Eserciziario - Reti di calcolatori

VR443470

gennaio 2023

Indice

Prefazione

Questo eserciziario è stato creato con il solo scopo di ripassare i concetti principali, attraverso i temi d'esame presentati durante gli anni accademici. Il documento è scritto da uno studente universitario. Di conseguenza, qualsiasi concetto proposto ***potrebbe*** essere errato. Si consiglia al lettore, di far riferimento al libro di testo e al professore per avere informazioni dettagliate e attendibili.

Il testo propone diversi temi d'esame con le classiche 3 domande di teoria iniziali e 3 esercizi. Ad ogni quesito teorico viene fornita una risposta completa, cercando di esporre i concetti in maniera chiara. Allo stesso modo, gli esercizi pratici presentano dei grafici e i vari calcoli per cercare di essere i più delucidanti possibili.

Infine, il documento presenta anche una serie di riferimenti agli esercizi affrontati e una tabella contenente le domande proposte nei temi d'esame. In questo modo, il lettore avrà un riferimento ordinato nel caso in cui, per esempio, voglia rivedere un argomento specifico.

Fonti delle informazioni presentate nel documento:

- Docente del corso di Reti di calcolatori - UniVR: Carra Damiano
- Libri del corso consigliati dal docente:
  1. Libro utilizzato dal sottoscritto:
     - Autori: *James F. Kurose, Keith W. Ross*
     - A cura di: *Antonio Capone, Sabrina Gaito*
     - Titolo: Reti di calcolatori e internet. Un approccio top-down. (7^a edizione)
     - ISBN-13: 978-8891902542
     - Link Amazon (no ref)
  2. Altro libro consigliato:
     - Autori: *Andrew S. Tanenbaum, David J. Wetherall*
     - Traduttore: *Dario Maggiorini, Sabrina Gaito*
     - Titolo: Reti di calcolatori. (5^a edizione)
     - ISBN-13: 978-8891908254
     - Link Amazon (no ref)

1 Temi d'esame

1.1 Esame - 05/02/2013

1.1.1 Domande sulla teoria

Le domande di teoria sono le seguenti:

1. Si descriva il problema del "terminale nascosto" (*hidden terminal problem*) nelle Wireless LAN e la soluzione adottata dallo standard 802.11.

2. In riferimento al livello di rete, si spieghi che cosa succede quando un host si connette ad una rete ed ha bisogno di ricevere un indirizzo IP (non è necessario andare nei dettagli dei protocolli, è sufficiente descrivere a grandi linee i messaggi scambiati).

3. L'header del protocollo UDP contiene solo 4 campi: Source Port, Destination Port, Length e Checksum. Si spieghi brevemente a cosa servono tali campi.

Risposte

1. Si supponga esistano tre stazioni A, B e C. La stazione A e C stanno trasmettendo certi dati alla stazione B. In questo scenario, si introduce il problema del terminale nascosto, il quale nasce per **due motivi**:

   - Gli **Ostacoli fisici**. Potrebbero essere presenti nell'ambiente impedimenti fisici che non consentono alle due stazioni trasmettenti (A, C) di sentirsi a vicenda, nonostante la destinazione sia la medesima.
   - **Fading (evanescenza)**. Potrebbe manifestarsi un fenomeno fisico, appunto l'evanescenza, che crea una collisione. Questo problema non viene rilevato dalla stazione ricevente.
     In altre parole, il trasmittente invia il segnale, ma a causa di una continua variazione d'intensità del segnale tra il valore massimo e quello minimo (*fading*), il destinatario riceve un segnale compromesso pensando che sia corretto. Questo accade perché il destinatario non può rilevare la collisione.

   La **soluzione** presentata dal **protocollo MAC 802.11** è quella di includere uno schema di prenotazione. Vengono creati due frame di controllo chiamati: RTS (*request to send*) e CTS (*clear to send*). Il primo viene inviato dal mittente al destinatario, indicando il tempo di connessione nel campo DATI; il secondo viene inviato dal destinatario una volta ricevuto l'RTS. Il *clear to send* viene **inviato in broadcast**, in questo modo viene comunicato a ciascun host collegato di non disturbare la comunicazione.
   Tale soluzione risolve il problema poiché il frame DATI viene trasmesso solamente una volta prenotato il canale tramite il frame RTS.

2. I messaggi scambiati durante l'assegnazione dell'indirizzo IP ad un host, sono 4: DHCP discover, DHCP offer, DHCP request, DHCP ACK:

   (a) **DHCP discover**, ovvero individuazione del server. Il mittente si collega alla rete e cerca di individuare un server. Per farlo, invia un segmento UDP, chiamato DHCP discover, in broadcast a tutti i server presenti nella rete. Al momento della connessione, il mittente ha come indirizzo IP speciale 0.0.0.0 e come indirizzo IP destinatario 255.255.255.255 (*broadcast address*).

   (b) **DHCP offer**, ovvero offerta del server. Qualsiasi server presente all'interno della rete, che è interessato a fornire un indirizzo IP al mittente, risponde al segmento precedente inviando un DHCP offer. Anche in questo caso, il destinatario invia il messaggio in broadcast specificando inoltre:

   - ID univoco rappresentante l'identificativo del messaggio ricevuto;
   - Indirizzo IP offerto al mittente;
   - Maschera della sottorete;
   - Durata di connessione (*lease time*), ovvero la durata di tempo in cui l'indirizzo IP offerto sarà valido.

   (c) **DHCP request**, ovvero richiesta. Una volta che il mittente ha valutato tutte le offerte, risponde al server inviando un segmento DHCP request. Da adesso, i messaggi non saranno più in broadcast ma *end-to-end*.

   (d) **DHCP AKC**, ovvero conferma. Il destinatario riceve la richiesta del mittente e risponde con un messaggio di conferma (ACK). Con quest'ultimo messaggio viene convalidato l'indirizzo IP, e gli altri campi, proposti al mittente.

3. Il protocollo UDP ha come intestazione solo quattro campi tutti da 16 bit. Il campo **porta di origine** (*Source Port*) e **porta di destinazione** (*Destination Port*), vengono utilizzati principalmente dal destinatario. In particolare, il *socket* del destinatario, utilizzando questi due campi, saprà a quale processo passare i dati presenti nel segmento UDP. Il campo ***Checksum*** viene inserito dal mittente per consentire al destinatario di verificare l'integrità del pacchetto. Dato che esso è una sequenza di bit calcolata tramite un algoritmo, il destinatario calcola questo valore e verifica che il pacchetto non sia stato compromesso. Infine, la **lunghezza** (*Length*) rappresenta la somma dell'intestazione (*header*) e il campo DATI. Dato che quest'ultimo è variabile, grazie a questo campo si è a conoscenza della lunghezza ed è possibile distinguere un segmento UDP dal successivo.