Study Guide

Section 1: Introduction to Networking Concepts

OSI Model & TCP/IP Model

OSI (Open System Interconnection) Model

Layer	What happens at each layer?
7. Application	Interfaces directly with the software application
6. Presentation	Data translation and encryption
5. Session	Establishes, manages, and terminates connections between applications
4. Transport	Provides reliable or unreliable delivery, and error recovery (e.g., TCP and UDP)
3. Network	Determines how data is sent to the receiver (IP addressing and routing)
2. Data Link	Handles physical addressing and error detection
1. Physical	Transmits raw bitstream over the physical medium.

How does the OSI model match to the TCP/IP model?

OSI	TCP/IP
7.Application HTTP, HTTPS, FTP, SMPT, IMAP	4.Application
6.Presentation encryption/decryption and formatting	
5.Session etablishment, maintenance and teardown	
4.Transport end to end comm- tcp and udp- segments- port addressing	3.Transport host-host
3.Network routes data pkts -IP, ARP, ICMP ip addresses, pkts	2.Internet internet
2.Data Link mac addresses, frames	1.Network Access network access
1.Physical transmist raw bitstream	

Network Media Devices

Device	Layer	What does the device do?
Hub	1	Broadcasts data to all connected devices
Modem	1	Converts digital signals into analog and vice versa
Repeater	1	Amplifies or regenerates signals to extend a network
Switch	2	Connects devices and filters traffic based on MAC addresses
Bridge	2	Divides network segments and reduces collisions.
Router	3	Routes data between different networks
Edge Router	3	Connects internal networks to external networks (e.g., Internet).
Core Router	3	Routes data within a large network (e.g., Internet backbone).
WRE	1	Extends the coverage of a wireless network.
WAP	2	Connects wireless devices to a wired network.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

Patch cable: Connects devices within a network, typically for short distances.

Patch Panel: A mounted hardware unit that contains ports to manage and organize network cables.

Basic Network Commands

What is each command used for?

- **Ping:** Tests connectivity between two devices on a network
- **ipconfig:** Displays IP configuration in Windows.
- **ifconfig:** Displays IP configuration in Linux/Unix
- **Traceroute/tracert:** Traces the path packets take to reach a network destination
- **Tracepath:** A network tool that traces the route packets take to a destination, identifying each hop and measuring delays, used for diagnosing connectivity issues.
- **ARP:** Displays and modifies the ARP table, which maps IP addresses to MAC addresses.
- **Netstat:** Displays network connections, routing tables, and interface statistics.
- Nslookup: Queries DNS to resolve domain names to IP addresses.
- **Dig:** Queries DNS servers for DNS records.
- **Whois:** Retrieves registration info about domains and IPs.
- **Route:** Views and manipulates the IP routing table.
- **SCP:** Securely transfers files between systems using SSH.
- **FTP:** Transfers files between systems (unencrypted).
- **TFTP:** Lightweight file transfer protocol without authentication.
- **Finger:** Displays user information on a system.
- **Nmap:** Scans networks for hosts and services.
- **Tcpdump:** Captures and analyzes network traffic.
- **Telnet/SSH:** Connects to remote systems (Telnet is insecure, SSH is secure).

Network Types

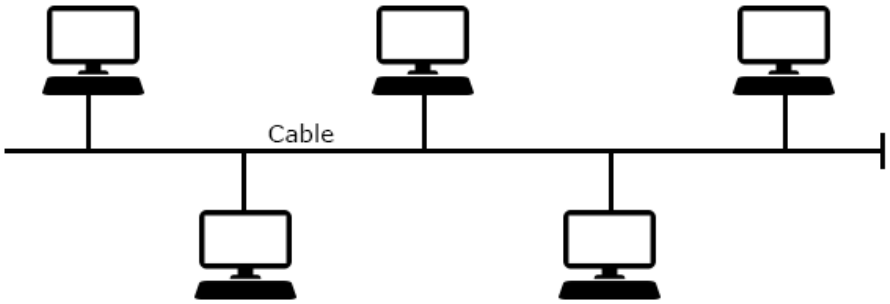
Describe each network type

- **Personal Area Network (PAN):** Small network for personal devices (e.g., Bluetooth).
- **Local Area Network (LAN):** Connects devices within a small area, like a building
- **Wireless Local Area Network (WLAN):** A network that spans a large geographic area, typically connecting LANs.
- **Storage Area Network (SAN):** A high-speed network that provides access to consolidated block-level storage.
- **Campus Area Network (CAN):** A network that connects multiple buildings within a campus or a limited geographic area.
- **Metropolitan Area Network (MAN):** A network that spans a city or large urban area, connecting multiple LANs.
- **Wide Area Network (WAN):** A network that covers a large geographic area, connecting multiple LANs and MANs, often over long distances.

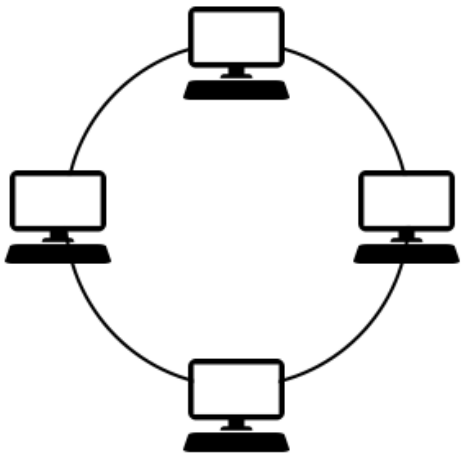
Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

Network Topologies

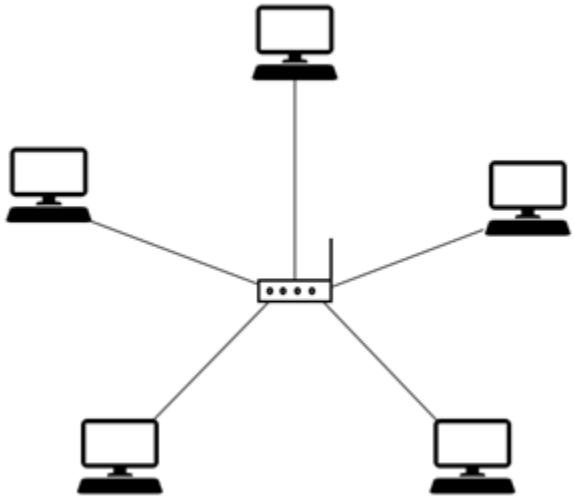
Describe each network topology.



Bus: All devices share a common backbone cable, and data is sent in both directions.

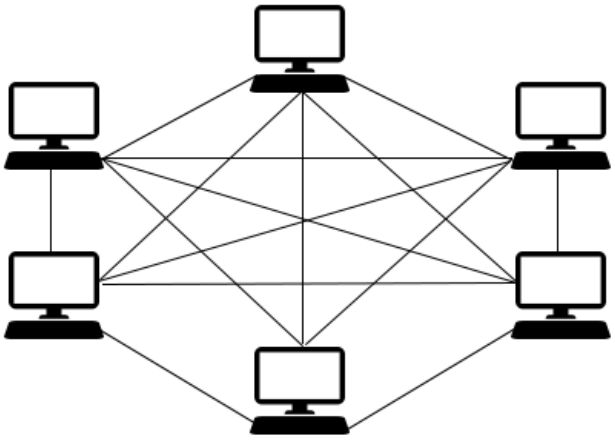


Ring: Each device is connected to two others, forming a circular pathway for data.



Star: All devices are connected to a central hub or switch.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)



Mesh: connects each node to multiple other nodes, creating multiple paths for data to travel, enhancing reliability and redundancy in the network.

Network Architecture

Explain each network architecture:

- **Centralized:** A single server manages the network resources.
- **Decentralized:** Resources are managed by multiple servers, reducing single points of failure
- **Client-Server Model:** A network architecture where clients request services or resources from a centralized server, which processes and delivers the requested data.
- **Peer-to-Peer Model:** A decentralized network architecture where each device (peer) can act as both a client and a server, sharing resources directly without relying on a central server.

Virtual and Cloud Computing

Hypervisors:

What is the difference between a Type 1 and Type 2 hypervisor?

- **Type 1:** Runs directly on the hardware (bare metal)
- **Type 2:** Runs on top of a host operating system.

Describe the Cloud Service Models (who is responsible for what?)

- **IaaS:** The provider manages networking, storage, and virtualization. The user is responsible for managing the operating system, applications, and data.
- **PaaS:** The provider manages the infrastructure and platform (OS, runtime, servers). The user is responsible for managing applications and data.
- **SaaS:** The provider manages everything, including applications, infrastructure, and data. The user just uses the software

Describe the Cloud Deployment Models

- **Private Cloud:** Cloud infrastructure is dedicated to a single organization, providing more control and security.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

- **Public Cloud:** Cloud services are provided to multiple organizations over the internet, shared between users but isolated.
- **Community Cloud:** Cloud infrastructure is shared by multiple organizations with common interests or regulatory concerns.
- **Hybrid Cloud:** A combination of private and public clouds, allowing data and applications to move between them.
- **Multi-Cloud:** The use of multiple cloud services from different providers to meet specific needs or improve redundancy.

Section 2: Introduction to Networking Security

Network Security Overview

Define each term:

- **SecOPs:** Practices and processes that monitor and manage security infrastructure, incident response, and threat detection.
- **Vulnerability:** A weakness in a system or software that can be exploited by attackers.
- **Zero – Day:** An attack that exploits a vulnerability that is unknown to the vendor or has not yet been patched.

Describe each attack Type:

- Describe each security team:
    - **Red team:** A group that simulates attacks to test the effectiveness of an organization's security.
    - **Blue team:** The defensive security team responsible for detecting, responding to, and defending against attacks.
    - **White team:** The group responsible for overseeing security tests and ensuring fair play between red and blue teams.
    - **Purple team:** A collaborative team combining both red and blue team activities to improve overall security.
- Describe each hacker:
    - **White Hat:** Ethical hackers who use their skills to improve security by finding vulnerabilities and reporting them.
    - **Black Hat:** Malicious hackers who exploit vulnerabilities for personal gain or to cause harm.
    - **Gray Hat:** Hackers who operate between ethical and unethical hacking, sometimes breaking laws without malicious intent.
- **What is Social Engineering:** The manipulation of people into divulging confidential information or performing actions that compromise security.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

Confidentiality, Integrity, and Availability (CIA) Triad

Confidentiality: Ensuring that sensitive information is accessible only to authorized users.

Integrity: Ensuring that data is accurate, consistent, and has not been tampered with.

Availability: Ensuring that systems and data are accessible to authorized users when needed.

Section 3: Network Security Operations

- **Defense in Depth:** A multi-layered approach to security where multiple controls are implemented to protect assets.
- **Separation of Privilege:** Granting access based on a strict need-to-know basis, requiring multiple conditions to be met for access.
- **Least Privilege:** Ensuring users and systems have only the minimum access rights needed to perform their tasks.
- **Psychological Acceptability:** Security measures should not hinder users' ability to complete their tasks and should be user-friendly.
- **Least Common Mechanism:** Minimizing shared resources between users or systems to reduce the risk of attack.
- **Open Design:** Security mechanisms should not depend on secrecy of design but rather on robust, well-understood principles.

Firewalls, IDS, and IPS

- **Firewalls** – A device or software that monitors and controls incoming and outgoing network traffic based on security rules.

Device	Description
Packet filtering Firewall	Inspects packets at a basic level, filtering traffic based on source/destination IP addresses, ports, and protocols.
Stateful Inspection Firewall	Monitors the state of active connections and makes decisions based on the state and context of traffic.
Application Layer Firewall	Examines traffic at the application layer, allowing more specific control over HTTP, FTP, and other protocols.
Intrusion Detection System	A system that monitors network traffic for suspicious activity and alerts administrators of potential attacks.
Intrusion Prevention System	Similar to IDS but can actively block or prevent detected malicious activities in real time.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

- **Honey POT:** A decoy system designed to attract and trap attackers to study their methods and gather intelligence.
- **Explain DMZ:** A network segment that separates internal networks from external networks (like the internet), used to host public-facing services.
- **Explain VPN:** A secure, encrypted connection over the internet that allows remote access to a private network.

OSI and TCP/IP Security – List an attack on each Layer and describe the mitigation

Attack	Description	Mitigation
SQL Injection attack	Inserting malicious SQL queries into web forms or URLs to manipulate databases.	Use parameterized queries and input validation.
Port Scanning Attack	Scanning open ports to find vulnerabilities in a system.	Use firewalls and limit open ports
Evil Twin Attack	Setting up a fake Wi-Fi access point to steal credentials from users.	Use encryption (WPA2/WPA3) and avoid public Wi-Fi.
Arp Poisoning Attack	Spoofing ARP messages to intercept network traffic between devices.	Use static ARP entries and network segmentation.
Deauthentication Attack	Sending fake DE authentication frames to disconnect devices from a Wi-Fi network.	Use WPA3 encryption and monitor Wi-Fi traffic for anomalies.
BlueSnarfing	Unauthorized access to a Bluetooth device's information.	Disable Bluetooth when not in use and use strong PIN codes.
War Chalking	Marking physical locations where Wi-Fi networks are available, often unsecure.	Use strong Wi-Fi encryption and disable open networks.

Encryption Fundamentals

- **Symmetric Key Encryption:** The same key is used for both encryption and decryption.
- **Asymmetric Key Encryption:** Uses a pair of keys (public and private) for encryption and decryption.
- **Public Key Infrastructure (PKI):** A system that manages encryption keys and digital certificates to enable secure, authenticated communication over networks.
- **SSL/TLS and what it is mainly used for:** Encrypts data transmitted over the internet, primarily used in securing HTTP traffic (HTTPS)
- **IPSec:** Secures IP communications by authenticating and encrypting each IP packet

Cloud Security

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

- **Data at Rest:** Data that is stored on physical devices, such as hard drives, databases, or cloud storage, and is not actively being transferred or processed.
- **Data in Transit:** Data that is actively moving from one location to another, such as across a network or between systems, typically over the internet or internal networks.

Wireless Security

Wireless Encryption Standards

- **Describe WEP:** Wired Equivalent Privacy, an outdated and insecure wireless encryption standard.
- **Describe WPA:** Wi-Fi Protected Access, an improved version of WEP.
- **Describe WPA2:** Stronger encryption (AES), replacing WPA
- **Describe WPA3:** Latest wireless encryption with more secure handshaking and encryption mechanisms.

- **3DES encryption:** A symmetric encryption algorithm that applies the DES cipher three times to each data block, increasing security over the original DES.
- **AES encryption:**
  - A secure and widely used symmetric encryption algorithm, with key sizes of 128, 192, or 256 bits, offering strong data protection.
- Wireless Network Infrastructure Modes
  - **Ad-hoc:** A peer-to-peer mode where devices communicate directly with each other without a central access point.
  - **Infrastructure:** Devices communicate through a centralized access point, commonly used in enterprise or home networks.

User Authentication and Access Control

- **AAA**
  - **Authentication:** The process of verifying a user's identity through credentials like passwords or biometrics.
  - **Authorization:** Determines what resources a user is permitted to access after authentication.
  - **Accounting:** Tracks and logs user activities for auditing and billing purposes.
- **Multifactor Authentication:** A security process that requires two or more verification methods (e.g., password, biometrics, security tokens) to authenticate a user.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)

Device Hardening

Windows 10 Hardening and list 3 techniques: Strengthening the security of a Windows 10 system to reduce vulnerabilities.

Techniques:

- Enable BitLocker for full disk encryption.
- Use Windows Defender Firewall.
- Apply regular security updates.

Windows Server 2019 Hardening and 3 techniques: Strengthening the security of Windows Server 2019 to protect against threats.

Techniques:

- Disable unnecessary services.
- Implement Group Policy for security configurations.
- Enable enhanced auditing and monitoring.

Security Governance

- **PIPEDA (Personal Information Protection and Electronic Documents Act):**
  Description: Canadian law governing how private-sector organizations collect, use, and disclose personal information during commercial business.

- **HIPAA (Health Insurance Portability and Accountability Act):**
  Description: U.S. law that sets standards for protecting sensitive patient health information and ensuring data privacy.

- **GDPR (General Data Protection Regulation):**
  Description: European Union regulation that protects individuals' personal data and privacy, applying strict rules on data handling and processing.

Downloaded by Itwela Ibomu (deanandnostrand@gmail.com)