

## Programma svolto nel modulo di RETI DI CALCOLATORI/A (a.a. 2011/2012)

### Introduzione al corso

- Obiettivi del corso, cenno ai contenuti, testo di riferimento, organizzazione del corso, modalità d'esame

### Introduzione alle reti

- Ingredienti base delle reti  
host, router, reti di accesso e collegamenti fisici, applicazioni, servizi (non)orientati alle connessioni, protocolli, reti a commutazione di circuito e a commutazione di pacchetto
- Ritardi e perdite nelle reti a commutazione di pacchetto  
ritardo di elaborazione, di coda, di trasmissione, di propagazione
- Strutturazione delle reti in livelli  
livelli, servizi, protocolli; modello TCP/IP; comunicazione logica e comunicazione fisica tra livelli

→ [KR08] Capitolo 1 (esclusi "1.6 Reti sotto attacco" e "1.7 Storia del computer networking e di Internet")

### Il livello application

- Concetti generali  
applicazioni, protocolli, agenti utente, processi, caratteristiche dei servizi di livello trasporto TCP e UDP, API
- World Wide Web  
pagine Web, URL; il protocollo HTTP: caratteristiche del protocollo, connessioni (non) persistenti, tipi di messaggi, cookies, Web caching e GET condizionale
- Protocollo FTP  
caratteristiche del protocollo, comandi
- Email  
agenti utente, funzionamento dei mailserver, il protocollo SMTP, formato dei messaggi, MIMES, cenno ai protocolli di accesso alla email (POP3,IMAP,HTTP)
- Domain Name System  
indirizzi IP, alias, domini, caratteristiche e ruolo del DNS, tipi di server DNS, query ricorsive e iterative, caching, record e messaggi DNS

→ [KR08] Capitolo 2 (esclusi "2.6 Applicazioni peer-to-peer", "2.7 Programmazione socket con TCP" e "2.8 Programmazione socket con UDP")

### Il livello transport

- Concetti generali  
(de)multiplexing, relazione con i livelli application e network, formato segmenti di trasporto
- Protocollo UDP  
caratteristiche, formato segmenti
- Protocollo Alternating Bit  
meccanismi per il trasferimento affidabile dei dati: error detection, riscontri, ritrasmissioni, numeri di sequenza, timer
- Protocolli pipelined per il trasferimento affidabile dei dati  
GBN, SR
- Protocollo TCP  
caratteristiche del protocollo (connessioni, numeri di sequenza e di riscontro, ritrasmissioni, stima RTT, formato segmenti, raddoppio intervallo timeout, ritrasmissione veloce, generazione dei riscontri), gestione delle connessioni, controllo di flusso, controllo di congestione

→ [KR08] Capitolo 3 (esclusi "3.6 Principi del controllo di congestione" e "3.7.1 Equità")

### Il livello network

- Concetti generali  
(de)multiplexing, relazione con i livelli transport e link, relazione tra instradamento-routing e inoltro-forwarding
- Protocollo IP  
formato dei datagram, frammentazione, indirizzi IP, CIDR
- Caratteristiche di DHCP, ICMP, NAT, IPv6
- Algoritmi di routing  
algoritmi link state e distance vector, routing gerarchico
- Routing in Internet  
Protocolli RIP, OSPF e BGP
- Routing broadcast  
flooding incontrollato e controllato, alberi di copertura

→ [KR08] Capitolo 4 (esclusi "4.2.1 Reti a circuito virtuale", "4.3 Cosa si trova all'interno di un router?", "4.4.5 Breve panoramica sulla sicurezza IP" e "4.7.2 Multicast").

## Il livello link

- Concetti generali  
relazione col livello network, tipi di collegamento, servizi offerti, adattatori
- Protocolli di accesso multiplo  
a suddivisione del canale (TDM,FDM), ad accesso casuale ([slotted] Aloha, CSMA/CD), a rotazione (polling, token passing)
- Reti locali
- Indirizzi fisici e protocollo ARP

→ [KR08] Capitolo 5: paragrafi "5.1 Livello di collegamento: introduzione e servizi", "5.3 Protocolli di accesso multiplo", "5.4 Indirizzi a livello di collegamento" e "5.5.2 CSMA/CD".

## Sicurezza nelle reti

- Esempi di problemi di sicurezza nelle reti  
packet sniffing, IP spoofing
- Riservatezza  
principi di crittografia con chiavi simmetriche e asimmetriche
- Integrità dei messaggi  
MAC, firme digitali, certificati
- Autenticazione end-to-end  
protocolli, nonce, attacchi "man-in-the-middle"
- Rendere sicura la posta elettronica  
utilizzo di crittografia e firme digitali, PGP
- Rendere sicure le connessioni TCP  
SSL

→ [KR08] Paragrafo "1.6 Reti sotto attacco"; capitolo 8 fino a "8.6 Rendere sicure le connessioni TCP: SSL" incluso.

## Introduzione alle applicazioni peer-to-peer

- Architetture basate su directory centralizzata, query flooding con raggio limitato, super-peer, DHT

→ [KR08] "2.6 Applicazioni peer-to-peer"

→ [Cho03] "IV. The Chord Protocol"

## Riferimenti

[KR08] J. Kurose e K. Ross. *Reti di calcolatori e Internet*. (quarta edizione) Pearson-Addison Wesley, 2008.

[Cho03] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, H. Balakrishnan. Chord: A Scalable Peer-to-peer Lookup Protocol for Internet Applications. *IEEE/ACM Transactions on Networking*, 11(1), 2003.  
<http://pdos.csail.mit.edu/chord/papers/paper-ton.pdf>