**Case Study: Secure Network Design for NALPAK's Raffles Place Office Expansion**

Kevin Del Rosario

Diploma in Information Technology, Kaplan Higher Education Institute

IT46 IDC: Introduction to Data Communications

Mr. Satish Kumar Sarraf

October 12, 2023

A new office for NALPAK staffed by HR professionals, sales consultants, and accounting experts is being planned to be established at Raffles Place. The goal is to build an effective and secure office network that can serve the many responsibilities that these employees have. The network's design and execution, including the selection of transmission medium, network hardware, IP address setup, DNS services, and network security, are covered in this study.

**Selection Of Transmission Media**

There are a few options for choosing a transmission media. Ethernet Cables (Twisted Pair Cables), Wi-Fi, Fiber-Optic Cables, and Coaxial Cables. All of these have their own advantages and disadvantages which depend on certain requirements such as scalability for future, budget proposed, and purpose of the business. One type of transmission media does not have the ability to provide all the solutions for networking within an office. Most often than not, small-operating businesses use a combination of transmission media. Also, the maximum number of personnel that will use the network is only 25. Taking that into consideration, I propose the use of the following combination: Wi-Fi and Ethernet Cables.

Wi-Fi and Twisted-Pair Cables is a great combination as it provides flexibility in terms of balance in latency connection; and when in need, Wi-Fi provides connection to Wi-Fi-enabled devices such as Printers, Smartphones, Scanners, etc. Furthermore, it is easy to work with, flexible, efficient, and fast (Panek, 2019). Twisted-Pair Cables, on the other hand, can be used to provide wired connection which has rapid and consistent transfer rate of data. This is a key requirement for devices and offices particularly HR, sales, and accounting functions. According to Dye et al. (2007), “Although wireless has advantages, there are some disadvantages to its use. A wireless connection is usually slower than a cable connection, and because the medium is open to anyone with a wireless receiver, it is more susceptible to security breaches than other media.” Taking that into consideration, Network Engineers of the company must be aware of these disadvantages to prevent any security breaches; and Maintenace of network security with up-to-date technology should be imposed in the company as failing to do so will have impacts on the company’s future.

Although there are other options such as coaxial cables and fiber-optic cables, they are not suitable for the needs of the office: complexity, scalability and cost-effectiveness. Panek (2019) study found the following:

In a LAN environment, each computer is connected to the network by way of a closed loop, which was historically done with coaxial cable. When it comes to today’s LANs, the use of coaxial cable has been deprecated. (p. 28)

Despite having the ability to deliver enormous bandwidth, coaxial cables are frequently connected to cable TV and high-speed internet. Due to their installation's complexity and expense, they are less ideal for local office network configurations. As a result, they are not thought to be the best option in this situation. Fiber optics are less practicable for a tiny office setting like NALPAK's due to their high installation costs and complexity. If the companies require long-distance connections with high bandwidth, they will often opt for Fiber optics.

**Networking Devices**

Several essential networking devices such as routers, switches, and firewalls are needed to set up a strong and effective office network for NALPAK's new office in Raffles Place. In addition to contributing to the network's overall operation and security, each device has a specialized function.

According to Panek (2019), “Routers also reside on the Network layer. Routers make connections between one or more IP networks. They are known as the gateway to another IP network, and you would utilize their IP address in the Gateway address fi eld of a computer’s IP Properties window, to allow the computer access through to other networks”. In the new Office, a human resources executive, sales consultant, and accounting manager can access external resources such as cloud-based applications and its website. Additionally, it ensures that data is securely routed between your office and external networks.

Ethernet switches are the basis for managing local network traffic. They play an important role in connecting and facilitating communication between devices within the office. Research by Dye et al. (2007) suggests that switches optimize data traffic, reduce latency, and improve network efficiency.

Network security is of paramount importance, especially when dealing with sensitive human or financial data. Firewalls act as important security components by filtering incoming and outgoing network traffic based on predefined rules. By implementing a firewall, NALPAK can protect its network from unauthorized access and potential threats, ensuring data confidentiality and integrity.

DNS and DHCP servers are important for efficient network management. Simplifies IP address management by dynamically assigning IP addresses to devices and resolving domain names to IP addresses. Dedicated DNS and DHCP servers are essential for a smooth and user-friendly experience, especially when accessing internal resources.

The primary network infrastructure can be wired, but they should consider deploying wireless access points. This option provides flexibility for mobile devices and guest access. Human resources managers, sales consultants, and accounting managers can use laptops or mobile devices and access points to securely connect to the network wirelessly.

Deploying network monitoring and management tools increases network visibility and enables IT teams to proactively identify and resolve network issues. This improves network performance and minimizes downtime (GeeksforGeeks, 2023).

In summary, the identified network devices are essential components for creating a secure, efficient and scalable network infrastructure for NALPAK's new office at Raffles Place. Together, these devices enable human resources managers, sales consultants, and accounting managers to work seamlessly, access external resources, and protect sensitive data.

**Network Address**

The network IP address provided for NALPAK's new office is 10.64.136.0/25. The Addresses above are derived from computing its counterparts. The first step is to identify the Network IP Address and Subnet Mask. The network information given is 10.64.136.105/25. This includes both the IP address (10.64.136.105) and the subnet mask (25 bits). The second step is to convert to binary using the division method. The subnet mask is /25, which means the first 25 bits are set to 1 in binary notation which represents the Network. The remaining 7 bits are set to 0 which is for the hosts. In binary, this looks like: 11111111.11111111.11111111.10000000

Based on this information, the following IP addresses can be derived according to the table below.

**Table 1**

*Assigning of Network Address for 10.64.136.0/25*

|  |  |  |
| --- | --- | --- |
|  | Binary | Decimal |
| Networking ID | 00001010.01000000.10001000.0**|**0000000 | 10.64.136.0/25 |
| First Assignable IP Address | 00001010.01000000.10001000.0**|**0000001 | 10.64.136.1 |
| Last Assignable IP Address | 00001010.01000000.10001000.0**|**1111110 | 10.64.136.126 |
| Broadcast IP Address | 00001010.01000000.10001000.0**|**1111111 | 10.64.136.127 |
| Range of IP Addresses | 00001010.01000000.10001000.0**|**0000001 to 00001010.01000000.10001000.0**|**1111110 | 10.64.136.1 to 10.64.136.126 |

**DNS Service**

Internet communication is made easier by the Domain Name System (DNS), which converts human-readable domain names (like www.nalpak.com) into IP addresses. A study by Panek (2019) shows that “Without this DNS server address, a client computer will not be able to connect by name to any resources on the Internet ". Software for DNS, such as BIND or Microsoft DNS Server, will be hosted on this server, which may be physical or virtual. Accessibility is ensured by integration with the network infrastructure. Testing ensures that the DNS system is working properly so that domain names can be resolved to IP addresses. Performance and security are continuously monitored and maintained, and updates are frequently made to preserve optimal performance and dependability.

**Network Security**

In today's digital landscape, computer network users face countless security threats that can jeopardize their data, privacy, and the overall integrity of their networks. Understanding these threats and employing effective prevention strategies is essential to maintaining strong cybersecurity. Below, we discuss five common cybersecurity threats and corresponding strategies to mitigate them.

According to Pfleeger and Margulies (2015), One of the most common threats in the digital realm is malware, a term that includes many different types of malwares such as viruses, worms, Trojans, and ransomware. Malware can infiltrate systems, compromise data integrity, disrupt network operations, or extort money from victims. Prevention strategies include deploying robust anti-virus and anti-malware solutions to detect and quarantine malicious files. Regularly updating all software, including operating systems and applications, with the latest security patches is essential to address known vulnerabilities. Additionally, it is essential to educate users about safe browsing practices, warning them not to download suspicious files or open attachments from unknown sources. Using web and email content filtering can help block potential sources of malware (Pfleeger & Margulies, 2015). Additionally, data should be backed up regularly to minimize the impact of ransomware attacks.

Phishing attacks involve fraudulent emails or websites designed to trick users into revealing sensitive information such as login credentials or even worse, financial data. Recognizing and mitigating these threats requires training users to identify phishing attempts. This includes being careful with unsolicited emails and verifying the authenticity of the sender's information. Web filtering can be deployed to block access to known phishing sites, reducing the risk of exposure. Multi-factor authentication (MFA) is a strong preventative measure that improves account security by requiring multiple forms of verification. Regular updates and patches to email clients and web browsers are essential to address known vulnerabilities that attackers can exploit.

Insider threats come from individuals within an organization, such as employees or contractors, who abuse their access privileges, whether intentionally or unintentionally. Just as the Roman poet Juvenal said, “Who watches the watchmen?”. Preventing insider threats requires implementing security measures such as the Principle of Least Privilege (PoLP), which limits user access to the minimum permissions required for their role. Comprehensive background checks and regular employee security training can minimize risks from insider threats. Continuous monitoring of user activities and network logs for unusual or suspicious behavior is important (Zaripova & Makhmudov, 2021). Clear and consistently applied security policies, combined with the other preventive methods mentioned before this, can significantly reduce the likelihood of insider threats.

Distributed denial of service (DDoS) attacks poses a significant threat to network availability by overwhelming servers or networks with excessive traffic (Pfleeger et al., 2015). These attacks can cause services to be unavailable to legitimate users. Preventing DDoS attacks involves deploying specialized DDoS mitigation solutions and services that can detect and filter malicious traffic (Eliyan & Di Pietro, 2021). Organizations can work with Internet Service Providers (ISPs) to redirect or absorb malicious traffic before it reaches their network. Additionally, deploying traffic monitoring tools and intrusion detection systems (IDS) can help quickly identify and respond to DDoS attacks. Developing and testing an incident response plan specific to DDoS attacks is essential to minimize downtime and maintain service availability.

Data theft and data breach threats involve unauthorized access to sensitive data, potentially leading to data breaches, identity theft, and financial loss. But studies showed that there is more to this, and it is much more complicated. In one of Pfleeger's et. al (2015) studies, “On average, the breached firms lost 2.1 percent of market value within two days of the breach’s disclosure, but security developers’ market value actually increased 1.36 percent.” To prevent these threats, organizations must employ strong access controls, including encryption and authentication mechanisms to protect data in transit and at rests. Training employees in data handling and security protocols is essential to prevent accidental data leaks. Additionally, organizations should invest in data loss prevention (DLP) solutions that can monitor and enforce data security policies, ensuring that sensitive information remains confidential and secure. Developing an incident response plan for a data breach is also important for quick and effective mitigation in the event of a security incident.

**Conclusion**

In summary, NALPAK can guarantee a robust, effective, and secure office network by carefully choosing transmission media, implementing necessary networking hardware, controlling IP addressing, optimizing DNS services, and giving network security top priority. The survey also emphasizes the significance of taking proactive steps to protect sensitive data as well as the persistent cybersecurity threats. Cybersecurity threats are ubiquitous in today's connected world, and effective prevention strategies are essential to protect computer networks and user data. A comprehensive approach that combines user education, strong security policies, and deployment of the right security technologies is essential to effectively mitigate these threats. In the end, a well-structured network infrastructure positions NALPAK for long-term success and growth by enhancing daily operations as well as fortifying the company against the changing challenges of the digital landscape.

**Bibliography**

Dye, M., McDonald, R. & Rufi, A. (2007). Network Fundamentals: CCNA Exploration Companion Guide. Cisco Press.

Pfleeger, C., Pfleeger, S. & Margulies, A. (2015). Security in Computing (5th ed.). Pearson.

Panek, C. (2019). Networking Fundamentals. Sybex.

Eliyan, F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2021.03.011

Zaripova, A. & Makhmudov, A. (2021). "Network Security Issues and Effective Protection Against Network Attacks." International Journal on Integrated Education, vol. 4, no. 2, 2021, pp. 79-85, https://doi:10.31149/ijie.v4i2.1204.

GeeksforGeeks. (2023b, May 15). Network devices (hub, repeater, Bridge, switch, router, gateways and Brouter). GeeksforGeeks. https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/