

**University of Southern California**  
**EE450: Introduction to Computer Networks**

**Catalog Description**

Network architectures; Layered protocols, Network service interface; Local Networks; long-haul Networks; Internal Protocols; Link protocols; Addressing; Routing; Flow and Congestion Control; Applications Protocols, Network Security

**General Topics Covered**

1. Basic concepts of Networking. Network Classifications and Topologies. The concept of layered architecture modeling including OSI and the TCP/IP protocol suite. Client-server communications using Sockets
2. Physical layer functionalities including signaling, modulation, multiplexing, line coding and synchronization. Transmission media. Network performance measures including throughput, delays are presented. Data vs. signaling rates, channel bandwidth and capacity.
3. Link layer functionalities including frame synchronization, error detection and control including ARQ, flow control mechanisms including sliding windows.
4. Wide area network technologies. Circuit and packet switching. Virtual circuit switching
5. Local area network technologies including ETHERNET, Token Rings, and Wireless. Multiple-access schemes such as CSMA/CD, CSMA/CA and Token-passing. MAC addressing. Switched vs. shared ETHERNETs. Performance evaluation, including throughputs and delays, of LAN technologies
6. Interworking devices including repeaters, bridges, switches, routers and gateways. Network layer protocols, including IP, ARP and ICMP. IP addressing schemes (Classful and Classless), Subnetting and Subnet Masking
7. Internet routing including protocols used in the Internet such as RIP, OSPF and BGP. Algorithms such as Bellman-ford and Dijkstra are discussed
8. Transport layer protocols including UDP and TCP. Ports and sockets. TCP connection establishment. Error, flow and congestion control in TCP.
9. Applications layer protocols such as HTTP, FTP, DNS, SMTP, etc...
10. Basics of Network Security measures such as encryption, digital signatures, authentication, firewalls, etc..

## Course Outline (Tentative)

### ◆ Introduction/Overview

- What is a Network? Why do we need Networking?
  - Network Classifications: Switched vs. Broadcast
  - Network Classifications based on Coverage
  - Network Topologies: Bus, Ring, Hub, Mesh, fully connected, etc..
  - Network Components: Hardware/Software
  - Transmission Media: Guided vs. Unguided
  - Process to Process Communications models: Client Server, Peer to Peer, Cloud Computing models
  - Network Infrastructures: Access, Metropolitan and Core Networks
  - The Internet: Topology and Infrastructure of the Internet
  - Service Models: Reliable vs. Unreliable, Best effort vs. QoS models
  - Network Performance Measures: Latency/Throughput, BWxDelay product, etc..
  - Switching Technologies: Circuit, Packet and Virtual Circuits
- 
- **Networking Protocols and the Layered Architecture**
    - **The concept of Layered Architecture, OSI & TCP/IP Protocol Suite**
      - Protocol Layering
      - Functionalities of the various layers of TCP/IP
      - Data Transfer using the layered architecture
    - **Addressing Hierarchy**
      - MAC, IP and Port addresses
      - Communications between hosts on the same network
      - Communications between hosts on different networks
    - **Introduction to Sockets and Socket programming**
      - Classifications of Sockets: Stream Sockets vs. Datagram Sockets
      - Socket Address Structure
      - Socket Programming with TCP and UDP
      - Creation and binding of sockets. Reading and writing into sockets, etc..
      - Concurrent vs. Iterative servers

## ◆ Putting the Pieces of the Puzzle Together

- **How does a host obtain an IP address?**
  - DHCP: Dynamic Host Configuration Protocol
  - Discover, Offer, Request and Acknowledge phases of DHCP
  - DHCP relay
- **How do we map a host name into an IP address**
  - DNS: Domain Name Servers
  - Name space and DNS in the Internet
  - Types of DNS servers: Local, Root, TLD and authoritative Name Servers, Iterative vs. Recursive DNS
  - DNS caching and records
- **How do we map an IP address to a MAC address?**
  - ARP: Address Resolution Protocol
  - ARP requests and responses
  - ARP Proxies
- **How do we distinguish between Applications running in same/different machines?**
  - Port numbers: Well known and ephemerals ports.

## ◆ Physical Layer

- Functions of the Physical Layer, Data vs. Signals
- Concept of Signal Bandwidth, Channel Bandwidth, Channel Capacity, Shannon Theorem, etc...
- Modulation: Why modulate?, Classifications of Modems: Binary vs. Multilevel, Data Rates (bps) vs. Signaling rates (Baud), etc...
- A/D and D/A conversion: Sampling, Quantization and Encoding. Nyquist Theorem
- Line Coding: NRZ, Manchester codes, etc...
- Resource Sharing/Multiplexing: Frequency Division Multiplexing, Synchronous Time Division Multiplexing, Statistical Time Division Multiplexing, Wave length Division Multiplexing
- T1/T3 and the Digital Carrier System in the US.
- Access Technologies: ADSL and Cable Access architectures

## ◆ Data Link Control Protocols: Part 1: Point-to-Point Links

- Functions of the DLC layer. Typical "frame" format
- Error Detection: Single and two dimensional parity, Frame Check Sequence, generation of FCS bits, Error detection algorithm
- Error/Flow Control Mechanisms
  - Stop and Wait
  - Go-Back-N ARQ
  - Selective Repeat ARQ
  - Sliding Windows
  - Evaluation of Link utilization and throughput of the above mechanisms

## ◆ Media Access Control Protocols: Part 2: Multipoint (Shared) Links

- **Taxonomy of MAC Protocols**
  - Channel Partitioning, FDMA/TDMA/CDMA
  - Random Access: ALOHA, Slotted ALOHA, CSMA/CD and CSMA/CA
  - Controlled Access; Token Passing, Polling/Selecting and Reservations
- **Shared ETHERNETS**
  - Carrier Sense Multiple Access/Collision Detection (IEEE802.3)
  - Classifications of Shared ETHERNETS
  - Shared vs. Switched ETHERNETS
- **Wireless LANs (Wi-Fi)**
  - Classifications of Wireless LANs: Infrastructure vs. Ad-hoc
  - Problems with wireless channels
  - Carrier Sense Multiple Access/Collision Avoidance schemes (IEEE802.11)
  - Frame Addressing in Wi-Fi
  - Brief introduction to Bluetooth

## ◆ Internetworking Devices

- Classifications of Internetworking Devices
  - Shared Hubs
  - Layer 2 Switches/Bridges. Spanning Tree Algorithm
  - Routers: Architecture, Configuration, etc...
  - Gateways

## ◆ Network Layer Protocols

- **The Internet Protocol (IP)**
  - IPv.4 Packet Format
  - Fragmentation of Packets
  - IP addressing: Classful and Classless (CIDR)
  - Subnetting and Subnet Masking
  - Private IP addressing, Network/Port Address Translations
  - Introduction to IPv.6
- **Routing Protocols**
  - Routing Architecture in the Internet: Intra and Inter-Domain Routing
  - Distance Vector Routing Protocol, Dijkstra Algorithm
  - Open Shortest Path First, Bellman-Ford Algorithm
  - Path Vector. Introduction to Border Gateway Protocol
  - Hierarchical Routing in the Internet

## ◆ Transport Layer Protocols

- **The Transmission Control Protocol (TCP)**
  - TCP Segment Format
  - TCP Connection Set-up and tear down
  - Reliable Service using TCP: Error and Flow Control
  - Congestion Control in TCP: Slow Start, Congestion Avoidance, Congestion window, Tahoe/Reno/Vegas implementations
- **The User Datagram Protocol (UDP)**
  - Datagram Format
  - Unreliable Service: Error detection, Multiplexing

## ◆ Application Layer Protocols (This section is handled by TAs during a couple of discussion sessions early in the semester dedicated to these topics)

- **Hypertext Transfer Protocol (HTTP)**
  - Non-Persistent, Non-Persistent with parallel connections, Persistent, Persistent with Pipelining
  - HTTP messages
  - Client/Server interactions
  - Web Caching
- **Simple Mail Transfer Protocol (SMTP)**
  - Mail message Format
  - Mail access protocols
- **Peer-to-Peer applications: Skype**

## ◆ Introduction to Network Security

- **Components of Network Security**
  - Data Privacy via Symmetric/Public Key encryption
  - Authentication procedures
  - Data Integrity via Digital Signature
  - Access control: Firewalls (Packet/Application Firewalls)
  - Security Threats: Viruses, Worms, Denial of Service, IP spoofing/Sniffing, etc...
  - Security Protocols (Time permitting): PGP, SSL, IPSec, etc...