SUNY OLD WESTBURY

DEPARTMENT OF MATHEMATICS AND COMPUTER & INFORMATION SCIENCE

SYLLABUS

COMPUTER NETWORKS CS 5710

Prerequisite: **CS4501** (Software Engineering) **or CS4550** (Database Management Systems), **MA3210** (Introduction to Probability & Statistics) **or MA2000** (Applied Statistics)

COURSE DESCRIPTION:
An introduction to the design and analysis of computer communication networks. Topics include application layer protocols, Internet protocols, network interfaces, local and wide area networks, wireless networks, bridging and routing, and current topics.

COURSE OBJECTIVES: As a result of successfully completing this course, students will:

1. Become familiar with layered communication architectures (OSI and TCP/IP).
2. Understand the client/server model and key application layer protocols.
3. Learn sockets programming and how to implement client/server programs.
4. Understand the concepts of reliable data transfer and how TCP implements these concepts.
5. Know the principles of congestion control and trade-offs in fairness and efficiency.
6. Learn the principles of routing and the semantics and syntax of IP.
7. Understand the basics of error detection including parity, checksums, and CRC.
8. Familiarize the student with current topics such as security, network management, sensor networks, and/or other topics.

TEXTBOOKS:
Computer Networking, 8th edition Published by Pearson By James Kurose, Keith Ross. ISBN: 0136681557 (or 0135928524)

Chapters 1-6 & 8 to be covered

TOPICS TO BE COVERED*

Chapter 1 Computer Networks and the Internet

- 1.1 What Is the Internet?
  - 1.1.1 A Nuts-and-Bolts Description
  - 1.1.2 A Services Description
  - 1.1.3 What Is a Protocol?
- 1.2 The Network Edge
  - 1.2.1 Access Networks
  - 1.2.2 Physical Media
- 1.3 The Network Core
  - 1.3.1 Packet Switching
  - 1.3.2 Circuit Switching
  - 1.3.3 A Network of Networks
- 1.4 Delay, Loss, and Throughput in Packet-Switched Networks
  - 1.4.1 Overview of Delay in Packet-Switched Networks
  - 1.4.2 Queuing Delay and Packet Loss
  - 1.4.3 End-to-End Delay
  - 1.4.4 Throughput in Computer Networks
- 1.5 Protocol Layers and Their Service Models
  - 1.5.1 Layered Architecture
  - 1.5.2 Encapsulation
- 1.6 Networks Under Attack
- 1.8 Summary
- Wireshark Lab

Chapter 2 Application Layer

- 2.1 Principles of Network Applications
  - 2.1.1 Network Application Architectures
  - 2.1.2 Processes Communicating
  - 2.1.3 Transport Services Available to Applications
  - 2.1.4 Transport Services Provided by the Internet
  - 2.1.5 Application-Layer Protocols
  - 2.1.6 Network Applications Covered in This Book
- 2.2 The Web and HTTP
  - 2.2.1 Overview of HTTP
  - 2.2.2 Non-Persistent and Persistent Connections
  - 2.2.3 HTTP Message Format
  - 2.2.4 User-Server Interaction: Cookies
  - 2.2.5 Web Caching
  - 2.2.6 HTTP/2
- 2.3 Electronic Mail in the Internet
  - 2.3.1 SMTP
  - 2.3.2 Mail Message Formats
  - 2.3.3 Mail Access Protocols
- 2.4 DNS—The Internet's Directory Service
  - 2.4.1 Services Provided by DNS
  - 2.4.2 Overview of How DNS Works
  - 2.4.3 DNS Records and Messages

2.5 Peer-to-Peer Applications
    2.5.1 P2P File Distribution
2.6 Video Streaming and Content Distribution Networks
    2.6.1 Internet Video
    2.6.2 HTTP Streaming and DASH
    2.6.3 Content Distribution Networks
    2.6.4 Case Studies: Netflix, YouTube, and Kankan
2.7 Socket Programming: Creating Network Applications
    2.7.1 Socket Programming with UDP
    2.7.2 Socket Programming with TCP
2.8 Summary

Socket Programming Assignments
Wireshark Labs: HTTP, DNS

Chapter 3 Transport Layer

3.1 Introduction and Transport-Layer Services
    3.1.1 Relationship Between Transport and Network Layers
    3.1.2 Overview of the Transport Layer in the Internet
3.2 Multiplexing and Demultiplexing
3.3 Connectionless Transport: UDP
    3.3.1 UDP Segment Structure
    3.3.2 UDP Checksum
3.4 Principles of Reliable Data Transfer
    3.4.1 Building a Reliable Data Transfer Protocol
    3.4.2 Pipelined Reliable Data Transfer Protocols
    3.4.3 Go-Back-N (GBN)
    3.4.4 Selective Repeat (SR)
3.5 Connection-Oriented Transport: TCP
    3.5.1 The TCP Connection
    3.5.2 TCP Segment Structure
    3.5.3 Round-Trip Time Estimation and Timeout
    3.5.4 Reliable Data Transfer
    3.5.5 Flow Control
    3.5.6 TCP Connection Management
3.6 Principles of Congestion Control
    3.6.1 The Causes and the Costs of Congestion
    3.6.2 Approaches to Congestion Control
3.7 TCP Congestion Control
    3.7.1 Classic TCP congestion Control
    3.7.2 Network-Assisted Explicit Congestion Notification and Delay-based Congestion Control
    3.7.3 Fairness
3.8 Evolution of transport-layer functionality
3.9 Summary

Wireshark Labs: Exploring TCP, UDP

Chapter 4 The Network Layer: Data Plane

4.1 Overview of Network Layer

6.2.2 Checksumming Methods
6.2.3 Cyclic Redundancy Check (CRC)
6.3 Multiple Access Links and Protocols
6.3.1 Channel Partitioning Protocols
6.3.2 Random Access Protocols
6.3.3 Taking-Turns Protocols
6.4 Switched Local Area Networks
6.4.1 Link-Layer Addressing and ARP
6.4.2 Ethernet
6.4.3 Link-Layer Switches
6.4.4 Virtual Local Area Networks (VLANs)
6.5 Link Virtualization: A Network as a Link Layer
6.5.1 Multiprotocol Label Switching (MPLS)
6.6 Data Center Networking
6.6.1 Data Center Architectures
6.6.2 Trends in Data Center Networking
6.7 Retrospective: A Day in the Life of a Web Page Request
6.7.1 Getting Started: DHCP, UDP, IP, and Ethernet
6.7.2 Still Getting Started: DNS and ARP
6.7.3 Still Getting Started: Intra-Domain Routing to the DNS Server
6.7.4 Web Client-Server Interaction: TCP and HTTP
6.8 Summary

Chapter 8 Security in Computer Networks

8.1 What Is Network Security?
8.2 Principles of Cryptography
8.2.1 Symmetric Key Cryptography
8.2.2 Public Key Encryption
8.3 Message Integrity and Digital Signatures
8.3.1 Cryptographic Hash Functions
8.3.2 Message Authentication Code
8.3.3 Digital Signatures
8.4 End-Point Authentication
8.4.1 Building an Authentication Protocol
8.5 Securing E-Mail
8.5.1 Secure E-Mail
8.5.2 PGP
8.6 Securing TCP Connections: SSL
8.6.1 The Big Picture
8.7 Network-Layer Security: IPsec and Virtual Private Networks
8.9 Operational Security: Firewalls and Intrusion Detection Systems
8.9.1 Firewalls
8.9.2 Intrusion Detection Systems
8.10 Summary

* The topics may vary slightly and need to be adjusted as we move through the semester.