RETI INFORMATICHE (9 CFU)

Docente: Giuseppe Anastasi

Numero totale di ore di lezione ed esercitazioni (L: 70):
Numero totale di ore di laboratorio (E: 20):

Prerequisiti: Capacità di programmare con il linguaggio C/C++. Conoscenza di base sull'architettura di un calcolatore. Propedeuticità di *Calcolatori Elettronici.*

Obiettivi: Il corso si propone di illustrare i concetti di base sulle reti informatiche, con particolare riferimento a Internet. Vengono presentate le principali tecnologie di rete, i protocolli di Internet, e le applicazione di rete di uso più comune. Alla fine del corso lo studente sarà in grado di progettare e realizzare applicazioni di rete *client-server* e *peer-to-peer*.

Programma:

CONCETTI INTRODUTTIVI. Reti di calcolatori e Internet. La periferia di Internet (reti di accesso, dispositivi di utente, programmi client e server). Il core di Internet (commutazione di circuito e commutazione di pacchetto, router, dorsali, Internet Service Provider). Servizi e protocolli. Architettura a livelli. Architetture TCP/IP e OSI.

APPLICAZIONI DI RETE. Paradigmi client-server e peer-to-peer. Tipologie di servizio richieste dalle applicazioni. Tipologie di servizio fornite da Internet. Applicazioni Web (Protocollo http). File Transfer (Protocollo FTP). Posta Elettronica (Protocollo SMTP, MIME, Protocolli di accesso POP3 e IMAP). DNS. Applicazioni Peer-To-Peer (P2P). Ricerca di contenuti. Distribuzione/condivisione di file. Protocollo BitTorrent. Internet telephony. Skype. Programmazione di applicazioni di rete. Interfaccia a socket. Client e server comunicanti tramite socket.

RETI A CONNESSIONE DIRETTA. Collegamenti Punto-Punto. Servizi del livello Data Link. Framing. Rilevamento e correzione dell'errore. Trasferimento affidabile dei dati. Controllo di flusso. Protocolli Stop-and-Wait, Go-Back-N, Selective Repeat (SR). Point-to-Point Protocol (PPP). Accesso Multiplo. Reti Locali (LAN). Protocollo MAC (Medium Access Control). Indirizzi MAC. Ethernet (formato del frame, protocollo CSMA/CD).

RETI A COMMUTAZIONE DI PACCHETTO. Switch (Filtraggio e instradamento, Self-learning). Switched Ethernet. LAN Virtuali. Reti a commutazione di pacchetto. Circuito virtuale e datagram. Reti ATM.

INTERCONNESSIONE DI RETI. Reti di reti. Router. Protocollo IPv4. Formato del datagram. Indirizzi IPv4. Assegnazione dinamica degli indirizzi. Protocollo DHCP. Traduzione degli indirizzi (NAT). Instradamento dei datagram. Risoluzione degli indirizzi IP (Protocollo ARP). Notifica di errori. Protocollo ICMP. Protocollo IPv6. Routing. Algoritmi Link-State e Distance Vector. Routing in Internet. Autonomous System (AS). Protocolli di routing Intra-AS (RIP, OSPF) e Inter-AS (BGP).

TRASPORTO END-TO-END DEI DATI. Multiplexing/demultiplexing dei datagram. Protocollo UDP. Formato del Messaggio UDP. Protocollo TCP. Formato del segmento TCP. Apertura/chiusura della connessione. Trasferimento affidabile dei dati. Stima di Round Trip Time (RTT) e Timeout. Controllo del flusso. Principi di controllo della congestione. Controllo della congestione nel protocollo TCP.

RETI WIRELESS E MOBILI. Reti Wireless: classificazione. Reti wireless con infrastruttura. Reti locali wireless (WiFi). Accesso a Internet tramite rete cellulare. Reti con utenti mobili. Indirizzamento e Instradamento. Mobile IP. Gestione della mobilità in reti cellulari. Impatto della mobilità sul protocollo TCP. Reti wireless senza infrastruttura (Bluetooth). Reti wireless con architettura ibrida (Mesh, WSN).

RETI PER APPLICAZIONI MULTIMEDIALI. Applicazioni multimediali: classificazione e requisiti. Applicazioni di streaming. Protocollo RTSP. Content Distribution Networks (CDN). Applicazioni real-time interattive. Protocolli RTP, RTCP, SIP, H323.

SICUREZZA. Minacce alla sicurezza in rete. Principi di crittografia. Crittografia a chiave segreta e a chiave pubblica. Riservatezza della comunicazione. Distribuzione e certificazione delle chiavi. Integrità dei messaggi. Funzioni Hash. Message Authentication Code. Firma digitale. Autenticazione della controparte. Applicazioni sicure (PGP). Connessioni TCP sicure (SSL). Sicurezza a livello IP (IP-Sec). Difese di sicurezza (firewall, IDS).

Testi di riferimento:

- J. Kurose, K. Ross, *Computer Networking, A Top-Down Approach - Fifth Edition*, Pearson Addison Wesley
- Altro materiale didattico fornito dal docente

Modalità di svolgimento dell'esame:

- **Prova orale** + realizzazione di un **progetto**. La discussione del progetto avviene preliminarmente alla prova orale. Quest'ultima ha luogo *solo se* il progetto ha ottenuto una valutazione almeno sufficiente.