UPRIGHT PUBLICATIONS
https://upright.pub/index.php/ijrstp/

Original Contribution

Networking Alchemy: Demystifying the Magic behind Seamless Digital Connectivity

Swathi Kaluvakuri[1], Karu Lal[2]

Keywords: Cloud Networking, Network Topologies, Protocols, IPv4 and IPv6, DNS and DHCP, Network Management

International Journal of Reciprocal Symmetry and Theoretical Physics

Vol. 4, Issue 1, 2017 [Pages 20-28]

Computer networking is essential to the operation of the internet and other forms of communication and data transfer made possible in today's digitally interconnected world. This article aims to unravel the complexities of computer networking in a clear and approachable manner. This in-depth article dives into the underlying ideas behind computer networking, including subjects such as the OSI model, TCP/IP protocols, network topologies, and routing; it elucidates the functions of various network equipment, including routers, switches, and firewalls, and describes how these devices work together to ensure the uninterrupted delivery of data. In addition, this study investigates contemporary developments and technologies in the realm of networking, including virtualization, cloud computing, and the Internet of Things (IoT). In this article, the readers will learn about best practices for network security, troubleshooting approaches, and performance optimization measures. Whether we're a novice looking to grasp the basics or a seasoned professional seeking a refresher, this article offers valuable insights to help you navigate the intricacies of computer networking. It demystifies the networking world with concise explanations and practical examples, making it accessible to a wide range of readers.

INTRODUCTION

In an age characterized by digital transformation and global connectedness, the unseen force that drives our daily lives is the computer networking that connects all our devices. Computer networking makes activities like sending an email, streaming a movie, doing online business transactions, and even reading this article possible. Whether we send an email, stream a movie, conduct online business transactions, or even read this article, it is true. However, the complexities of this technological marvel are still a mystery to many people because of the language that surrounds it.

The purpose of the paper "Demystifying Computer Networking: A Comprehensive Guide" is to demystify the complexity of computer networking by providing a transparent and user-friendly entry point into the convoluted world of technology. Understanding the principles of computer networking is no longer just the purview of those with professional training in information technology today when our world is intimately linked by networks that span the globe (Lal, 2015). It is a crucial talent for people interested in pursuing employment in the technology industry, from software development to cybersecurity, and it is a necessary ability for the informed citizen.

This all-encompassing tutorial will take us on a journey to demystify the world of computer networking, beginning with the fundamentals and moving on to more sophisticated ideas as the

[1] Department of Computer Science, Southern Illinois University Carbondale, Carbondale, Illinois, USA
[2] Integration Engineer, Ohio National Financial Services, USA (karu.lal84@gmail.com)

voyage progresses. We will get an appreciation for the underlying infrastructure that makes it all possible as soon as the data leaves our device and begins its journey through the enormous expanse of the internet. In the first step of this process, we will analyze the OSI model, a basic framework for comprehending how data is packaged and sent over networks. To explain how data moves across the web, the TCP/IP protocols, the fundamental building blocks of internet communication, are broken down. We will learn about the many network topologies that define the architecture of these complex systems, as well as the function that crucial networking equipment such as routers, switches, and firewalls play in ensuring that data transit is performed without a hitch.

We investigate the most recent networking trends and emerging technologies, such as virtualization, cloud computing, and the Internet of Things (IoT). This is because technology is constantly developing and changing. We will also learn about the critically important topic of network security, which will equip us with the knowledge necessary to protect information and devices in a world that is becoming increasingly connected. We hope that by the time we have finished reading this guide, we can confidently make decisions about networking solutions, efficiently maintain network infrastructure, and successfully navigate the ever-changing computer networking environment. Let's take this adventure together and, along the way, unravel some of the mysteries surrounding the intriguing world of computer networking.

BASICS OF COMPUTER NETWORKING

The foundation of our modern digital world comprises interconnected computer networks. It is what makes it possible for different devices to talk to one another, share information, and access the immense resources of the internet. Understanding this complex technology is necessary to have a firm grip on the fundamental principles and components that support computer networking.

Computer Networking

The fundamental aspect of computer networking is linking many computing devices to ease the flow of information and facilitate communication. This can range from something as simple as a local area network (LAN) connecting a few devices in a home or office to something as complex as the internet, a worldwide network of networks (Lal, 2016). Computer networking facilitates the flow of data between devices, such as files, communications, and media, regardless of the location of those devices in the actual world.

The OSI Model: A Layered Approach

Understanding how data is transported via a network can be simplified using the Open Systems Interconnection (OSI) model, which provides a systematic framework. It comprises seven levels, each accountable for a specific activity within the communication process. The following is the order of these strata, starting at the top:

- **Application Layer:** is the part of the stack that manages end-user services like web browsers, email clients, and file transfer programs.
- **Presentation Layer:** It is in charge of encrypting, compressing, and translating data, and its primary function is to ensure that data transmitted from one system can be read and understood by another.
- **Session Layer:** The session layer is responsible for the management and control of communication sessions that take place between devices.
- **Transport Layer:** This layer ensures reliable communication and data flow from beginning to finish by performing functions such as error checking and flow control. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are notable examples of protocols operating at this level.
- **Network Layer:** Data is routed and forwarded between devices under the control of the network layer, which also determines the most efficient path for the data to take. The Internet Protocol, sometimes known as IP, is a crucial protocol used in this layer.
- **Data Link Layer:** is in charge of the data's physical addressing and deals with transmitting data frames between physically connected devices. Direct connections are typically made via Ethernet or Wi-Fi.
- **Physical Layer:** The hardware layer deals with the physical media and transferring raw bits over the network through cables or wireless signals. It is also known as the lowest layer (Lin et al., 2012).

IP Addresses and MAC Addresses

Devices require individual IDs to communicate over a network successfully. IP addresses, which stand for "Internet Protocol," and MAC addresses for "Media Access Control," are two critical identifiers. On the internet, devices each have what is known as an IP address, which is analogous to a street address. They are essential to routing data and might be either public or private. On the other hand, media access control addresses, or MAC addresses, are one-of-a-kind hardware addresses connected to every network interface card, or NIC (Thaduri et al., 2016). They play a role in the communication that takes place at the data link layer of the network.

Routers and Switches

Routers and switches are two of the most essential equipment in computer networking.

- **Routers:** Routers are devices that connect separate networks and determine the path that data should take based on the IP addresses of the devices it comes from. They make it possible for devices connected to separate networks, such as our home network and the internet, to communicate with one another. To protect a network, routers typically come equipped with firewall features.
- **Switches:** Switches connect devices that are part of the same network. They function at the data connection layer of the networking stack. They identify where within a local network to transfer data by using MAC addresses, which makes communication within a local network more effective overall.

Protocols: The Language of Networking

Data transfer over a network is governed by a set of rules and conventions known as protocols. Protocols are a set of rules and conventions. They ensure that different devices can communicate with one another. The following are examples of standard network protocols:

- **TCP (Transmission Control Protocol)** is an abbreviation for "Transmission Control Protocol." Communication that is both dependable and connection-oriented is provided via TCP. It guarantees that the data will be delivered successfully and in the appropriate sequence.
- **UDP (User Datagram Protocol):** UDP is a connectionless protocol that, while it is faster, does not offer any guarantees on the delivery of data or the sequence in which it will be delivered.
- **HTTP (Hypertext Transfer Protocol):** On the World Wide Web, the movement of web pages and data is handled with the help of HTTP.
- **FTP (File Transfer Protocol):** File transmission Protocol, or FTP, is a protocol that allows users to share data between computers.
- **SMTP (Simple Mail Transfer Protocol):** The protocol is utilized while sending email messages.

Network Topologies

The configuration of the various devices that make up a network is called its topology. Typical topologies include the following:

- **Bus Topology:** Refers to a network architecture in which all of the devices are linked together by a single "bus."
- **Star Topology:** Devices are connected to a central hub or switch in a star topology, also known as a star topology.
- **Ring Topology:** Devices are connected in a ring-like pattern in a topology known as ring topology.
- **Mesh Topology**: A high level of reliability is achieved through the intricate and redundant interconnection of the many devices.

Depending on several parameters, including scalability, fault tolerance, and cost, each topology has both advantages and disadvantages that are unique to it. Learning these fundamentals of computer networking is essential for anyone who wants to efficiently navigate the digital landscape, whether for their usage or as part of a professional IT job (Dekkati et al., 2016). Because it serves as the basis upon which more complex networking ideas and technologies are developed, a solid understanding of it is necessary in today's technology-driven world.

NETWORKING COMPONENTS

Computer networks rely on various components operating in concert to support data exchange and connectivity. Anyone who wants to set up, manage, or debug networks, whether at home, in an office, or across the great expanse of the internet, has to have a solid understanding of these networking components. We'll examine these essential components (Shariat et al., 2017).

Network Devices

The physical components that come together to make up the infrastructure of a network are referred to as "network devices." They are as follows:

- **Routers:** Routers are devices that connect various networks to the internet. One example of this is a local area network (LAN). They rely on routing tables to determine where information should be transmitted, which is determined by the IP addresses of the destinations. Routers typically include a firewall and other security mechanisms to prevent unauthorized users from accessing the networks they serve.
- **Switches** connect several devices in the same network, most commonly a local area network (LAN). They function at the data link layer, which corresponds to Layer 2 of the OSI model, and they make use of MAC addresses to decide where within the local network data should be routed. Switches are necessary for establishing effective and rapid connections inside a local area network.
- **Access Points (APs):** Access points are essential components of any network that seeks to expand its wireless coverage. They enable mobile devices such as laptops, cellphones, and tablets to connect to the network wirelessly. Access points are frequently incorporated into wireless routers as a part of their design.
- **Firewalls:** It is only possible to have adequate network security with firewalls. They examine and control every traffic entering into and going out of the network based on the security rules that have been specified. Firewalls are an effective means of preventing harmful behavior and restricting unauthorized access to a network.
- **Modems:** The transmission of digital data across analog communication lines, such as telephone lines or cable systems, requires modems, which are devices that can modulate and demodulate digital data. In most cases, they are utilized to establish a connection to the internet.

Network Cables and Wireless Connectivity

The use of both wired and wireless connections is required for networking.

- **Ethernet Cables:** The most frequent cable type for wired connections is Ethernet cables, such as Cat5e and Cat6. They are appropriate for local area networks (LANs) and direct connections between different devices since they offer dependable and quick connections.
- **Fiber Optic Cables:** Data can be transmitted over fiber optic cables using light, which results in fast data transfer rates. Wide area networks (WANs) frequently use them because of their high-speed, long-distance connection capacity.
- **Wireless Connections:** Radio transmissions are used as the medium for communication in wireless networking. This comprises cellular networks for mobile devices and Wi-Fi for establishing local wireless connections. Wireless networking components include wireless routers, access points, and wireless adapters within individual devices (Prasad & Anusha, 2017).

Network Protocols

Data transmission and reception over a network are governed by a set of rules and conventions known as network protocols. They ensure that different electronic gadgets can comprehend and communicate with one another. The following are some essential network protocols:

- **TCP (Transmission Control Protocol):** The Transmission Control Protocol (TCP) is a connection-oriented protocol that ensures the reliable delivery of data by establishing a connection, checking for errors, and retransmitting data if necessary.
- **UDP (User Datagram Protocol):** UDP is a connectionless protocol that transfers data faster than TCP but does not guarantee that the data will be transmitted reliably. Real-time applications, such as online gaming and video conferencing, are frequent users of this technology.
- **IP (Internet Protocol):** addresses are used to identify each device connected to a network. IPv4, which has a bit size of 32, and IPv6, which has a bit size of 128, are the two primary versions of the Internet Protocol.
- **HTTP (Hypertext Transfer Protocol):** On the World Wide Web, the movement of web pages and data is handled with the help of HTTP. The use of HTTP is required to visit websites.
- **FTP (File Transfer Protocol):** File transmission Protocol, or FTP, is a protocol that allows users to share data between computers.
- **SMTP (Simple Mail Transfer Protocol):** This protocol is utilized while sending email messages.

Networking Services

The capabilities of a network can be expanded through the use of various software programs and features that are known as network services. Standalone servers can deliver these services or be incorporated into existing networking hardware.

- **DNS (Domain Name System):** DNS is a service that converts domain names that are readable by humans, such as "www.example.com," into their corresponding IP addresses. Users can access websites and other resources by name rather than by entering a numerical IP address. This is made possible by a service.
- **DHCP (Dynamic Host Configuration Protocol):** When devices connect to a network, DHCP is the service that is responsible for automatically assigning IP addresses, subnet masks, and other settings related to the configuration of the network to those devices. Administration of the network is made more accessible as a result.
- **NAT (Network Address Translation):** Network address translation is a method that maps several private IP addresses to a single public IP address. It is frequently used in home networks to facilitate the sharing of a single public IP address among several devices (Kumar et al., 2017).
- **Proxy Servers**: Clients and the internet are connected through proxy servers, which act as go-betweens. They are valuable for network services because they provide increased security, caching, and content screening.

Network Security Components

Network security is an essential component of networking, and many aspects play a part in ensuring that data and communications are kept secure while maintaining their integrity.

- **Firewalls:** Firewalls filter both incoming and outgoing network traffic depending on the security rules that have been set. They safeguard the system against illegal access and traffic that could be damaging.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** IDS and IPS systems analyze the traffic on a network in search of indications of malicious or suspicious behavior. They can provide notifications to administrators or take action to stop or prevent potential dangers.
- **Virtual Private Networks (VPNs):** VPNs, or virtual private networks, protect data while it is being transmitted over public networks like the internet by creating encrypted secure tunnels. Remote access and encrypted communication are two common uses for these technologies.
- **Antivirus and Antimalware Software:** These software solutions remove dangerous malware as well as identify it, thereby protecting networks and devices.

Client Devices

End-user devices, which might include computers, smartphones, tablets, and other gadgets connected to the Internet of Things (IoT), are critical elements that make up a network. These devices establish a connection to the network to access the resources and services provided by the network.

Servers

Servers are specialized computers that offer services and resources to client devices. Client devices connect to servers via a network. Web servers, email servers, file servers, and database servers are all examples of what can be included in this category. Most of the time, servers are assigned static IP addresses and are set up to run a particular set of apps.

Understanding these networking components' interaction is essential for building and operating reliable, secure, and efficient networks. These components are the fundamental building blocks of modern networking, and they are necessary to have on hand whether we are setting up a Wi-Fi network in our house or working in an intricate business setting.

NETWORK DESIGN AND ARCHITECTURE

Network design and architecture are essential for a dependable, efficient, secure computer network. A well-planned network can boost productivity, data integrity, and performance. This overview will cover computer network design and architecture basics (Shanmugam et al., 2016).

Network Design vs. Architecture

Although commonly used interchangeably, these phrases refer to various network planning and implementation characteristics.

- **Network Design:** Network design determines device connectivity and data flow by logically and physically arranging the network. This covers topology, addressing, routing, and security decisions. Scalability and future adaptability are considered in network design.
- **Network Architecture:** Network architecture is the framework and ideas that guide network design. High-level strategy, technological choices, and standards affect network component design and integration.

Critical Considerations in Network Design

Understanding an organization's needs and goals is essential to network design. Several factors influence decision-making:

- **Scalability:** A network should expand and adapt to the organization's needs. Scalability depends on user and device numbers, data volume, and expansion plans.
- **Performance:** Effective data transfer requires network performance. Bandwidth, latency, and throughput affect data transmission speed and reliability.
- **Redundancy:** Network designers use redundancy to maximize availability and minimize downtime. If something fails, redundant components and pathways take over.
- **Security:** Network security is crucial. Firewalls, intrusion detection, encryption, and secure authentication are used.
- **Quality of Service (QoS):** Methods prioritize network traffic to ensure vital applications have enough capacity and minimal latency.
- **Cost-Effectiveness:** Performance, security, and money must be considered in network architecture. Designers should seek for cost-effective, organization-specific solutions.

Network topology

A network's topology is its physical and logical arrangement of devices and connections. Common topologies have pros and cons:

- **Star Topology**: Star topologies connect devices to a hub or switch. Setting it up and managing it is simple, and a device failure doesn't affect the network. It relies mainly on the central hub, which can collapse.
- **Bus Topology:** A central wire connects devices in a bus topology. Simple and cheap, yet challenging to diagnose, and failures can interrupt the network.
- **Ring Topology:** In a ring topology, devices are connected circularly. Data travels through the ring to its destination. It's efficient, but one device failure can disrupt the network (Bakhshi, 2017).
- **Mesh Topology:** Mesh topologies are highly connected. Partial mesh topologies have some redundancy, while full mesh topologies have total redundancy and excellent availability. Strong mesh networks are difficult and expensive to set up.
- **Hybrid Topology:** Many real-world networks balance pros and cons with diverse topologies. A central bus may connect numerous star topologies in a star-bus hybrid.

Network Addressing

Network devices receive unique identifiers through network addressing. Most people utilize two handling systems:

- **IPv4 (Internet Protocol version 4):** 32-bit IPv4 addresses are four sets of three-digit numbers (192.168.1.1). However, IPv4 address exhaustion prompted IPv6 development and adoption.
- **IPv6 (Internet Protocol version 6):** IPv6 employs hexadecimal 128-bit addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334) . IPv6 has a much bigger address space and is needed to support more internet devices (Hilas & Politis, 2014).

Network Protocols

Data communication is governed by rules and conventions defined by network protocols. The following are essential protocols:

- **TCP (Transmission Control Protocol):** TCP is a connection-oriented protocol that enables reliable data transfer by establishing connections, error-checking, and retransmitting if necessary. TCP is connection-oriented and ensures reliable data transfer by establishing connections.
- **UDP (User Datagram Protocol):** while it is faster than TCP and does not require a connection, it does not ensure reliable data transport. Applications that operate in real-time frequently make use of it.
- **HTTP (Hypertext Transfer Protocol):** Hypertext Transfer Protocol is the protocol that allows web pages and data to be transferred across the World Wide Web.

- **FTP (File Transfer Protocol):** File Transfer Protocol is a protocol that allows users to move data from one computer to another.
- **SMTP (Simple Mail Transfer Protocol):** Simple Mail Transfer Protocol is the protocol that is utilized while delivering email messages.

Network Security

The importance of network security in design and architecture cannot be overstated. It involves using techniques and technology to secure data and devices from unauthorized access and potential dangers. The following are essential components:

- **Firewalls:** Firewalls protect against malicious activity and unauthorized access by filtering network traffic based on security rules. Firewalls are also known as intrusion prevention systems.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** IDS and IPS systems monitor network traffic for suspicious or malicious activity signals, delivering alerts or taking action to block or avoid potential threats. IDS and IPS systems are also known as intrusion detection and prevention systems.
- **Virtual Private Networks (VPNs):** VPNs are designed to protect data while it is being transmitted over public networks by creating encrypted secure tunnels.
- **Antivirus and Antimalware Software:** Antivirus and antimalware software detect and eliminate dangerous software from computers, mobile devices, and network systems.
- **Authentication and Access Control:** Role-based access helps ensure that only authorized users can access network resources. Authentication and Access Control (Rawat et al., 2017).

Implementation/Management

Implementing and managing a network design is required. This involves:

- Configuring routers, switches, and firewalls.
- Setting up DNS, DHCP, and VPNs.
- Continuous monitoring and maintenance for performance and security.
- Regular patches to fix vulnerabilities and enhance network performance.

WIRED AND WIRELESS NETWORKING

In this day and age, there are two unique but complementary ways to link devices, and those ways are wired networking and wireless networking. Each one has certain advantages as well as drawbacks, which enables them to be utilized in a variety of settings and applications. It is essential to have a solid understanding of the distinctions between the two to make educated judgments regarding the design and execution of a network.

Wired Networking

As its name suggests, wired networking entails physically connecting various devices through cables or other wired infrastructure. It is well-known for its consistency, reliability, and fast data transfer speeds. The following are some essential elements of wired networking:

- **Ethernet Cables:** For wired connections, the most common type of cable utilized are Ethernet cables such as Cat5e and Cat6. They provide dependable and fast connections and are appropriate for local area networks (LANs) and direct connections between devices. They have a high bandwidth, minimal latency, and are immune to any possible wireless interference.
- **Fiber Optic Cables:** Compared to Ethernet cables made of copper, which carry data via electrical current, the data transmission rates offered by fiber optic cables are far higher. Wide area networks (WANs) frequently use them because of their high-speed, long-distance connection capacity.
- **Stability and Reliability:** Because they are less prone to interference from the surrounding environment and signal degradation, wired connections are ideally suited when stability is paramount.
- **Security**: Wired connections are intrinsically more secure than wireless connections because they are less likely to be intercepted for eavesdropping. Wireless connections can be blocked more readily.
- **Limited Mobility:** The most significant disadvantage of wired networking is that it limits the mobility of devices because devices are physically connected to the network through cables. In circumstances that call for flexibility and movement, this restriction might be a severe impediment and work against us (Harris et al., 2014).

Wireless Networking

Wireless networking, on the other hand, enables users to move around freely and is widely used in today's mobile devices, including laptops, smartphones, and other Internet of Things devices. The following is a list of essential aspects of wireless networking:

- **Wi-Fi:** The most widespread type of wireless networking is known as Wi-Fi, and it enables electronic devices to connect to a network without physical connections. It uses radio frequencies as its operation mode, allowing the users to move around freely.
- **Mobility:** Wireless networks are the best option in situations when the mobility of the connected device is of the utmost importance, such as in homes, offices, public spaces, and surroundings that are outdoors. Users can move about unrestrictedly while still maintaining their connection to the network.
- **Easy Installation:** In most cases, installing a wired infrastructure is more complex and time-consuming than setting up a wireless network. Wireless LAN routers and access points can be set up without wires in a concise amount of time.
- **Scalability:** Due to the ease with which they may be expanded, wireless networks are well suited for settings where the number of devices connected to the network may fluctuate often (Ou et al., 2013).
- **Interference and Security Challenges:** Interference, signal degradation, and potential security flaws are more likely to affect wireless networks because of their decentralized nature. Encryption and other security measures are essential to prevent unauthorized access to wireless connections.

Hybrid Networks

The benefits of wired and wireless networking are often combined to take full use of all these technologies offer. Both individuals and businesses do this. Flexibility, reliability, and scalability are all made possible by utilizing this hybrid method. On the other hand, Wi-Fi provides mobile connectivity for laptops and other mobile devices. A wired network may provide a stable backbone in an office, while Wi-Fi could be used instead.

CONCLUSION

Our lives are becoming increasingly digital, and the world of computer networking is the unseen web that holds it all together. As we draw to a close on this examination of computer networking, it is becoming abundantly evident that technology plays an essential part in today's interconnected world. We have set out on a trip through the fundamental principles, network components, and network design considerations that drive this technology, and we are currently in the midst of that adventure. Computer networking, whether wired or wireless, local or global, is the backbone of modern communication. It enables data to travel over great distances and makes global connectedness feasible. We have arrived at an understanding of the significance of addresses, protocols, and security measures in maintaining the privacy and integrity of data. As we end our conversation, it is vital to remember that computer networking is continuously changing. The terrain is constantly being reshaped due to new technologies and problems. Maintaining constant awareness, adaptability, and vigilance about security is more important than ever. In a world where telecommuting, online teamwork, and the Internet of Things are becoming more commonplace, computer networking continues to push the frontiers of what is technically feasible. Individuals and organizations can unlock the full potential of this technology by embracing it and gaining a knowledge of its subtleties. This will help to stimulate creativity, communication, and advancement on a global scale. As a result, as we say goodbye to this exploration, we look forward to the exciting new advances and challenges the constantly developing world of computer networking offers.

REFERENCES

Bakhshi, T. (2017). State of the Art and Recent Research Advances in Software Defined Networking. *Wireless Communications & Mobile Computing (Online)*, *2017*. https://doi.org/10.1155/2017/7191647

Dekkati, S., Thaduri, U. R., & Lal, K. (2016). Business Value of Digitization: Curse or Blessing?. *Global Disclosure of Economics and Business*, *5*(2), 133-138. https://doi.org/10.18034/gdeb.v5i2.702

Harris, S. E., Kurpius, R., Sharon, E. (2014). Social Networking and Professional Ethics: Client Searches, Informed Consent, and Disclosure. *Professional Psychology: Research and Practice*, *45*(1), 11-19. https://doi.org/10.1037/a0033478

Hilas, C. S., Politis, A. (2014). Motivating Students' Participation in a Computer Networks Course by Means of Magic, Drama and Games. *SpringerPlus*, *3*(1), 1-12. https://doi.org/10.1186/2193-1801-3-362

Kumar, P., Dutta, R., Dagdi, R., Sooda, K., Naik, A. (2017). A Programmable and Managed Software Defined Network. *International Journal of Computer Network and Information Security*, *10*(12), 11. https://doi.org/10.5815/ijcnis.2017.12.02

Lal, K. (2015). How Does Cloud Infrastructure Work?. *Asia Pacific Journal of Energy and Environment*, *2*(2), 61-64. https://doi.org/10.18034/apjee.v2i2.697

Lal, K. (2016). Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs. *American Journal of Trade and Policy*, *3*(3), 121–126. https://doi.org/10.18034/ajtp.v3i3.663

Lin, S-s., Hung, M-h., Tsai, C-l., Chou, L-p. (2012). Development of an Ease-of-Use Remote Healthcare System Architecture Using RFID and Networking Technologies. *Journal of Medical Systems*, *36*(6), 3605-19. https://doi.org/10.1007/s10916-012-9836-0

Ou, C. X., Sia, Ling, C., Hui, C. K. (2013). Computer-Mediated Communication and Social Networking Tools at Work. *Information Technology & People*, *26*(2), 172-190. https://doi.org/10.1108/ITP-04-2013-0067

Prasad, K. L., Anusha, P. (2017). Implementing Preserved Access of Cloud Networking. *i-manager's Journal on Cloud Computing*, *4*(1), 8-14. https://doi.org/10.26634/jcc.4.1.13753

Rawat, D. B., Song, M., Xin, C. (2017). Advances on Software Defined Wireless Networking. *EAI Endorsed Transactions on Wireless Spectrum*, *3*(11). https://doi.org/10.4108/eai.9-1-2017.152095

Shamugam, V., Murray, I., Leong, J. A., Sidhu, A. S. (2016). Software Defined Networking Challenges and Future Direction: A Case Study of Implementing SDN Features on OpenStack Private Cloud. *IOP Conference Series. Materials Science and Engineering*, *121*(1), https://doi.org/10.1088/1757-899X/121/1/012003

Shariat, Z., Movaghar, A., Hoseinzadeh, M. (2017). A Learning Automata and Clustering-Based Routing Protocol for Named Data Networking. *Telecommunication Systems*, *65*(1), 9-29. https://doi.org/10.1007/s11235-016-0209-8

Thaduri, U. R., Ballamudi, V. K. R., Dekkati, S., & Mandapuram, M. (2016). Making the Cloud Adoption Decisions: Gaining Advantages from Taking an Integrated Approach. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *3*, 11–16. https://upright.pub/index.php/ijrstp/article/view/77

--0--