Data Center Maintenance

Faria Afrin Niha
Lecturer
Department of CSE & CSIT

Course Code: CSE 3316

Course Title: Data Center Management

Network Operations Center (NOC)

- A **Network Operations Center (NOC)** is a centralized, secure facility inside an organization or data center where technical staff continuously monitor, manage, and maintain IT infrastructure, networks, and services. It ensures maximum **uptime, performance, and reliability** of critical systems.
- The NOC works **24 hours a day, 7 days a week**, especially in large organizations, banks, telecom companies, and cloud service providers.

❑ **Functions of a NOC:**

A NOC is responsible for:

- • Monitoring all **network devices** (routers, switches, firewalls)
  • Monitoring **servers** (physical and virtual)
  • Checking performance of **applications and databases**
  • Identifying failures, bottlenecks, and security warnings
  • Sending automatic alerts when thresholds are crossed
  • Managing disaster recovery and system restoration
  • Coordinating with engineers and technicians for quick repairs

NOC

❑ Hardware and Software in a NOC

- **Hardware**
  - High-performance monitoring servers
  - Multiple large display screens (video wall)
  - Monitoring consoles/workstations
  - Backup power (UPS and generators)
- **Software Tools**
  - **HP OpenView**
  - **BMC Patrol**
  - **IBM Tivoli**
  - **CA UniCenter**
- SIEM systems for security monitoring
- These tools monitor:
  - ✔ CPU usage
  - ✔ Memory usage
  - ✔ Network traffic
  - ✔ Errors and failures
  - ✔ System availability

Role of SNMP in NOC

- **Simple Network Management Protocol (SNMP)** is used to communicate with:
  - • UPS systems
    • HVAC systems (cooling)
    • NAS storage devices
    • SAN switches
- SNMP agents installed on devices collect data such as:
  - Temperature
  - Power status
  - Disk failure
  - Fan speed
  - System load
- This information is sent to the NOC software for **real-time monitoring and alerts**.
- **Benefits of a NOC**

✅ Faster problem detection
✅ Reduced downtime
✅ Better performance management
✅ Improved security monitoring
✅ Centralized control system
✅ Increased system reliability

Network Monitoring

- A critical requirement of data centers is **proactive monitoring** of:
  - Servers
  - Network resources
  - Services
- Network monitoring helps IT and network managers **understand what is happening** in the environment in real time.
- It works like a **smoke alarm system**:
  - Detects problems early
  - Sends warnings when something goes wrong
- Monitoring software is **proactive, not just reactive**:
  - Alerts on sudden bursts in network traffic
  - Warns when file systems approach capacity limits
  - Detects early signs of **Internet attacks** (e.g., on edge routers)
- Helps prevent:
  - System failures
  - Network downtime
  - Security breaches
- Improves:
  - System reliability
  - Performance management
  - Business continuity

Monitoring Requirements

- Without network monitoring, IT management becomes **reactive**
  - Problems are discovered only after users complain
  - Leads to **delays and downtime**
- Network monitoring enables **proactive management**
  - Issues are detected before they impact users
  - Improves overall system reliability
- Monitoring tools gather **real-time data** from:
  - Servers
  - Network devices
  - Applications
- Collected data is classified into **two main categories**:
  1. **Performance Issues**
     - Used to predict future capacity and scaling needs
  2. **Outages**
     - Trigger immediate alerts to on-call staff
- **Alert Mechanisms** include:
  - Pager notifications
  - Urgent phone calls from the NOC
  - Real-time warnings on dashboards
- A **Network Operations Center (NOC)** serves as:
  - The central monitoring hub
  - The point of action during emergencies

Figure 6-1 A network operation center (NOC) is used to resolve problems or escalate them to the appropriate personnel.

SNMP

- SNMP is the **primary protocol** used for monitoring network and system resources in a data center.
- It helps discover:
  - What devices exist on the network
  - The status and performance of each device
- It sends health and performance data to a **central monitoring server** (usually in the NOC).
- SNMP data is presented in **visual dashboards**, charts, and reports for easy analysis.
- Reduces the need for manual checking of devices.

❑ Technical Operation

- SNMP operates over the **User Datagram Protocol (UDP)**.
- It mainly communicates through **port 161**.
- The SNMP daemon (service) is called:
  - **snmpd** (Linux/Unix)
  - **snmpdx** (Solaris/others)
- Devices running SNMP are referred to as **SNMP agents**.
- The central monitoring system is called the **SNMP manager** or **collector**.

SNMP

❑ OIDs and MIB

- SNMP uses **Object Identifiers (OIDs)** to identify each piece of data.
- A **Management Information Base (MIB)** is a structured collection of OIDs.
- MIB is arranged in a **hierarchical tree format**.
- Each "object" in the MIB may represent:
  - CPU temperature
  - Disk usage
  - Network traffic
  - Router interface status
  - Application (httpd) status
- By extending the SNMP daemon, **custom events and hardware sensors** can also be monitored.

❑ Vendor Assignment

- SNMP assigns **unique number ranges to vendors** in a nested format.
- Example:
  - Cisco Systems = **1.3.6.1.4.1.9**
- This allows each manufacturer to define its **own device-specific metrics**.

SNMP

❑ SNMP Commands / Actions

1. **GET**
    1. Used to request an OID value
    2. Example: Checking disk usage or CPU load
2. **SET**
    1. Used to modify device configurations
    2. Example: Changing threshold values or allowed connections
3. **TRAP**
    1. Automatically sends a message when a specific event occurs
    2. Example: Sending an alert when a server goes down

❑ Security Issues & Protection

- SNMP is **insecure by default** and can expose sensitive data.
- Uses weak authentication in older versions:
    - **Public community string** (read-access)
    - **Private community string** (write-access)
- Many devices keep the default string **“public”**, which is a serious risk.
- Attackers can poll SNMP-enabled devices without a password if defaults are unchanged.
- Most data centers **disable SNMP SET** to prevent unauthorized modification.

SNMP

◦ **SNMPv3 – Enhanced Security**

- SNMP version 3 provides better protection:
  - Encrypted communication
  - Strong authentication (MD5 / DES)
  - User-based access control
- SNMPv3 is preferred for **secure data centers**.

In-Band and Out-of-Band Monitoring

- In-band monitoring is the capability to change system status through the existing network infrastructure.
- Out-of-band monitoring is the capability to control systems not through existing network infrastructure but via a different data network or via a dial-in capability for individual devices.
- Several vendors have phone-line modems connected to their devices in customer data centers. These send device alarms to the vendor support personnel.
- It is important to get immediate alarms from equipment. It has been found that mean time to repair (MTTR) contributes more to service outage periods than mean time before failure (MTBF).
- The sooner you are alerted to a problem, the sooner it can be resolved. Critical systems must have no downtime.
- Besides monitoring the devices, servers, and storage subsystems, several other data center–wide features must be monitored, such as
    - ■ Power from the utility provider
    - ■ UPS status and usage
    - ■ Generator status and usage
    - ■ Leak detection from HVAC and air ducts and from liquid in the HVAC units
    - ■ Temperature in the data center
    - ■ Relative and absolute humidity in the data center
    - ■ Intrusion in the facility

Data-Center Physical Security

- Physical security is critical for protecting servers and data.
- Security breaches at the data-center level can compromise all hosted systems, even if network security is strong.

❑ Access Control

- All entry points must be **controlled and monitored**:
  - Card readers
  - Security personnel
- **Biometric readers** (palm, fingerprint, iris) enhance access control.
- **Cameras** should monitor:
  - Data-center doors
  - Corporate entrances
- **Restricted access**:
  - Only authorized employees may enter
  - One-time access policies for visitors
  - Access events are logged for accountability

Data-Center Physical Security

- **Types of Data Centers & Security Needs**

1. **Co-location (CoLo) Data Centers**
    1. Hundreds or thousands of customers visit daily
    2. Critical to **control and monitor access** for each visitor
    3. Risk: Visitors may accidentally or intentionally damage other customers' equipment
2. **Managed Hosting Data Centers**
    1. Only a few trusted employees have access
    2. Customers generally **do not have access**
    3. If access is required:
        1. Must be escorted
        2. Given temporary badges
    4. **Biometric systems** often used for secure access
    5. Advantages:
        1. Activities are logged
        2. Cards cannot be shared
        3. Immediate removal of unauthorized employees

Data-Center Physical Security

❑ **Complementary Security Measures**

- **CCTV Surveillance**:
  - Monitors and records all activities
  - Focus on all entry and exit points
- **OS and Security Updates**:
  - Servers are vulnerable to network attacks even with strong physical security
  - Up-to-date OS images and patch sets are critical
  - Managed hosting providers should evaluate and deploy patches safely
- **Practical Considerations**:
  - Enterprise servers may not be updated immediately to avoid affecting production systems
  - Testing on development/staging servers first is standard practice

Data-Center Logical Security

- **Importance**
  - Protects **valuable organizational information** stored online.
  - Prevents **unauthorized access** via the network.
  - Complements **physical security** by securing server and network access.
- **Core Principles**
  - **Prevent illicit access** to data and servers.
  - **Restrict access** only to authorized personnel.
  - Make it difficult for intruders to **reach login prompts**.
- **Access Control Measures**
  - **Close vulnerable ports** (e.g., Telnet).
  - Use **secure protocols** like SSH for remote access to UNIX/Linux servers.
  - Limit the use of **low-number ports (<1024)** to essential services only.
  - Control **console-level access**:
    - Allows remote diagnosis during boot-up before network services start.
    - Introduces a potential security risk if not properly controlled.

Data-Center Logical Security

❑ **Multi-Layer Authentication**

- Implement **more than one layer of authentication** before login.
- Allow only **necessary users** to access consoles beyond authentication layers.
- Force users to authenticate via a **central login server**:
  - Only the central server has direct console access.
  - Enhances monitoring and accountability.

❑ **Best Practices**

- Restrict access to **critical servers and devices**.
- Monitor login attempts and unauthorized access attempts.
- Use **centralized logging** for auditing purposes.
- Regularly review and update authentication methods and access lists.

Data-Center Cleaning

❑ Importance of Proper Cleaning

- Data centers are **different from office environments**; require specialized cleaning.
- Improper cleaning can **cause power outages or damage equipment**.
- Recommended frequency: **every 3–6 months** or after structural changes.
- Cleaning is typically performed by **qualified vendor crews**.

❑ Access & Safety Rules

- Cleaning crew must be **trained and familiar** with the data-center environment.
- Must have a **map of electrical outlets and restricted areas**.
- Rules for cleaning crew:
  - No food or drinks in the data center
  - Do not interfere with operations
  - No doors left open
  - Only authorized personnel allowed
- **Safety cones** around open tiles or damp-mopped areas.

Data-Center Cleaning

- **Approved Cleaning Supplies**
  - **HEPA vacuums** (triple-filtration) – remove 99.97% of particles ≥0.3 μm.
  - **Electrical cords** must be grounded, in good condition.
  - **Cleaning chemicals**: pH neutral, static dissipative.
  - **Mops**: lint-free, non-metal handles, looped ends.
  - **Wipes**: lint-free, antistatic.
  - Avoid leaving threads or debris on equipment or racks.
- **Floor Cleaning**
  - Care taken around **cables routed through floor tiles**.
  - HEPA vacuum for accessible floor areas:
    - Notched, perforated, and solid tiles.
  - Stains treated with **approved solutions** and medium-grade scrub pads.
  - Mop **damp (not wet)** with clean, warm water.
  - Avoid cleaning **under racks/equipment** to prevent disruption.

Data-Center Cleaning

- **Subfloor & Above-Ceiling Cleaning**
  - For **raised floors**: clean space under tiles carefully.
  - For **ceiling plenum**: clean above lowered ceilings where cables run.
  - Remove **no more than 10% of tiles at a time**, using **checkerboard pattern**.
  - Dispose of large debris manually.
  - Vacuum around **cable bundles, walls, and columns** carefully to avoid unplugging cables.
- **Equipment Cleaning**
  - **Do not spray chemicals directly** on equipment.
  - Use **lint-free cloths with antistatic cleaners** for racks, cabinets, servers, storage, and network devices.
  - HEPA vacuums for horizontal surfaces of equipment.
  - **Do not touch keyboards** during cleaning.
  - Report or correct any unusual floor conditions:
    - Loose floor pedestals
    - Cracked tiles
    - Condensation or wet areas
    - Loose brackets

Thank You