Annotated Bibliography

Maxwell Stratford

February 4, 2026

References

[1] O. Bonaventure, Q. De Coninck, F. Duchêne, A. Gégo, M. Jadin, F. Michel, M. Piraux, C. Poncin, and O. Tilmans. Open educational resources for computer networking. *SIGCOMM Comput. Commun. Rev.*, 50(3):38–45, July 2020.

This article describes the new way in which colleges should be teaching a Computer Networking course and the importance of offering such course for future students. Most of the practical use of this paper is to reference larger scale free textbooks for each of the listed sections, making a pool of resources for students to use and learn from the listed authors. The paper also dives deeper into the overarching topics professors should be covering, such as Learning protocols by dissecting packets, running virtual labs, implementing a simple transport protocol, and much more.

[2] Pradeep Dogga, Rachee Singh, Suman Nath, Ravi Netravali, Jens Palsberg, and George Varghese. Software managed networks via coarsening. In *Proceedings of the 24th ACM Workshop on Hot Topics in Networks*, HotNets '25, page 201–209, New York, NY, USA, 2025. Association for Computing Machinery.

This paper introduces the concept of Software Managed Networks (SMN) as opposed to Software Defined Networks (SDN). It gives examples for the weaknesses of Siloed Network management (A practice where work is divided up by working on different TCP/IP layers) and how SDNs still do not allow for the best management of all layers. It continues into the deeper workings of SMNs via Coarsening (The idea of mapping complex data to a more compact and abstract representation that has approximately the same effect.)

[3] Sina Rostami, Tiago Heinrich, and Taha Albakour. Poster: An investigation into internet-facing router services. In *Proceedings of the 2024 ACM on Internet Measurement Conference*, IMC '24, page 775–776, New York, NY, USA, 2024. Association for Computing Machinery.

This paper dives into how unprotected at least 40of peoples routers are by having an open port for at least one type of outward services (SNMPv1 and

v2, HTTP, NTP, SSH, TELNET, FTP). These vulnerabilities and open ports need to be mitigated for secure personal networks. They focus on IPv4 address for this paper, but plan to re-examine current findings and look into the status of IPv6.