books kim
book summaries for easy reading

Computer Networks

ndrew S. Tanenbaum, David J. Wetherall

Book summary & main ideas

MP3 version available on www.books.kim
Please feel free to copy & share this abstract

Summary:

Computer Networks by Andrew S. Tanenbaum and David J. Wetherall is a comprehensive guide to the fundamentals of computer networks, from basic concepts to advanced topics such as network security and distributed systems. The book covers all aspects of networking, including hardware, software, protocols, applications, and management issues. It also provides an overview of current trends in networking technology.

The first part of the book introduces fundamental concepts such as data transmission techniques, communication media types (wired/wireless), topologies (star/bus/ring), addressing schemes

(IPv4/IPv6) and routing algorithms (distance vector/link state). It then moves on to discuss more complex topics such as network architectures (OSI model), transport layer protocols (TCP/UDP) and application layer protocols (HTTP/FTP).

The second part focuses on network security issues such as authentication methods, encryption algorithms and firewalls. It also discusses various tools for monitoring networks including intrusion detection systems and packet sniffers. Finally it looks at distributed systems which are used for large-scale computing tasks.

The third part examines emerging technologies in networking such as wireless LANs, mobile IP networks and peer-to-peer networks. It also explores how these technologies can be used to create new services or improve existing

ones.

Overall Computer Networks is an excellent resource for anyone interested in learning about computer networks or keeping up with the latest developments in this field.</

Main ideas:

#1. Network Architecture: Network architecture is the design of a computer network, which includes the hardware, software, protocols, and media used to connect computers and other devices. (This book provides an overview of the different types of network architectures, including client-server, peer-to-peer, and distributed systems.)

Network architecture is the design of a computer network, which includes the hardware, software, protocols, and media used to connect computers and other

devices. It is important for organizations to have an effective network architecture in order to ensure that their networks are secure and efficient. There are several different types of network architectures available today, each with its own advantages and disadvantages.

The most common type of network architecture is client-server. In this model, one or more servers provide services such as file storage or web hosting to multiple clients connected over a local area network (LAN). This type of architecture allows for centralized control over resources while still providing users with access from any location.

Peer-to-peer networks also exist where all nodes on the network can communicate directly with each other without relying on a central server. This type of architecture has become increasingly popular due to its

scalability and flexibility; however it does not offer the same level of security as client-server networks.

Finally, distributed systems use multiple computers located in different locations that work together as part of a single system. These systems allow for greater scalability than either client-server or peer-to-peer models but require more complex management tools.

#2. Network Protocols: Network protocols are the rules and conventions that govern how computers communicate with each other over a network. (This book covers the most commonly used protocols, such as TCP/IP, Ethernet, and Wi-Fi, as well as newer protocols such as IPv6 and Bluetooth.)

Network protocols are the rules and

conventions that govern how computers communicate with each other over a network. These protocols define the format of data packets, as well as how they should be sent, received, and processed. They also specify which type of hardware is required for communication to take place. Commonly used network protocols include TCP/IP, Ethernet, Wi-Fi, IPv6 and Bluetooth.

TCP/IP (Transmission Control Protocol / Internet Protocol) is one of the most widely used networking protocols in existence today. It provides reliable end-to-end communication between two or more computers on a network by breaking down messages into smaller chunks called "packets" that can be routed through different paths across the internet.

Ethernet is another popular protocol that enables high speed local area networks (LANs). It uses cables to connect multiple devices together so they can share

resources such as printers or files.
Wi-Fi is a wireless networking technology based on IEEE 802.11 standards that allows users to access the internet without having to use physical cables or wires.
IPv6 (Internet Protocol version 6) is an upgrade from its predecessor IPv4 and offers improved security features along with larger address space for better scalability when connecting large numbers of devices over a single network.
Finally, Bluetooth is a short range wireless technology designed primarily for exchanging data between two compatible devices within close proximity of each other such as mobile phones or laptops.
By understanding these various types of network protocols it becomes easier to troubleshoot any issues related to computer networks.</p

#3. Network Security: Network security is the practice of protecting a

network from unauthorized access and malicious attacks. (This book provides an overview of the different types of security measures, such as firewalls, encryption, and authentication, as well as how to detect and respond to security threats.)

Network security is the practice of protecting a network from unauthorized access and malicious attacks. It involves implementing measures such as firewalls, encryption, authentication, and intrusion detection systems to protect networks from external threats. Firewalls are used to block unwanted traffic from entering or leaving a network while encryption ensures that data sent over the network remains secure. Authentication requires users to prove their identity before they can gain access to the system, while intrusion detection systems monitor for suspicious activity on the network.

In addition to these technical measures, organizations should also have policies in place that define acceptable use of their networks and outline procedures for responding to security incidents. These policies should be regularly reviewed and updated as needed in order to ensure that they remain effective against new threats.

#4. Network Performance: Network performance is the measure of how well a network is able to deliver data from one point to another. (This book covers topics such as bandwidth, latency, throughput, and Quality of Service, as well as how to measure and improve network performance.)

Network performance is an important factor in the success of any network. It measures how well a network can deliver data from one point to another, and it

encompasses many different aspects such as bandwidth, latency, throughput, and Quality of Service (QoS). Bandwidth refers to the maximum amount of data that can be transferred over a given period of time; latency is the delay between when a packet is sent and when it arrives at its destination; throughput is the rate at which packets are successfully delivered; and QoS determines how much priority each type of traffic has on the network. Measuring these metrics helps administrators identify areas where improvements need to be made in order for their networks to perform optimally.

In addition to measuring network performance, there are also ways to improve it. This includes optimizing routing protocols so that they take advantage of available resources more efficiently, using caching techniques like content delivery networks (CDNs) or proxy servers for

faster access times, implementing quality-of-service policies for prioritizing certain types of traffic over others, upgrading hardware components like routers or switches with higher capacity models if needed, and ensuring that all devices connected to the network have up-to-date software installed.

Computer Networks by Andrew S. Tanenbaum and David J. Wetherall provides comprehensive coverage on topics related to networking performance including measurement methods as well as strategies for improving it. With this book readers will gain valuable insight into what makes a successful computer network.

#5. Network Topology: Network topology is the physical or logical arrangement of the nodes in a network. (This book covers the different types of

topologies, such as bus, star, and mesh, as well as how to design and configure a network topology.)

Network topology is an important concept in computer networking. It refers to the physical or logical arrangement of nodes in a network, and how they are connected together. Different types of topologies exist, such as bus, star, and mesh networks. Each type has its own advantages and disadvantages depending on the application.

Designing a network topology requires careful consideration of factors such as cost, scalability, reliability, security and performance. The choice of which type to use depends on the specific requirements for each individual situation. For example, if cost is a major factor then a bus network may be more suitable than a star or mesh configuration.

The book Computer Networks by Andrew S Tanenbaum and David J Wetherall covers all aspects of designing and configuring different types of network topologies in detail. It provides readers with an understanding of how these different configurations work so that they can make informed decisions when setting up their own networks.

#6. Network Routing: Network routing is the process of selecting the best path for data to travel from one node to another. (This book covers the different types of routing algorithms, such as distance vector and link state, as well as how to configure and troubleshoot routing protocols.)

Network routing is an essential part of any computer network. It involves selecting the best path for data to travel from one node

to another, and it can be done using a variety of different algorithms. Distance vector routing algorithms use information about the distance between nodes in order to determine the best route for data packets. Link state routing algorithms use information about the links between nodes in order to determine which paths are available and how long they will take. Both types of algorithms have their advantages and disadvantages, so it is important to understand them both before deciding which one is right for your network.

Configuring and troubleshooting routing protocols can also be challenging. Different routers may require different configurations, depending on their capabilities and settings. Troubleshooting issues with routes or connections can also be difficult if you dont know what youre looking for or how to interpret error messages correctly.

The book Computer Networks by Andrew S Tanenbaum and David J Wetherall covers all aspects of network routing in detail, including different types of routing algorithms, configuration techniques, as well as troubleshooting tips.

#7. Network Addressing: Network addressing is the process of assigning IP addresses to devices on a network. (This book covers the different types of IP addressing, such as static and dynamic, as well as how to configure and troubleshoot IP addresses.)

Network addressing is an essential part of any computer network. It involves assigning IP addresses to devices on a network so that they can communicate with each other. This process is necessary for the proper functioning of a network, as it allows different devices to identify and

locate one another in order to exchange data.

The book Computer Networks by Andrew S. Tanenbaum and David J. Wetherall covers the various types of IP addressing, such as static and dynamic, as well as how to configure and troubleshoot them. Static IP addresses are assigned manually while dynamic ones are assigned automatically by DHCP servers or routers when a device connects to the network. The book also explains how these addresses can be used for security purposes, such as restricting access to certain parts of the network.

In addition, it provides detailed instructions on how to set up networks using both IPv4 and IPv6 protocols, which are two commonly used versions of Internet Protocols (IP). Furthermore, it offers guidance on troubleshooting common

networking issues related to IP addressing.

#8. Network Services: Network services are the applications and services that run on a network. (This book covers the different types of network services, such as web, email, and file sharing, as well as how to configure and troubleshoot these services.)

Network services are the applications and services that run on a network. These can include web servers, email servers, file sharing systems, and other types of applications. Network services allow users to access data from remote locations or share information with others over the internet. They also provide security measures such as firewalls and encryption protocols to protect user data.

This book covers different types of network services in detail, including how they work and how to configure them for optimal performance. It also provides troubleshooting tips for common problems related to these services so that readers can quickly identify and resolve any issues they may encounter.

In addition, this book explains the importance of keeping network services up-to-date with the latest security patches in order to ensure maximum protection against malicious attacks. It also discusses best practices for setting up secure networks so that users can enjoy safe online experiences without worrying about their data being compromised.

#9. Network Management: Network management is the process of monitoring, controlling, and maintaining a network. (This book

covers the different types of network management tools, such as SNMP and WMI, as well as how to use these tools to manage a network.)

Network management is an essential part of running a successful network. It involves monitoring, controlling, and maintaining the network to ensure that it runs smoothly and efficiently. Network management tools such as SNMP (Simple Network Management Protocol) and WMI (Windows Management Instrumentation) are used to manage networks. These tools allow administrators to monitor the performance of their networks, detect any problems or potential issues, configure settings on devices connected to the network, and troubleshoot any issues that arise.
SNMP is a protocol used for managing IP-based networks. It allows administrators to query devices on the network for

information about their status and configuration settings. WMI is Microsofts implementation of SNMP which provides similar functionality but with additional features tailored specifically for Windows systems.
Using these tools effectively requires knowledge of how they work as well as experience in using them in real-world scenarios. This book covers all aspects of network management from basic concepts through advanced topics such as scripting with SNMP/WMI and integrating third-party applications into your existing infrastructure.

#10. Network Troubleshooting: Network troubleshooting is the process of diagnosing and resolving network problems. (This book covers the different types of network troubleshooting techniques, such as packet sniffing and traceroute, as well

as how to use these techniques to troubleshoot a network.)

Network troubleshooting is an essential part of maintaining a reliable and secure network. It involves identifying the source of any problems that arise, diagnosing them, and then resolving them in order to restore normal operation. Network troubleshooting techniques can range from simple ping tests to more complex packet sniffing or traceroute analysis.

This book covers the different types of network troubleshooting techniques available, such as packet sniffing and traceroute. It also explains how these techniques can be used to identify and resolve common network issues. Additionally, it provides guidance on how to use various tools for monitoring networks in order to detect potential problems before they become serious.

The book also discusses best practices for preventing future network issues by implementing proactive measures such as regular maintenance checks and security audits. Finally, it offers advice on how to respond quickly when a problem does occur so that service disruptions are minimized.

Thank you for reading!

If you enjoyed this abstract, please share it with your friends.

Books.kim