I believe **security protocols** should be the first thing on any network. Communication and management protocols are critical to achieve functionality and performance, but security is one of the cornerstones to ensure the trusts for data integrity, privacy and system reliance. In today's world, with attacks increasing in occurrence and levels of sophistication, securing your network infrastructure is no longer a choice: it's a necessity.

Security measures should help in protecting data at the time of transmission and storing period. And secure communication is made possible through protocols such as **SSL/TLS**, **IPSec** and **HTTPS**, which ensure messages being transmitted are encrypted and secured from unauthorized access. So, everything must work smoothly, whether the best ordered communication protocols, the most brilliant management technologies in the world, as data and information continue to be leaked. For example, without security standards, critical financial data or consumer information exchanged over the network becomes accessible to hackers and dangerous malware. This can lead to identity theft, financial loss, and harm to an organization's reputation (Stallings, 2020).

In contrast, communication protocols such as **TCP/IP** or **UDP** ensure that data is delivered between devices consistently and effectively. Management protocols like **SNMP** (Simple Network Management Protocol) assist monitor and control devices on the network. These are crucial, but they assume a secure environment to work correctly. Without effective security standards, these systems can be abused or disrupted. For instance, a weakly protected network might be brought down by a DDoS assault, making even the greatest communication and management protocols meaningless.

Security methods also help compliance with legal and business norms. For firms working with financial, health, or personal data, following to rules like **GDPR** or **HIPAA** is vital. These

standards mandate secure transfer and management of data. Implementing solid security policies from the start helps assure compliance and prevent large penalties or legal implications (Kim & Solomon, 2018).

From a practical viewpoint, I've seen how crucial security is even in academic institutions. During remote learning, institutions adopted secure VPNs and multi-factor authentication to protect access to instructional platforms and research data. Without these standards, systems might easily be hacked, affecting thousands of students and teachers.

That said, addressing security doesn't imply disregarding the other two areas. Communication and management protocols are still crucial for a network's performance and maintainability. But security gives the basis. If the network isn't secure, it cannot be trusted—no matter how fast or well-managed it is.

In conclusion, while all three protocol groups play vital roles, **security protocols must come first** when developing any network. They not only defend against threats but also ensure that the other systems may perform securely and effectively. By emphasizing security, we develop networks that are not just smart and efficient but also trustworthy and durable in the face of ever-evolving cyber dangers.

References:

Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning. https://www.amazon.com/Fundamentals-Information-Systems-Security-David/dp/128411645X

Stallings, W. (2020). *Data and Computer Communications* (11th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/data-and-computer-communications/P200000003353/9780137561704?srsltid=AfmBOooDCHPbGxmy-vJcbIPXP9FV-9-UIt64rrnA_LixqzbM9X1nJtwx

Wordcount: 460