Overview IKT204

Contents

[Course description: 2](#_Toc198720207)

[IKT204 Datakommunikasjon (Vår 2025) 3](#_Toc198720208)

[Emnet er tilknyttet følgende studieprogram 3](#_Toc198720209)

[Undervisningsspråk 3](#_Toc198720210)

[Anbefalte forkunnskaper 3](#_Toc198720211)

[Læringsutbytte 3](#_Toc198720212)

[Innhold 3](#_Toc198720213)

[Undervisnings- og læringsformer 4](#_Toc198720214)

[Vilkår for å gå opp til eksamen 4](#_Toc198720215)

[Eksamen 4](#_Toc198720216)

[Module descriptions 4](#_Toc198720217)

[Module 1: Computer Networks and the Internet 4](#_Toc198720218)

[Module 2: Application Layer 5](#_Toc198720219)

[Module 3: Transport Layer 5](#_Toc198720220)

[Module 4: The Network Layer: Data Plane 6](#_Toc198720221)

[Module 5: The Network Layer: Control Plane 7](#_Toc198720222)

[Module 6: The Link Layer and LANs 7](#_Toc198720223)

[Module 7: Wireless and Mobile Networks 8](#_Toc198720224)

[Module 8: Security in Computer Networks 9](#_Toc198720225)

[Syllabus: 10](#_Toc198720226)

[Book: Computer Networking: A Top Down Approach 10](#_Toc198720227)

[Covered chapters and sections ToC: 10](#_Toc198720228)

[**Chapter 1 Computer Networks and the Internet** 10](#_Toc198720229)

[Road-Mapping This Book 14](#_Toc198720230)

[Lecture summaries: 15](#_Toc198720231)

[**Chapter 1 *Introduction*** 15](#_Toc198720232)

[**Chapter 2 *Application-Layer Protocols*** 16](#_Toc198720233)

[**Chapter 3A *UDP + Reliable-Data Principles*** 16](#_Toc198720234)

[**Chapter 3B *TCP & Congestion Control*** 16](#_Toc198720235)

[**Chapter 4 *Network-Layer I: Forwarding & SDN*** 16](#_Toc198720236)

[**Chapter 5 *Network-Layer II: Control Plane*** 17](#_Toc198720237)

[**Chapter 6 *Link Layer & LANs*** 17](#_Toc198720238)

[**Chapter 7 *Wireless & Mobile*** 17](#_Toc198720239)

[**Chapter 8 *Network Security*** 17](#_Toc198720240)

[**Packet Analysis with Wireshark** 18](#_Toc198720241)

[**TCP Socket Programming (Winsock)** 18](#_Toc198720242)

[**UDP Socket Programming (Winsock)** 18](#_Toc198720243)

# IKT204 Course Material: Indexed Overview & Information Map

This index provides a structured guide to the core IKT204 course materials, including lecture notes, lab guides, past exams, and comprehensive review questions. It's designed to help both students and language models quickly locate relevant information by topic and sub-topic.

## I. Core Lecture Materials (Organized by Course Flow/Chapter)

### **File:** Chapter\_1\_24V\_Lecture - Tagged.pdf (L1)

* + **Primary Focus:** Introduction to Computer Networks and the Internet.
  + **Key Concepts Mapped:** Internet definition (nuts-and-bolts, services), protocols, network edge (hosts, access networks, physical media), network core (packet/circuit switching, ISP structure), performance metrics (delay, loss, throughput), protocol layers (OSI & 5-layer model), encapsulation, basic network security threats, history of networking.
  + **Information Density:** High for foundational concepts and terminology.
  + **LLM Cue:** "Fundamentals of Internet, layers, delay types, Ch1 concepts"

### **File:** Chapter\_2\_25V.pdf (L2)

* + **Primary Focus:** Application Layer.
  + **Key Concepts Mapped:** Principles of network applications (client-server, P2P), process communication (sockets, IP/port), transport layer service needs, HTTP (versions, persistent/non-persistent, messages, cookies, HOL blocking, HTTP/2), Email (SMTP, mail formats, POP3/IMAP), DNS (hierarchy, resolution, RR types, caching, security), P2P file distribution (BitTorrent), Video Streaming & CDNs (DASH).
  + **Information Density:** Very high for major application protocols.
  + **LLM Cue:** "HTTP, DNS, SMTP, P2P, CDN, application layer services, Ch2 details"

### **File:** Chapter\_3A\_25V - Tagged.pdf (L3A)

* + **Primary Focus:** Transport Layer (Part 1 - Services, UDP, RDT Principles).
  + **Key Concepts Mapped:** Transport layer services (multiplexing/demultiplexing), UDP (header, checksum, use cases, unreliability), principles of reliable data transfer (rdt1.0-rdt3.0, stop-and-wait, ACKs, NACKs, timers, sequence numbers), pipelining (Go-Back-N, Selective Repeat).
  + **Information Density:** High for UDP and foundational RDT.
  + **LLM Cue:** "UDP, port numbers, multiplexing, reliable data transfer principles, rdt3.0, GBN, SR, Ch3 Part A"

### **File:** Chapter\_3B\_25V.pdf (L3B)

* + **Primary Focus:** Transport Layer (Part 2 - TCP).
  + **Key Concepts Mapped:** TCP overview (connection-oriented, reliable byte stream), TCP segment structure (all fields), connection management (3-way handshake, 4-way close), TCP reliable data transfer (sequence/ACK numbers, RTT estimation, timeout, fast retransmit), TCP flow control (receive window), TCP congestion control (AIMD, slow start, ssthresh, fast recovery, fairness).
  + **Information Density:** Extremely high for TCP mechanics.
  + **LLM Cue:** "TCP details, handshake, flow control, congestion control (slow start, AIMD), RTT, segment structure, Ch3 Part B"

### **File:** Chapter\_4\_25V - Tagged.pdf (L4)

* + **Primary Focus:** Network Layer: Data Plane.
  + **Key Concepts Mapped:** Forwarding vs. routing, router architecture (input/output ports, switching fabric), IP datagram format (IPv4), fragmentation & reassembly, IPv4 addressing (CIDR, subnets, subnet masks, getting IP addresses via DHCP), NAT (operation, translation table), IPv6 (motivation, datagram format, tunneling), generalized forwarding/SDN basics (match-action).
  + **Information Density:** Very high for IP addressing, subnetting, NAT, and DHCP.
  + **LLM Cue:** "IPv4, IPv6, datagrams, fragmentation, CIDR, subnetting, DHCP, NAT, router data plane, Ch4 content"

### **File:** Chapter\_5\_24V.pdf (L5)

* + **Primary Focus:** Network Layer: Control Plane.
  + **Key Concepts Mapped:** Routing algorithms (Link-State/Dijkstra, Distance-Vector/Bellman-Ford, count-to-infinity), intra-AS routing (OSPF), inter-AS routing (BGP: AS-PATH, NEXT-HOP, policy), SDN control plane (controller, OpenFlow basics), ICMP (messages, ping, traceroute).
  + **Information Density:** High for routing algorithms and inter/intra-AS protocols.
  + **LLM Cue:** "Routing algorithms (Dijkstra, Bellman-Ford), OSPF, BGP, ICMP, SDN control plane, Ch5 topics"

### **File:** Chapter\_6\_25V - Tagged.pdf (L6)

* + **Primary Focus:** The Link Layer and LANs.
  + **Key Concepts Mapped:** Link layer services (framing, MAC access, error detection/correction), error detection techniques (parity, checksum, CRC), Multiple Access Protocols (channel partitioning: TDMA/FDMA; random access: ALOHA, CSMA/CD/CA; taking turns: polling, token), Switched LANs, MAC addressing, ARP, Ethernet (frame structure, standards), learning switches, VLANs, Data Center Networking, "Day in the Life" synthesis.
  + **Information Density:** High for MAC protocols, ARP, and Ethernet.
  + **LLM Cue:** "Link layer, MAC addresses, ARP, Ethernet, switches, VLANs, CRC, multiple access protocols, Ch6 details"

### **File:** Chapter\_7\_25V - Tagged.pdf (L7)

* + **Primary Focus:** Wireless and Mobile Networks.
  + **Key Concepts Mapped:** Wireless link characteristics (path loss, multipath, interference, SNR), infrastructure vs. ad-hoc mode, WiFi 802.11 (architecture: BSS/AP, channels, association, beacon frames), 802.11 MAC (CSMA/CA, RTS/CTS, ACKs, hidden terminal), 802.11 frame format (addressing fields), mobility in same subnet, rate adaptation, power management, Bluetooth basics.
  + **Information Density:** High for 802.11 MAC and architecture.
  + **LLM Cue:** "Wireless, WiFi, 802.11, CSMA/CA, RTS/CTS, hidden terminal, beacons, Ch7 concepts"

### **File:** Chapter\_8\_25V - Tagged.pdf (L8)

* + **Primary Focus:** Security in Computer Networks.
  + **Key Concepts Mapped:** Security properties (confidentiality, integrity, authenticity, availability, non-repudiation), attack types, cryptography principles (Kerckhoff, symmetric/asymmetric encryption, block ciphers: DES/AES, modes: ECB/CBC/CTR), public key crypto (RSA, Diffie-Hellman), message integrity (hash functions: MD5/SHA, MACs: HMAC), digital signatures, digital certificates (CAs, X.509), authentication protocols, PGP, SSL/TLS (handshake, record protocol, nonces, forward secrecy), operational security (firewalls: stateless/stateful/proxy, IDS/IPS).
  + **Information Density:** Very high for cryptographic primitives and TLS.
  + **LLM Cue:** "Network security, crypto, symmetric/asymmetric keys, hashes, MACs, signatures, certificates, TLS, firewalls, Ch8 details"

## II. Lab Materials & Practical Application Guides

### **File:** Packet analysis using Wireshark - Tagged.pdf (LAB-WS)

* + **Primary Focus:** Practical packet analysis using Wireshark.
  + **Key Concepts Mapped:** ping command, ICMP echo request/reply, DNS lookups initiated by ping, Wireshark filters (capture vs. display), nmap for host discovery (ARP sweep, ICMP probing), interpreting tcp.stream index, analyzing HTTP and DNS traces.
  + **Information Density:** High for practical Wireshark usage and interpreting common protocol traces.
  + **LLM Cue:** "Wireshark usage, ping analysis, nmap, ICMP trace, DNS trace, HTTP trace practicals"

### **File:** TCP socket programming - Tagged.pdf (LAB-TCP)

* + **Primary Focus:** TCP socket programming (Winsock API).
  + **Key Concepts Mapped:** Socket API sequence (server: socket, bind, listen, accept, recv/send, closesocket; client: socket, connect), 3-way handshake initiation by connect, 4-tuple for distinguishing flows, netstat for diagnostics, firewall implications.
  + **Information Density:** High for TCP socket API steps.
  + **LLM Cue:** "TCP socket programming, Winsock API, client-server TCP steps"

### **File:** UDP socket programming - Tagged.pdf (LAB-UDP)

* + **Primary Focus:** UDP socket programming (Winsock API).
  + **Key Concepts Mapped:** Socket API sequence (server: socket, bind, recvfrom/sendto, closesocket; client: socket, sendto, recvfrom), stateless nature, application-level reliability, endianness (htons, htonl), loopback address, ncat for UDP.
  + **Information Density:** High for UDP socket API steps and endianness.
  + **LLM Cue:** "UDP socket programming, Winsock API, endianness, ncat UDP"

## III. Examination & Review Materials

### Files:

* + dat204-exam-fall 2016.pdf (EXAM16F)
  + dat204-exam-fall 2017.pdf (EXAM17F)
  + dat204-exam-spring 2017.pdf (EXAM17S)
  + IKT204-exam-fall 2018.pdf (EXAM18F)
  + DAT204-G utsatt skoleeksamen 26.2.18.pdf (EXAM18S\_utsatt) *(The text-pasted exam)*
  + dat204-exam-fall 2019.pdf (EXAM19F)
  + IKT204 school exam V24 with answers.pdf (EXAM24V)
  + **Primary Focus:** Actual past exam questions and expected answer styles.
  + **Key Concepts Mapped:** Covers the entire syllabus with varying emphasis per exam. Essential for understanding question phrasing, complexity distribution, and point allocation trends.
  + **Information Density:** High for specific problem types and tested concepts.
  + **LLM Cue:** "Past exam questions, IKT204 exam format, typical DAT204 problems from [year]"

### **File:** IKT204 – all review questions with answer guides.docx (REV\_Q)

* + **Primary Focus:** Comprehensive review questions with solutions, chapter by chapter.
  + **Key Concepts Mapped:** Exhaustive coverage of all syllabus topics, including definitional (R-type) and problem-solving (P-type) questions. Provides model answers.
  + **Information Density:** Extremely high and detailed across the entire course.
  + **LLM Cue:** "IKT204 review questions, solutions for [Chapter X topic], R-type questions, P-type questions"

## IV. Course Meta-Information

### **File:** Overview IKT204.docx (OVERVIEW)

* + **Primary Focus:** Course structure, learning outcomes, module descriptions, syllabus outline (ToC references).
  + **Key Concepts Mapped:** Meta-level information about the course itself. Provides context for how individual topics fit into the larger curriculum.
  + **Information Density:** High for course structure and intended learning objectives.
  + **LLM Cue:** "IKT204 course description, syllabus, module objectives, learning outcomes"

### **File:** Lecture topic, content and keyword map.json (LECTURE\_MAP\_JSON)

* + **Primary Focus:** A structured JSON map of lecture topics, their content, and associated keywords.
  + **Key Concepts Mapped:** This file *is* a map of concepts derived from lectures.
  + **Information Density:** High, structured data about lecture content.
  + **LLM Cue:** "Lecture keywords, topic map from lectures JSON"

# Course description:

The course covers basic principles and concepts of data communications. The course follows a “layered”, top-down approach, beginning with the application layer:

* Application layer protocols, such as HTTP and DNS as well as basic socket programming, addressing.
* Transport layer protocols, such as UDP and TCP, reliable data transfer, flow control and congestion control.
* Network layer protocols, such as IPv4 and IPv6, network structure, routing principles, and addressing.
* Network layer control protocols and architectures, routing algorithms, ICMP.
* Link layer protocols, concepts, link-layer addressing and ARP, Ethernet.
* Wireless and mobile networks, network structures, network components and access principles (wireless LAN 802.11).
* Security in computer networks.

## IKT204 Datakommunikasjon (Vår 2025)

### Emnet er tilknyttet følgende studieprogram

* [Ingeniørfag - data, bachelorprogram](https://www.uia.no/studier/program/data-ingeniorutdanning-bachelor/)
* [Ingeniørfag - elektronikk, bachelorprogram](https://www.uia.no/studier/program/elektronikk-ingeniorutdanning-bachelor/)
* [Kunstig intelligens, 5-årig masterprogram](https://www.uia.no/studier/program/kunstig-intelligens-master-5-ar/)

### Undervisningsspråk

Emnet undervises på norsk.

### Anbefalte forkunnskaper

Grunnleggende nettverk og sikkerhetsforståelse som f.eks. IKT100-G Nettverk, sikkerhet og personvern.

### Læringsutbytte

#### Kunnskap:

* Ha kunnskap om de grunnleggende prinsippene for datakommunikasjonssystemer.
* Kjenne til nettstrukturer, nettkomponenter og de viktigste protokollene i et IP basert datanett

#### Ferdigheter:

* Forstå prinsippene for hvordan nettkomponenter og protokoller virker sammen for å muliggjøre datatransport og nettbaserte tjenester.

#### Generell kompetanse:

* Ha nødvendig fundament for å kunne jobbe med problemer og utfordringer innen feltet.

### Innhold

Grunnleggende prinsipper, begreper og standarder med vekt på moderne Internett teknologi.

Kablet og trådløst linklag, nettstrukturer, nettkomponenter og aksessprinsipper (Ethernet og 802.11).

Nettlaget, IPv4 og IPv6, nettstruktur, rutingprinsipper og programvaredefinerte nettverk.

Transportlaget, UDP, TCP, pålitelig dataoverføring, flytkontroll og metningskontroll.

Avanserte IP-baserte nettarkitekturer.

Applikasjonslagsprotokoller som HTTP, SMTP og DNS samt grunnleggende socketprogrammering.

Operasjonell sikkerhet, grunnleggende kryptografi og SSL programmering.

## Undervisnings- og læringsformer

Forelesninger, teoriøvinger og lab-øvinger. Avdelingsingeniør, studentassistent og/eller faglærere er til stede. Det gis opplæring i bruk av fagrelatert programvare og maskinvare.

Forventet arbeidsbelastning for gjennomsnittsstudenten er 27 timer pr studiepoeng.

## Vilkår for å gå opp til eksamen

Obligatoriske øvingsoppgaver må være godkjent for å gå opp til eksamen. Oversikt over obligatoriske oppgaver gis i Canvas ved semesterstart.

## Eksamen

3 timer individuell skoleeksamen. Gradert karakter.

# Module descriptions

## Module 1: Computer Networks and the Internet

This chapter gives a high-level overview over how computer networks and the Internet works. It quickly goes into all areas that will be covered more in-depth in the subsequent chapters and in particular introduces some important basic theory for calculating delay components in computer networks.

**By the end of this module you will be able to:**

* Know the definition of a protocol as well as some Internet protocols.
* Know several concepts - host/end system, router.
* Understand the layered Internet architecture and encapsulation as well as know each layer of the Internet protocol stack.
* Have knowledge about access network technologies, the core network and which protocol layers that run in each of them.
* Know what packet switching and circuit switching is.
* Calculate traffic intensity and end-to-end packet delay (including transmission delay, propagation delay) for network scenarios and understand throughput, queueing delay and the reasons for packet loss.
* Some attacks against network security.
* The history of Internet, including the Cerf and Kahn principle.

## Module 2: Application Layer

This module covers chapter 2 of the textbook. The focus is on conceptual and implementation aspects of network applications. It begins with covering key application layer concepts including network services required by applications, clients, servers, processes and transport layer interfaces. Some popular network applications are studied in detail, including Web, e-mail, DNS and peer-to-peer (P2P) file distribution. (An introduction to socket programming with UDP and TCP will be moved to chapter 3).

## Module 3: Transport Layer

This module covers chapter 3 Transport Layer in the textbook. The chapter gives an introduction to transport layer services as well as the relationship between the transport layer and the network layer. This includes an overview of how connectionless transport (UDP) and connection-oriented transport (TCP) works in the Internet, including multiplexing/demultiplexing of data, segment structure and the Internet checksum. The chapter gives an introduction to the principles of reliable data transfer by a step-by-step refinement to demonstrate how the Stop-and-Wait protocol works as well as pipelined protocols such as Go-Back-N and Selective Repeat. The chapter goes into more detail on how TCP works, including connection setup using 3-way handshake and connection teardown. It describes the TCP segment structure and how the round-trip-time (RTT) and timeout value is estimated for TCP as well as how TCP implements reliable data transfer, flow control and connection management. The last part of the chapter is devoted to the principles of congestion control and how this is implemented for TCP.

**By the end of this module you will be able to:**

* Know how transport layer services are implemented in the Internet.
* Understand the concepts of multiplexing and demultiplexing in the transport layer.
* Know the principles of reliable data transfer.
* Know how TCP and UDP are implemented.
* Understand TCP flow and congestion control as well as TCP connection management.

## Module 4: The Network Layer: Data Plane

This module covers the data plane part of the Network Layer. Important topics that you will learn in this chapter include understanding forwarding and routing as well as the network data and control plane. It then describes what is inside a router and how it processes data in input ports, how it forwards data and how data is handled at the output port. The chapter also discusses different bottlenecks inside a router where queuing of data can occur and packet scheduling disciplines to provide bandwidth guarantees to different traffic flows. The chapter then discusses the IPv4 and IPv6 addressing and packet format as well as IPv4 datagram fragmentation and network address translation (NAT). Finally the chapter covers generalized forwarding based on the Software-Defined Networking paradigm, and illustrates how SDN forwarding can be done using the match-plus-action flow table in the OpenFlow protocol.

**By the end of this module you will be able to:**

* Understand forwarding in the Network Layer and what the Data Plane entails.
* Get an overview of how a router is built up and the main functions it consists of.
* Understand where queuing may occur in a router.
* Know some common packet scheduling disciplines, such as Weighted Fair Queuing.
* Know the IPv4 and IPv6 packet formats and differences between them.
* Understand how IPv4 fragmentation, addressing and how NAT works.
* Get an overview over generalized forwarding and Software-Defined Networking.

## Module 5: The Network Layer: Control Plane

This chapter focuses on the control plane of the network layer. It starts with describing two common routing algorithms that have been widely used in routing protocol implementations: Dijkstra's Link-State routing algorithm and the Distance-Vector routing algorithm based on the Bellman-Ford equation for dynamic programming. The chapter then describes Open Shortest Path First (OSPF) as a routing table implementation that is based on the Link-State algorithm and then describes the Border Gateway Protocol (BGP), which is a distributed routing algorithm in a similar way as the Distance Vector algorithm. BGP is important to understand, since this is the "glue" that keeps different autonomous systems (ASs) in the Internet together, making it possible to announce routes to the interconnected networks and new networks. BGP is also different by focusing on more on policy and less on routing efficiency, since it is designed to handle commercial agreements between Internet backbone providers. The chapter then describes the SDN control plane and SDN control applications. It goes more into detail on how the OpenFlow protocol is managed in a SDN as well as illustrating the data and control plane interaction. The chapter then describes the Internet Control Message Procotol (ICMP).

**By the end of this module you will be able to:**

* Understand the Link-State and Distance Vector routing algorithms.
* Have an overview over OSPF used for intra-AS routing in the Internet.
* Get a high-level perspective on how the Border Gateway Protocol (BGP) works.
* Understand the SDN control plane architecture and SDN applications, including OpenFlow.
* Know what ICMP is used for.

## Module 6: The Link Layer and LANs

Module 6 covers the Link Layer, focusing on wired technologies. It first gives an introduction to services provided by the Link Layer and shows where it is implemented. It then discusses error detection and correction techiques such as parity checks, checksumming and the Cyclic Redundancy Check (CRC). Then different types of Multiple Access Links and Multiple Access Protocols are presented including channel partitioning protocols, random access protocols and taking turns protocol. The next section describes switched Local Area Networks (LANs). This section describes link layer addressing and the Address Resolution Protocol (ARP) which is used for mapping IP addresses on the network layer to MAC addresses on the network layer and vice versa. It furthermore describes how Ethernet LANs work including link-layer switches and virtual LANs (VLANs). The chapter then illustrates how networking is implemented on the link layer for large data centres, and the chapter ends with a detailed explanation of what happens during the life of a web page request, including the interaction between all protocols that are involved: DHCP, UDP, IP, Ethernet, DNS, ARP, TCP and HTTP.

**By the end of this module you will be able to:**

* Understand what link layer services and LANs are.
* Know how error correction techniques such as parity, checksumming and CRC works.
* Get an overview over how different Multiple Access Control (MAC) protocols work, such as:
  + Channel partitioning (TDM/FDM);
  + Random access (CSMA/CD used in Ethernet);
  + Taking turns protocols (polling and token passing);
* How switched Ethernet LANs work, including link-layer addressing and ARP, learning switches and VLANs.
* Understand how big data center networks are implemented as a hierarchy of link layer switches to support load balancing, redundancy and scalability.
* Get an overview over how all protocol layers from the Link Layer and up to the Application Layer work together.

## Module 7: Wireless and Mobile Networks

Module 7 Wireless and Mobile Networks. The module covers the initial part of the chapter on wireless links and network characteristics and WiFi: 802.11 Wireless LANs. It amongst others describes the 802.11 CSMA/CA MAC protocol, frame format and how hosts are associated with an access point and how IEEE 802.11 frames are transmitted from a host via an access point and to the router out of the network. Celluar Internet access is not part of this course.

**By the end of this module you will be able to:**

* Understand some of the basic characteristics and challenges with wireless communications - hidden terminal problem, fading, signal/noise ratio.
* Understand how IEEE 802.11 Wireless LAN (WiFi) works.
* Get a high-level introduction to Personal Area Networks (Bluetooth).

## Module 8: Security in Computer Networks

This module covers application- and transport layer security, which is described in chapter 8.

* To learn early how to secure applications and systems - design secure systems from the start.
* TLS is probably the most important security protocol now.
* The principles and practice behind application and transport layer security is very important, and should be part of the curriculum of a Bachelor program in computer science and electronics.
* Broad range of use cases, from developing software for web services, embedded systems, mobile systems or an Internet of Things.
* You will need to understand application and transport security as well as possibly being able to design secure code when you start working.

**By the end of this module you will be able to:**

* Understand the fundamentals of network security and the principles of cryptography.
* Get an overview over how symmetric key and public key cryptography works as well as cryptographic hash functions, message authentication code, digital signatures, and certificates.
* Understand authentication protocols, how secure email, PGP and TLS works.
* Know what a firewall is and how it works.
* Know what an intrusion detection system is and how it works.

# Syllabus:

## Book: Computer Networking: A Top Down Approach

### Covered chapters and sections ToC:

● Chapter 1 Computer Networks and the Internet  
 ● 1.1 What Is the Internet?  
  • 1.1.1 Nuts-and-Bolts – “network-of-networks”; edge hosts run apps, core routers/switches forward packets; links = fiber / copper / radio / satellite  
  • 1.1.2 Services – infrastructure exposes hooks for Web, video, gaming, IoT, etc.  
  • 1.1.3 Protocol – rules for message syntax, order, actions; ex. HTTP, TCP, IP; standardised by IETF RFCs

 ● 1.2 The Network Edge  
  • 1.2.1 Access Networks – DSL 24–52 Mb/s, cable ≤1.6 Gb/s, FTTH ≥1 Gb/s, Wi-Fi 11–2400 Mb/s, 4G ≈10 Mb/s, 5G ↑  
  • 1.2.2 Physical Media – twisted-pair Cat-5/6, coax, fibre 10-100 Gb/s, radio bands (Wi-Fi, LTE, sat.)

 ● 1.3 The Network Core  
  • 1.3.1 Packet Switching – store-and-forward; delay = L/R; queues when λ > μ  
  • 1.3.2 Circuit Switching – FDM/TDM slots; dedicated resources, idle wastage  
  • 1.3.3 A Network of Networks – tier-1, regional, access ISPs; IXPs; content-provider backbones

 ● 1.4 Delay, Loss & Throughput  
  • 1.4.1 Nodal Delay = dproc + dqueue + dtrans + dprop (dproc < µs)  
  • 1.4.2 Queuing Delay & Loss – traffic intensity ρ = La/R; ρ→1 ⇒ delay↑; full buffer ⇒ drop  
  • 1.4.3 End-to-End – sum of per-hop delays; traceroute measures RTT  
  • 1.4.4 Throughput – bottleneck link governs flow; statistical multiplexing shares capacity

 ● 1.5 Protocol Layers & Encapsulation  
  • 1.5.1 Layered Architecture – application, transport, network, link, physical  
  • 1.5.2 Encapsulation – message → segment → datagram → frame; headers/trailers added then stripped

 ● 1.6 Networks Under Attack  
  • Threats – malware, DDoS, spoofing; mitigations = crypto, firewalls, IDS

 ● 1.7 History of Networking  
  • 1.7.1 1961-72 – Kleinrock queuing theory; ARPANET 1969  
  • 1.7.2 1972-80 – TCP/IP design, Ethernet, 200-node ARPANET  
  • 1.7.3 1980-90 – SMTP, DNS, congestion control; 100 k hosts  
  • 1.7.4 1990s Explosion – NSFNET commercial, Web, Mosaic/Netscape  
  • 1.7.5 2000-present – broadband, SDN 2008, mobile > fixed 2017, hyperscale clouds

 ● 1.8 Summary – hosts, packets, delay, throughput, layering, security, history

● Chapter 2 Application Layer  
 ● 2.1 Principles of Network Applications  
  • 2.1.1 Architectures – client-server ⇆ P2P; CDN-assisted P2P.  
  • 2.1.2 Processes Communicating – socket = (IP, port); OS demux via 5-tuple.  
  • 2.1.3 Transport Needs – reliability, jitter, throughput, security.  
  • 2.1.4 Internet Services – TCP reliable vs UDP best-effort.  
  • 2.1.5 App-Layer Protocols – syntax, semantics, state rules (e.g., HTTP GET/200).  
  • 2.1.6 Application Set – HTTP, SMTP, DNS, BitTorrent, DASH.

 ● 2.2 The Web and HTTP  
  • 2.2.1 Overview – stateless request/response over TCP 80 / TLS 443.  
  • 2.2.2 Connections – non-persistent (2 RTT/object) vs persistent (1 RTT/page); HTTP/1.1 pipelining.  
  • 2.2.3 Message Format – start-line, header K:V\*, blank, body.  
  • 2.2.4 Cookies – Set-Cookie / Cookie maintain session id.

 ● 2.3 Electronic Mail  
  • SMTP push: HELO → MAIL FROM → RCPT TO → DATA → QUIT (TCP 25/587).  
  • Mail Format RFC 5322; MIME multipart.  
  • IMAP vs POP3 retrieval models.

 ● 2.4 DNS Directory Service  
  • 2.4.1 Services – hostname → IP, MX lookup, load-balance.  
  • 2.4.2 Operation – root → TLD → authoritative; recursive / iterative; caching TTL.  
  • 2.4.3 RR Types – A, AAAA, MX, NS, CNAME, TXT; UDP 53 message.

 ● 2.5 Peer-to-Peer File Distribution  
  • BitTorrent – .torrent, tracker, rarest-first pieces, tit-for-tat choking.

 ● 2.6 Video Streaming / CDN  
  • 2.6.3 CDNs – DNS or HTTP redirect selects edge; DASH client selects segment bitrate.

● Chapter 3 Transport Layer  
 ● 3.1 Introduction & Services  
  • logical end-to-end; multiplex/demux; reliable delivery; flow & congestion control.

 ● 3.2 Multiplexing / Demultiplexing  
  • src/dst ports tag segments; OS delivers to correct socket.

 ● 3.3 Connectionless UDP  
  • Header {srcPort, dstPort, len, checksum}; no handshake; apps: DNS, VoIP, QUIC.

 ● 3.4 Reliable Data Transfer  
  • 3.4.1 rdt3.0 Stop-&-Wait – seq {0,1}, ACK/NACK, timeout → reliability on loss/duplication.  
  • (3.4.2 pipelining noted, 3.4.3 GBN & 3.4.4 SR omitted).

 ● 3.5 TCP Connection-Oriented  
  • Three-way SYN → SYN-ACK → ACK setup; four-way FIN close.  
  • Segment fields – seq, ack, HLEN, rwnd, flags, options (MSS, WS).  
  • RTT/timeout – EstRTT + 4·DevRTT adaptive.  
  • RDT – cumulative ACK, fast retransmit (3 dupACK), fast recovery.  
  • Flow control – rwnd advertises receiver buffer.

 ● 3.7 TCP Congestion Control  
  • Slow-start, ssthresh, AIMD, fast recovery; fairness objective.

 ● 3.8 Summary

Chapter 4 Network Layer – Data Plane  
 ● 4.1 Overview  
  • Forwarding (per-router) vs routing (network-wide).

 ● 4.2 Inside a Router  
  • 4.2.1 Input Port – line-card, LPM lookup.  
  • (brief) 4.2.3 Output Port; 4.2.5 Scheduling FIFO, priority, WFQ.

 ● 4.3 Internet Protocol  
  • IPv4 datagram, fragmentation flags/offset.  
  • CIDR addressing; DHCP lease; ARP mapping.  
  • NAT port-mapped translation.  
  • IPv6 40-B header, no checksum; transition via tunnels / dual-stack.

 ● (brief) 4.4 Generalised Forwarding / SDN – match-action tables, OpenFlow rules.

Chapter 5 Network Layer – Control Plane  
 ● 5.1 Introduction – distributed LS/DV vs SDN centralised.

 ● 5.2 Routing Algorithms  
  • 5.2.1 Link-State (Dijkstra) O(N²).  
  • 5.2.2 Distance-Vector (Bellman-Ford); count-to-∞ solved by poison reverse.

 ● 5.3 Intra-AS OSPF – areas, cost = 1/BW, ECMP, auth.

 ● 5.4 Inter-AS BGP  
  • 5.4.1 Purpose – policy-driven ISP interconnect.  
  • 5.4.2 Advertisements – AS-PATH, NEXT-HOP.  
  • 5.4.3 Best-Path – LOCAL\_PREF → AS-len → origin → MED.  
  • (5.4.4 Anycast & 5.4.5 Policy omitted).

 ● 5.5 SDN Control Plane – controller, northbound API, OpenFlow southbound.

 ● 5.6 ICMP – echo, dest-unreach, time-exceeded.

Chapter 6 Link Layer & LANs

  ● **6.1 Intro**

• NIC implements link-layer services: framing, MAC access, error detection.

● **6.2 Error Detection/Correction**

• Parity, Internet checksum, CRC (poly division).

● **6.3 Multiple-Access Protocols**

• Channel partition (TDMA/FDMA).  
   • Random (Slotted ALOHA, CSMA/CD, CSMA/CA).  
   • Taking-turns (token, polling).  
   • DOCSIS as hybrid.

● **6.4 Switched LANs**

• 6.4.1 Link-Layer Addressing & ARP.  
   • 6.4.2 Ethernet frame ≤1500 B, exponential back-off (legacy).  
   • 6.4.3 Self-learning switches, cut-through.  
   • 6.4.4 VLAN 802.1Q tags isolate traffic.

● **6.5 Link Virtualisation (MPLS)** **omitted**.

● **6.6 Data Center Networking**

• fat-tree, ECMP, MLAG.

● **6.7 Day-in-Life**

• Walk-through DHCP→DNS→ARP→TCP→HTTP.

● **6.8 Summary**.

● Chapter 7 Wireless & Mobile

 ● **7.1 Introduction**

• Wireless spectrum, challenges: fading, interference, mobility.

 ● **7.2 Wireless Links/Characteristics**

• CDMA orthogonal codes; SNR limits rate (Shannon).

 ● **7.3 Wi-Fi 802.11**

• Architecture – BSS, ESS, scanning & association.  
   • MAC – CSMA/CA + ACK; optional RTS/CTS for hidden terminals.  
   • Frame format, addr1-4, seq ctrl, CRC.  
   • Mobility in subnet (re-associate),   
 advanced features: MIMO, frame aggregation, 802.11ax OFDMA.

### ● Chapter 8 Security

 ● **8.1 What Is Network Security?**

• Assets, threats, adversary capabilities.

 ● **8.2 Cryptography Principles**

• Symmetric (AES, 3DES) key K shared; cipher modes ECB/CBC/CTR.  
   • Public-key (RSA, DH) – kpub/kpriv, key exchange.

 ● **8.3 Message Integrity & Digital Signatures**

• Hash SHA-256 → fixed fingerprint.  
   • HMAC = hash(k⊕ipad ∥ msg ∥ k⊕opad).  
   • Signature = encrypt\_kpriv(hash).

 ● **8.5 Securing E-mail** – PGP

• Secrecy (session K encrypted w/ RSA), integrity (sig).

 ● **8.6 Securing TCP (SSL/TLS)**

• Handshake: client hello → cert+key exchange → finished; derives shared secrets; forward secrecy via (EC)DH.  
• Record Protocol: MAC-then-encrypt blocks; sequence numbers defend replay.

 ● **8.9 Operational Security**

• Firewalls: stateless ACL, stateful inspection, app-layer proxy, NGFW.  
   • Intrusion Detection Systems: signature vs anomaly; IPS can drop packets.

*(● section • sub-point — dense yet header-aligned for both quick human scan and LLM token lookup.)*

### Road-Mapping This Book

Before starting any trip, you should always glance at a road map in order to become familiar with the major roads and junctures that lie ahead. For the trip we are about to embark on, the ultimate destination is a deep understanding of the how, what, and why of computer networks. Our road map is the sequence of chapters of this book:

1. Computer Networks and the Internet
2. Application Layer
3. Transport Layer
4. Network Layer: Data Plane
5. Network Layer: Control Plane
6. The Link Layer and LANs
7. Wireless and Mobile Networks
8. Security in Computer Networks
9. Multimedia Networking

**Chapters 2** through **6** are the five core chapters of this book. You should notice that these chapters are organized around the top four layers of the five-layer Internet protocol. Further note that our journey will begin at the top of the Internet protocol stack, namely, the application layer, and will work its way downward. The rationale behind this top-down journey is that once we understand the applications, we can understand the network services needed to support these applications. We can then, in turn, examine the various ways in which such services might be implemented by a network architecture.

Covering applications early thus provides motivation for the remainder of the text.

The second half of the book—**Chapters 7** through **9**—zooms in on three enormously important (and somewhat independent) topics in modern computer networking. In **Chapter 7**, we examine wireless and mobile networks, including wireless LANs (including WiFi and Bluetooth), Cellular telephony networks

(including GSM, 3G, and 4G), and mobility (in both IP and GSM networks). **Chapter 8**, which addresses security in computer networks, first looks at the underpinnings of encryption and network security, and then we examine how the basic theory is being applied in a broad range of Internet contexts. The last chapter, which addresses multimedia networking, examines audio and video applications such as Internet phone, video conferencing, and streaming of stored media. We also look at how a packet switched network can be designed to provide consistent quality of service to audio and video applications.

## Lecture summaries:

**Chapter 1 *Introduction***

● **Internet overview** – “network of networks”; edge hosts (clients/servers) run apps; routers + links form core   
• **Protocol concept** – agreed message *syntax | semantics | timing* → governs distributed actions  
• **Edge/access tech** – DSL 24–52 Mbps ↓ / 3,5–16 Mbps ↑; cable HFC ≤ 1,6 Gbps ↓; Wi-Fi 11–2400 Mbps; 4G ≈ 10 Mbps; 5G higher  
○ **Home LAN** – modem ⇆ NAT/WAP ⇆ devices  
• **Core/switching** – store-&-forward packet switching; tier-1 ↔ regional ↔ local ISPs  
• **Performance metrics** – delay (proc + queue + tx + prop), throughput bottleneck, loss (queue overflow)  
• **Layer stack** – app, transport, network, link, physical; PDU names (message/segment/datagram/frame)  
• **Security hooks** – cryptography, firewalls, IDS (intro level)  
• **History timeline** – 1983 TCP/IP launch; 1990s Web boom; 2008 SDN; 2017 mobile > fixed devices

**Chapter 2 *Application-Layer Protocols***

● **Models** – client-server vs P2P; service needs = reliability, timing, throughput, security   
• **HTTP** – stateless, uses TCP/80; non-persistent (2 RTT/object) vs persistent (1 RTT/page); cookies, caching, HTTP/2 framing, HTTP/3 (QUIC)   
• **E-mail** – SMTP (TCP 25/587) handshake HELO–MAIL FROM–RCPT TO–DATA–QUIT; message format per RFC 5322; IMAP/POP3 retrieval   
• **DNS** – hierarchical root→TLD→authoritative; RR types A, AAAA, NS, MX, CNAME; UDP 53; caching (TTL)   
• **P2P/BitTorrent** – pieces 512 KB, tracker, tit-for-tat; self-scaling upload capacity   
• **Video streaming/DASH + CDN** – manifest + segmented files, client-side rate adaptation, edge caches

**Chapter 3A *UDP + Reliable-Data Principles***

● **Transport services** – multiplex/demux via port numbers (well-known 0-1023)   
• **UDP** – header {srcPort,dstPort,length,checksum}; no setup, no congestion ctl; used by DNS, VoIP, streaming   
• **Reliable data** – Stop-&-Wait (rdt 3.0), utilisation U=L/R ÷ (RTT+L/R); pipelining: Go-Back-N (single timer) vs Selective Repeat (per-pkt timers)

**Chapter 3B *TCP & Congestion Control***

● **TCP properties** – byte-stream, full-duplex, 4-tuple socket, reliable + flow + congestion control   
• **Segment fields** – seq, ack, window, flags (SYN,ACK,FIN), options, checksum   
• **Connection management** – three-way SYN/SYN-ACK/ACK; four-way close FIN → ACK │ FIN → ACK   
• **RDT mechanisms** – cumulative ACK, fast retransmit (3 dupACK), timeout = EstRTT + 4·DevRTT  
• **Flow control** – rwnd advertises buffer space  
• **Congestion control** – slow-start, AIMD, fast recovery; throughput ≈ MSS / (RTT·√p·2)  
• **QUIC** – user-space over UDP, multiplexed encrypted streams, 0-RTT setup

**Chapter 4 *Network-Layer I: Forwarding & SDN***

● **Data vs Control plane** – per-router forwarding vs network-wide routing/SDN   
• **Router internals** – input port → switch fabric (memory|bus|crossbar) → output port; queueing/scheduling (FIFO, priority, RR, WFQ)   
• **Forwarding logic** – longest-prefix match lookup (TCAM/trie)   
• **IP datagram** – header fields, fragmentation; IPv6 40-B base hdr, ext-hdrs  
• **Addressing/NAT** – CIDR a.b.c.d/x, private 10/172/192, port translation  
• **Generalised forwarding** – match-action flow tables (OpenFlow); actions: forward, drop, modify, send to controller

**Chapter 5 *Network-Layer II: Control Plane***

● **Routing algorithms** – Link-State (Dijkstra O(n²)) vs Distance-Vector (Bellman-Ford); count-to-∞ mitigations   
• **Intra-AS (OSPF)** – LS flooding, areas, ECMP, auth   
• **Inter-AS (BGP)** – path-vector; attributes AS-PATH, NEXT-HOP, LOCAL\_PREF; policy-driven selection; eBGP/iBGP sessions over TCP   
• **SDN controllers** – OpenFlow southbound, global view enables programmable policies  
• **ICMP** – echo, dest-unreach, time-exceeded; used by ping/traceroute

**Chapter 6 *Link Layer & LANs***

● **Service palette** – framing, MAC access, error detect/correct, flow control, reliable delivery on noisy links   
• **Error mechanisms** – checksum (16-bit), parity (1-bit / 2-D), CRC polynomial division   
• **Multiple-access families** – TDMA | FDMA | Slotted ALOHA | CSMA / CSMA-CD (legacy) | token/polling; efficiency = traffic-dependent   
• **LAN tool-kit** – MAC-48 addr, ARP resolution, Ethernet 1500-byte MTU, self-learning switches, 802.1Q VLAN tagging   
○ **Datacenter fabric** – fat-tree, ECMP, MLAG for lossless layer-2 spine/leaf   
• **Day-in-life flow** – DNS → TCP 3WH → HTTP → frames → ARP; maps layer interactions end-to-end

**Chapter 7 *Wireless & Mobile***

● **Link traits** – fading, interference, hidden/exposed terminals; no CD feasible → collision-avoid needed   
• **802.11 stack** – ISM 2.4/5 GHz, BSS/ESS, passive+active scanning, CSMA/CA with RTS/CTS, ACK-based reliability   
○ **Rates** – b 11 Mb/s, g 54, n 600, ac 3.5 Gb/s, ax 14 Gb/s; MIMO, channel bonding, frame agg   
• **Cellular** – reuse cells, LTE OFDM/EPC, 5G NR mmWave & slicing   
• **Mobility mgmt** – home/foreign agents, tunnelling; paging + handoff; transport impact mitigated by TCP Westwood/QUIC

**Chapter 8 *Network Security***

● **Goals** – confidentiality, integrity, (entity | message) authenticity, availability, non-repudiation   
• **Threat modes** – eavesdrop, modify, spoof, replay, DoS, hijack   
• **Crypto primitives** – AES, 3DES, RSA, Diffie-Hellman, hash (SHA-2), HMAC, digital sig   
• **Key infrastructure** – X.509 certs, TLS handshake, IPsec (AH/ESP) tunnels   
• **Layer defenses** – PGP/S-MIME email, WPA3 SAE Wi-Fi, stateful firewalls, IDS/IPS   
○ **Replay guards** – nonces, seq nos, timestamps

**Packet Analysis with Wireshark**

● **Ping path** – optional DNS lookup → ICMP echo req/rep; RTT stats illustrated   
• **Filters** – capture vs display, follow-stream for TCP flow reconstruction   
• **nmap scans** – ARP sweep (-sn) for host discovery; ICMP for external probing; interpret “filtered/closed” states

**TCP Socket Programming (Winsock)**

● **API sequence (server)** – WSAStartup → socket(AF\_INET, SOCK\_STREAM) → bind → listen → accept → recv/send → closesocket → WSACleanup   
• **Client handshake** – socket + connect triggers 3-way SYN/SYN-ACK/ACK   
• **Concurrency** – per-client socket returned by accept; 4-tuple distinguishes flows   
• **Diagnostics** – netstat -b, nmap port scan; firewall may block inbound port bind

**UDP Socket Programming (Winsock)**

● **API sequence (server)** – WSAStartup → socket(AF\_INET, SOCK\_DGRAM) → bind → recvfrom/sendto → closesocket → WSACleanup   
• **Client flow** – socket → sendto(target IP:port) → recvfrom for echo/response   
• **Stateless traits** – no connection, no reliability; app must handle loss/ordering  
○ **Endianness helpers** – htons/htonl ensure network (big-endian) byte order on little-endian hosts

*(Bullet legend: ● major • sub-topic ○ detail; designed for quick token lookup yet human readable.)*