CAGAYAN STATE UNIVERSITY
APARRI, CAGAYAN, PHILIPPINES
GRADUATE SCHOOL

Student Name : John Lloyd Olipani
Student ID : 25-GS-20021
Subject Code : MSIT 206A - Network Administration
Program Chair : Dr. JULIETA B. BABAS, DIT

Activating Prior Knowledge

Network Knowledge Warm-up

- What I know…
  - Networking is an important field not only in the IT industry but also to large business enterprises and government offices
  - This is a field that generally handles how our human tools/technology communicate with each other
  - Network Administrators are responsible for the security of the networks and they make sure that it is always functional, reliable and devoid of any problems from outside interference.
  - It has something to do with CISCO technology

- I'm unsure of…
  - The technologies involved like routers, cables and switches
  - The different threats that could potentially destroy a network
  - The similarities and differences of WAN and LAN

- I want to learn…
  - More about CISCO gadgets
  - Hands on practices through simulation and if possible through the real deal
  - How much does it cost for a Network Admin to troubleshoot
  - The day to life of a Network Administrator
  - How to configure networks using Terminal
  - About DHCP, DNS and IP configurations

Formative Assessment
Network Knowledge Warm-up

Network issues in an organization: What Network administration areas are involved?" and "How did they resolve the issues?"

PhilHealth Ransomware Attack (2023) - MEDUSA

Reference:https://www.rappler.com/technology/philhealth-ransomware-attack-medusa-september-2023/

The agency also told the newspaper that the specific ransomware tied to the attack is the Medusa ransomware. "We have been coordinating with PhilHealth since this morning. We are assessing the impact at the moment. They are temporarily down [on the] eGovApp, but there are no indications eGov is affected," Dy said.

The Immediate Containment & Eradication (The First 48-72 Hours) response was conducted.The IT team's first action was to disconnect and isolate the infected servers and workstations from the main network to prevent the ransomware (Medusa) from spreading to other systems, particularly the backup servers. A critical step was creating forensic images (bit-by-bit copies) of the infected machines. This preserved evidence for investigation while allowing recovery work to continue on clean systems. Instead of trying to decrypt the files (which can be unreliable), the strategy was to completely wipe the infected systems and reinstall the operating systems and applications from scratch. This ensures no remnants of the malware remain.

The team checked their isolated, offline backup servers. Fortunately, these were not infected because they were disconnected from the main network which is a crucial practice. They began the process of restoring encrypted data from the clean backups onto the newly rebuilt servers. This is a time-consuming but essential step to recover operational data. Services were restored in phases, prioritizing critical functions.

The article mentions plans to procure and implement advanced cybersecurity tools to prevent similar future attacks. This incident was handled by PhilHealth IT Department & Cybersecurity Personnel, Management & Incident Command, Department of Information and Communications Technology - Cybersecurity Bureau (DICT-CSB), National Privacy Commission (NPC), National Bureau of Investigation - Cybercrime Division (NBI-CCD)

Role-mapping: Duties of NetAdmin vs. Network Engineer, produce a 2-page comparative brief

A network administrator and a Network Engineer have specific roles to fulfill and they are both critical to an organization's IT infrastructure. They operate at different scopes, their responsibilities differ from each other and their levels of strategies are exclusive to their own position. In a smaller organization, the differences of these two are sometimes not recognized and become normalized as overlapping fields of the same position.

For a Network Admin, their field involves Operational Stability and End-User Support. To put it simply in an analogy, they are the ants that work for the queen. They do operational work like maintenance and troubleshooting of day-to-day business operations.

Specific Responsibilities according to Google and AI Search Engines:

- Daily Operations
    - Monitor network performance & availability
    - Manage user accounts, permissions, and access controls
    - Perform routine backups and verify integrity
    - Apply patches and updates to network devices
    - Troubleshoot connectivity issues for end-users
- Security Maintenance
    - Configure and manage firewalls (basic rules)
    - Implement and maintain VPN access for remote users
    - Monitor security logs for anomalies
    - Enforce security policies and compliance standards
    - Manage antivirus/anti-malware on network level
- Infrastructure Management
    - Manage IP addressing (DHCP, DNS)
    - Configure and maintain switches, routers (basic)
    - Manage wireless access points and controllers
    - Document network configurations and changes
    - Manage network inventory and licensing
- Support & Troubleshooting
    - Tier 2/3 support for network-related issues
    - Coordinate with vendors for hardware repairs
    - Train end-users on network resources
    - Create and maintain network documentation for support teams

Network Engineers on the other hand, primarily focuses on Architectural Design and Strategic Implementation. When I say implementation, this basically means that it is heavily involved in project-based strategies. My analogy for this is if the ants are the workers for the queen(Network Admins), the Network Engineers are the strategic commanders that guide these ants. They basically design, build and optimize network infrastructures to meet objectives and growth required by the organization.

Specific Responsibilities according to Google and AI Search Engines:

- Design & Architecture
  - Design network topology and architecture
  - Plan network capacity and scalability
  - Select hardware/software solutions for projects
  - Create network diagrams and technical specifications
  - Design disaster recovery and redundancy solutions
- Implementation & Deployment
  - Configure complex routing protocols (BGP, OSPF, EIGRP)
  - Implement advanced switching (VLANs, STP, EtherChannel)
  - Deploy and optimize SD-WAN solutions
  - Implement network automation using scripts/tools
  - Lead network migration and upgrade projects
- Optimization & Performance
  - Analyze network traffic patterns and bottlenecks
  - Optimize network for specific applications (VoIP, video)
  - Conduct network performance testing and benchmarking
  - Implement Quality of Service (QoS) policies
  - Plan and execute network segmentation strategies
- Advanced Security
  - Design and implement security architectures
  - Configure advanced firewall policies and IDS/IPS
  - Implement zero-trust network access frameworks
  - Design and deploy network access control (NAC)
  - Conduct security assessments and penetration testing

In summary, Network admins focuses on the already existing infrastructures while Network Engineers focuses on new implementations and redesigns. One works for the short term while the other on the long term.