

Esame di **Progettazione di servizi web e reti di calcolatori (01NBE)**

Corsi di Laurea in Ing. Gestionale e dell'Organizzazione d'Impresa

Prova scritta di teoria (22/6/2022)

Esercizio 1 (punti: 6)

Spiegare il funzionamento dei campi SYN, ACK, SequenceNumber e AcknowledgmentNumber in un segmento TCP, indicandone la correlazione e facendo un esempio con valori concreti.

Esercizio 2 (punti: 6)

Disegnare lo schema di una delle due possibili architetture web 3-tier, illustrarne i componenti e discuterne vantaggi e svantaggi.

Esercizio 3 (punti: 5)

Spiegare che cosa è la codifica *chunked* presente in HTTP/1.1, come viene implementata, in quale tipo di trasmissione è importante e quale problema si aveva in HTTP/1.0 in cui tale codifica è assente.

Esercizio 4 (punti: 6)

Spiegare cosa sono i seguenti tipi di nameserver e per ciascuno dire come si fa ad identificarlo: *root*, *primary*, *secondary*.

Esercizio 5 (punti: 5)

Un server web con scheda di rete a 100 Mbps è collegato ad una rete locale di ateneo che opera a 1 Gbps ed a cui si accede dai laboratori didattici. Il laboratorio L1 è collegato tramite uno switch con porte a 100 Mbps verso gli utenti e scheda di rete a 1 Gbps verso il backbone. Il laboratorio L2 è collegato tramite un access point wireless a 54 Mbps con scheda di rete a 1 Gbps verso il backbone. Sono attivi simultaneamente 30 studenti, di cui 20 presenti nel laboratorio L1 e 10 nel laboratorio L2. Ogni studente opera tramite un laptop con scheda Ethernet a 100 Mbps e scheda wireless a 54 Mbps.

Sapendo che gli studenti del laboratorio L1 scaricano dal server un file da 100 MB mentre quelli del laboratorio L2 scaricano un file da 10 MB, calcolare il tempo minimo entro cui tutti gli studenti avranno ricevuto il file richiesto.

Esercizio 6 (punti: 5)

Se un utente A crea un messaggio cifrandolo con la chiave pubblica di un altro utente B, chi e come potrà leggere il contenuto del messaggio cifrato? quale funzionalità di sicurezza è stata ottenuta?

Se invece l'utente A crea un messaggio cifrandolo con la propria chiave privata, chi e come potrà leggere il contenuto del messaggio cifrato? quale funzionalità di sicurezza è stata ottenuta?