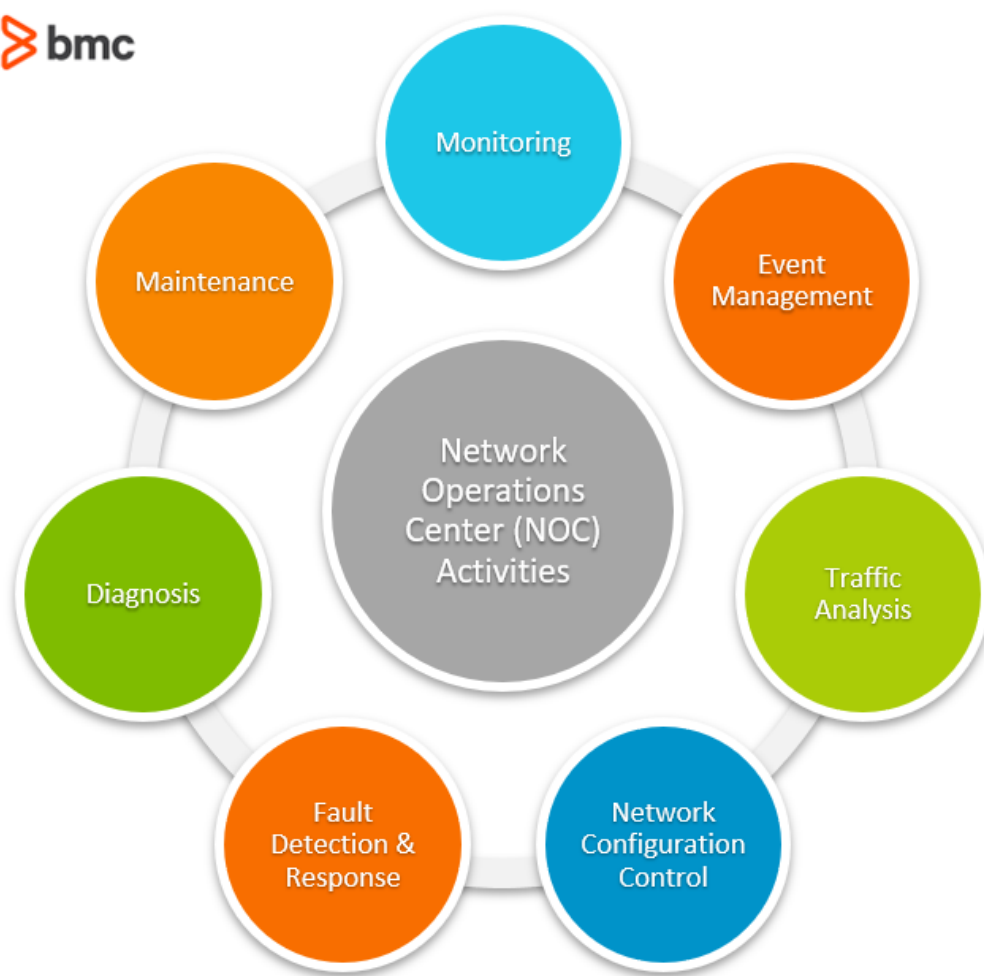
What happens at the NOC?

In terms of activities at the NOC, the two main jobs are monitoring and event management.

Other activities at the NOC include:

- Traffic analysis
- Network configuration control
- Fault detection and response
- Diagnosis
- Maintenance

Some NOCs are also used for monitoring security events, though some practitioners advocate for separation using a [Security Operations Centre (SOC)](#) due to confidentiality concerns.

Monitoring

According to the [ITIL® 4](#) Practice Guides, monitoring focuses on:

- Detecting conditions of potential significance in configuration items
- Tracking and recording their state
- Providing this information to relevant parties

Event management

On the other hand, event management focuses on those monitored changes of state defined by the organization as an event, determining their significance, and identifying and initiating the correct response to them.

Information about events is also recorded, stored, and provided to relevant parties.

Additional service management practices

Monitoring and event management activities are key inputs to other service management practices where visibility, uptime, and performance are critical such as:

- **[Incident management](#)**. Minimizing the negative impact of incidents by restoring normal service operation as quickly as possible.
- **Deployment management**. Moving service components into live environments.
- **[Release management](#)**. Making new and changed services and features available for use.
- **Information security management**. Protecting an organization by understanding and managing risks to the [confidentiality, integrity, and availability](#) of information.
- **[Service continuity management](#)**. Ensuring service availability and performance are maintained at a sufficient level in case of a disaster.

Who works in a NOC?

The NOC engineer is a frontline staff who is expected to:

- Know how things work
- Be able to pinpoint where issues are coming from, using both experience and analysis

The scope of a NOC engineer's job can be quite wide depending on the service provider's service offerings and infrastructure layout. Some organizations also assign backup and patch management activities to NOC staff.

(Learn more about [what NOC engineers do](#).)

Network Operations Center

What's inside a NOC?

Being the mission control for a service provider, screens are the hallmark of any NOC. Due to your centralized location, you likely have both:

- Large screens, such as video walls, for sharing key indicators like traffic and node status.
- Smaller monitors, usually part of an operator's desk console, for viewing specific elements.

More often than not, the main screens show outputs from a centralized monitoring system that gathers, synthesizes, and correlates data from numerous sources—hence the need for visibility by a large number of people.

The operator desks display actual event information including:

- Alarm status
- Source
- Time
- Other relevant data

So, the screens are the main feature on the walls. Then you have the operator desks and other capabilities that would be required, including:

- Telephones for contacting relevant field/specialist support staff and third parties
- Computers with office software for email, collaboration tools, and reporting tools
- Service management software tools for logging and escalating significant events
- Software tools for remote access into and troubleshooting affected elements
- Knowledge bases for referencing system information and troubleshooting guides
- Television screens displaying news, social media feeds, and other relevant information sources

Designing a NOC

When it comes to setting up a NOC, it is important to consider both people and environment.

The people aspects will include:

- [Ergonomic office furniture](#) and IT equipment to support NOC engineers during their shifts
- Spacious design to allow air flow, comfort, easy mobility (due to the need to gather at screens to discuss what's going on)
- Adjoining break rooms with kitchen facilities as NOC engineers are expected to stay near the NOC during their breaks

The environment aspects will include:

- Layouts that allow for unhindered viewing of the larger wall screens across the NOC
- Quadrants that separate specialist NOC teams monitoring designated elements
- Redundancy for power and connectivity to ensure unhindered 24/7/365 operations
- Scalability to support future growth needs for people, equipment, stations, and screens

Due to its critical nature, the design, implementation, and operation of the NOC cannot be left to chance. The input of all stakeholders—especially the NOC engineers—is crucial in ensuring that the NOC achieves the key objectives of the service provider: availability and performance of its technology services and systems.

Related reading

- [BMC IT Operations Blog](#)
- [State of IT Monitoring: A Report Roundup](#)
- [What Is High Availability? Concepts & Best Practices](#)
- [What is Security Information and Event Management (SIEM)?](#)
- [Top IT Operations Trends in 2021](#)