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)

> NOTA
> Le tracce delle soluzioni fornite in questo testo sono da considerarsi solo come un aiuto per comprendere i principali punti da toccare nel risolvere gli esercizi proposti ma non sono né esaustive né presentate in forma adeguata per l'elaborato da consegnarsi in sede d'esame.
> In particolare per molti esercizi le soluzione è volutamente schematica e ci si attende che il candidato spieghi adeguatamente i singoli punti, per dimostrare reale comprensione dell'argomento invece che semplice capacità mnemonica di ricordare i punti elencati nelle slide (o in queste tracce di soluzione).

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.

Traccia di una possibile risposta

SYN e ACK sono flag mentre SN ed AN sono campi numerici, tutto all'interno dell'header di un segmento TCP.

Se SYN=1 si tratta del primo segmento di una trasmissione ed il SN indica la posizione iniziale nello stream di dati da cui partire per inserire i dati trasmessi nei segmenti successivi. Ad esempio, SYN=1 e SN=30 indica che i dati trasmessi nei segmenti successivi dovranno essere inseriti a partire dalla posizione 31.

Se SYN=0 si tratta di un segmento dati ed il SN indica la posizione nello stream di dati da cui partire ad inserire i dati trasmessi nel segmento stesso. Ad esempio, SYN=0 e SN=64, indica che i dati contenuti nel segmento devono occupare le posizioni 64, 65, 66, . . .

Se ACK=1 allora AN conterrà la posizione dell'ultimo dato ricevuto correttamente. Ad esempio, ACK=1 e AN=70 indica che tutti i dati sino alla posizione 70 sono stati ricevuti correttamente ed il prossimo che ci si aspetta di ricevere è quello della posizione 71.

Se ACK=0, il segmento non indica nessuna conferma per dati già ricevuti ed il campo AN non è significativo.

Esercizio 2 ***(punti: 6)***

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

Traccia di una possibile risposta

Le architetture web sono composte da un'interfaccia utente, divisa tra parte client (implementata dal browser) e parte server (implementata da un server HTTP), la logica applicativa ed i dati.

In un'architettura web 3-tier, il primo livello è sempre il browser, il secondo livello è il server HTTP che può ospitare anche la logica applicativa (delegando al terzo livello solo la gestione dei dati) oppure la logica applicativa è ospitata sul terzo livello insieme ai dati.

Per lo schema si vedano le slide intitolate "3-tier: modello web (caso I)" e "3-tier: modello web (caso II)".

Vantaggi e svantaggi di ciascuna soluzione sono relativi al carico sui vari livelli.

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.

Traccia di una possibile risposta

La codifica chunked serve a trasmettere una risposta la cui dimensione non è nota a priori e non è quindi possibile dichiararne la dimensione tramite l'header Content-length.

In HTTP viene implementata dichiarando nell'header "Transfer-encoding: chunked" e poi trasmettendo nel body la risposta frammentata. Ogni frammento è preceduto dalla sua dimensione in byte, espressa in esadecimale.

Risolve il problema delle risposte generate dinamicamente (come quelle prodotte da uno script PHP).

In HTTP/1.0 se una risposta dinamica veniva troncata a causa di un problema di rete, il client non poteva accorgersene perché non sapeva quanti dati doveva ricevere e quindi poteva erroneamente credere di aver ricevuto tutta la risposta.

Esercizio 4 ***(punti: 6)***

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

Traccia di una possibile risposta

Un NS di tipo root è uno dei NS mondiali che gestiscono il dominio "." ed hanno informazioni su tutti i domini di primo livello. La lista dei root NS e pubblicata in Internet e deve essere configurata manualmente su un NS affinché esso possa operare correttamente.

Un NS di tipo primary è il NS master di un certo dominio (es. "polito.it.") e mantiene quindi i dati di tale dominio in forma editabile (dal sistemista con le dovute autorizzazioni). Per conoscere il primary di un certo dominio bisogna fare una query di tipo SOA per tale dominio.

Un NS di tipo secondary è un NS slave di un certo dominio (es. "polito.it.") e mantiene quindi una copia (in sola lettura) dei dati di tale dominio, ottenuti dal primary. Per conoscere i secondary di un certo dominio bisogna fare una query di tipo NS per tale dominio (così si ottiene la lista di tutti i NS di tale dominio) e poi escludere da tale lista il primary (ottenuto tramite query SOA).

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.

Traccia di una possibile risposta

Il collo di bottiglia è la scheda di rete sul server, quindi inizialmente per ciascun utente è disponibile una banda pari a:

$$100\,\text{Mbps}/30 = 3.33\,\text{Mbps}$$

Gli studenti in L2 avranno terminato dopo un tempo pari a:

$$10 \cdot 8/3.33 = 24\,\text{s}$$

A questo punto anche gli studenti in L1 avranno scaricato la stessa quantità di dati ma ora la loro velocità aumenterà a:

$$100\,\text{Mbps}/20 = 5\,\text{Mbps}$$

Quindi per scaricare i restanti dati impiegheranno:

$$90 \cdot 8/5 = 144\,\text{s}$$

Il tempo totale affinché tutti gli stduenti abbiano scaricato i relativi file sarà:

$$24 + 144 = 168\,\text{s}$$

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?

Traccia di una possibile risposta

Nel primo caso, solo l'utente B (che detiene la chiave privata corrispondente alla chiave pubblica usata per la cifratura) potrà leggere il contenuto del messaggio cifrato decifrandolo con la sua chiave privata; si è quindi ottenuta la proprietà di riservatezza (senza aver condiviso chiavi segrete).

Nel secondo caso, qualunque persone potrà leggere il contenuto del messaggio, decifrandolo con la chiave pubblica di A (che è appunto pubblica); in questo modo si è ottenuta l'autenticazione del mittente perché solo lui detiene la chiave privata usata per cifrare il messaggio.