Term 3 Mid-Term Summary Sheet

Grade 9

- A network is a collection of devices that can communicate and share resources using a common set of rules or protocols.
- A network topology is the physical or logical arrangement of devices on a network. The common types of network topologies are star, mesh, client-server, and bus. A star topology has a central device that connects to all other devices. A mesh topology has multiple paths between any two devices. A client-server topology has one or more servers that provide services to clients. A bus topology has a single cable that connects all devices.
- A network protocol is a set of rules that defines how devices communicate on a network. The common network protocols are TCP, UDP, DHCP, and HTTP. TCP (Transmission Control Protocol) is a reliable and connection-oriented protocol that ensures data delivery and error recovery. UDP (User Datagram Protocol) is an unreliable and connectionless protocol that provides fast and low-overhead data transmission. DHCP (Dynamic Host Configuration Protocol) is a protocol that assigns IP addresses to devices on a network. HTTP (Hypertext Transfer Protocol) is a protocol that transfers web pages and other data over the Internet.
- An IP address is a unique identifier for a device on a network. A subnet mask is a binary number that defines the network and host portions of an IP address. The network portion identifies the network to which the device belongs, and the host portion identifies the device within the network. A subnet mask also defines the range of valid IP addresses for a network.
- A network cable is a physical medium that carries data signals between devices on a network. The common types of network cables are coaxial cable, fiber optic cable, twisted pair cable, and USB cable. Coaxial cable has a central copper wire surrounded by a braided metal shield. Fiber

optic cable has a core of glass or plastic that transmits light signals. Twisted pair cable has pairs of copper wires twisted together to reduce interference. USB cable has four wires that connect devices to a computer or a hub.

- A network connection is a logical link between devices on a network. The speed of a network connection is measured by the data rate or bandwidth, which is the amount of data that can be transferred per unit of time. The common network connections are Ethernet, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet. Ethernet is a network connection that operates at 10 Mbps (megabits per second). Fast Ethernet is a network connection that operates at 100 Mbps. Gigabit Ethernet is a network connection that operates at 1 Gbps (gigabits per second). 10 Gigabit Ethernet is a network connection that operates at 10 Gbps.
- A server is a device that provides services to other devices on a network. The common types of servers are web server, file server, database server, and print server. A web server hosts and delivers web pages and other web content. A file server stores and shares files. A database server stores and manages data in a database. A print server manages and controls printers and print jobs.
- A storage device is a device that stores data permanently or temporarily. The common types of storage devices are hard disk drive (HDD), solid-state drive (SSD), optical drive, and flash drive. A hard disk drive (HDD) is a storage device that uses magnetic disks to store data. A solid-state drive (SSD) is a storage device that uses flash memory to store data. An optical drive is a storage device that uses lasers to read and write data on optical discs. A flash drive is a storage device that uses flash memory to store data and has a USB interface.
- A RAID array is a collection of storage devices that work together to provide increased performance, reliability, or capacity. RAID stands for Redundant Array of Independent Disks. The common types of RAID levels are RAID 0, RAID 1, RAID 5, and RAID 10. RAID 0 (striping) splits data across multiple disks to increase speed, but provides no redundancy. RAID 1 (mirroring) duplicates data on two disks to provide redundancy, but reduces capacity by half. RAID 5 (parity) distributes data and parity

information across three or more disks to provide redundancy and speed, but reduces capacity by one disk. RAID 10 (nested) combines RAID 0 and RAID 1 to provide redundancy and speed, but reduces capacity by half.

- A SAN (Storage Area Network) is a network of storage devices that provides block-level storage to servers. A NAS (Network Attached Storage) is a single storage device that provides file-level storage to clients. A SAN is more expensive, more scalable, and more secure than a NAS. A NAS is cheaper, easier to manage, and more accessible than a SAN.
- A backup is a copy of data that can be used to restore the original data in case of data loss or corruption. The common types of backups are full backup, incremental backup, and differential backup. A full backup copies all the data from the source to the destination. An incremental backup copies only the data that has changed since the last backup. A differential backup copies only the data that has changed since the last full backup.
- A system image backup is a backup that copies the entire operating system and all installed programs from the source to the destination. A system image backup can be used to restore the system to any previous state. A restore point is a backup that creates a snapshot of the system at a specific point in time. A restore point can be used to restore the system to its previous state. A restore point is faster to create than a system image backup, but a system image backup is more reliable than a restore point.
- A group policy is a set of rules that controls user access to resources, configures system settings, and deploys software on a network. A group policy can be applied to a single computer, a group of computers, or a domain. A local group policy is a group policy that applies to a single computer. A domain group policy is a group policy that applies to all computers in a domain. A domain group policy can override a local group policy, unless the local group policy is more restrictive. A domain group policy is easier to configure than a local group policy, but a local group policy is more secure than a domain group policy.
- A network security threat is any action or event that can compromise the confidentiality, integrity, or availability of data on a network. The common types of network security threats are malware, phishing, social

engineering, and denial of service (DoS) attack. Malware is malicious software that can infect, damage, or control a device or a network. Phishing is a fraudulent attempt to obtain sensitive information by impersonating a legitimate entity. Social engineering is a technique that exploits human psychology to manipulate or deceive people into revealing information or performing actions. Denial of service (DoS) attack is an attack that overwhelms a network or a device with excessive traffic or requests, rendering it unavailable or slow.

- A firewall is a device or a software that monitors and filters the incoming and outgoing network traffic based on predefined rules. The purpose of a firewall is to block unauthorized access to a network, protect data from unauthorized access, and encrypt data. The common types of firewalls are packet-filtering firewall and stateful inspection firewall. A packet-filtering firewall only checks the source and destination IP addresses of packets, while a stateful inspection firewall also checks the port numbers and the state of the connection. A stateful inspection firewall is more effective than a packet-filtering firewall at blocking attacks, but a packet-filtering firewall is faster and simpler than a stateful inspection firewall.
- Packet-Filtering Firewall vs. Stateful Inspection Firewall: - A packet-filtering firewall checks the source and destination IP addresses of packets, while a stateful inspection firewall also checks the port numbers and the state of the connection. - A stateful inspection firewall is more effective than a packet-filtering firewall at blocking attacks.
- 19. Encryption: - The purpose of encryption is to protect data from unauthorized access, modification, and deletion.
- 20. Symmetric Encryption vs. Asymmetric Encryption: - Symmetric encryption uses the same key to encrypt and decrypt data, while asymmetric encryption uses different keys for encryption and decryption. - Both encryption methods have their own advantages and use cases.