PROTOCOLLI PER TRASMISSIONE DATI

Tema di Esame - 16 Aprile 2003

Soluzioni

1. *Definire formalmente il traffico smaltito S e il traffico offerto G per un generico protocollo MAC. Considerando il protocollo di accesso Slotted-ALOHA e una popolazione di clienti infinita, dimostrare la relazione tra G ed S, discutendo tutte le ipotesi del modello utilizzato.*

   Per traffico smaltito si intende la quantità di PDU per unità di tempo consegnate con successo agli utenti. Per rispettare le condizioni di equilibrio del sistema, esso coincide anche con la quantità di PDU offerte dagli utenti al canale. Il traffico offerto è dato invece dal numero di PDU per unità di tempo che vengono generate dalle stazioni e che possono essere consegnate o meno con successo. Esso include dunque anche tutte le PDU ritrasmesse in seguito a collisioni.

   Per il calcolo di G ed S fare riferimento alle dispense del corso.

2. *Descrivere un possible algoritmo di sincronizzazione di trama che può essere adottato da apparati Sonet/SDH.*

   Si identificano 4 stati possibili: (S)earch, (C)onfirmed, (F)ound, (L)ost. All'accensione, il terminale si posiziona nello stato (S) e continua a monitorare le sequenzedi bit ricevuti al fine di trovare le parole di sincronizzazione posizionate ad inizio di ogni trama. Quando queste vengono trovate, esso si muove nello stato (C) dove attende esattamente una trama e poi si aspetta di ritrovare la parola di sincronizzazione. Se questo avviene con successo, si sposta nello stato (F) dove si dichiara sincronizzazione avvenuta. Altrimenti si ritorna nello stato (S). Una volta nello stato (F), l'apparato verifica la corretta sincronizzazione ad ogni trama. Nel caso la parola di sincronizzazione non sia presente, esso si sposta nello stato (L) prima di dichiarare persa (S) la sincronizzazione.

   Gli stati (C) e (L) prendono il nome di "volano di sincronizzazione".

3. *Spiegare in Ethernet il meccanissmo di backoff, discutendo (i) quando viene attivato, (ii) cosa serve e (iii) come funziona.*

   Il meccanismo di backoff entra in azione nel tempo di calcolo di attesa prima di una ritrasmissione in seguito a collisione rivelata dalla sorgente. Questo meccanismo prevede che le stazioni coinvolte nella collisione attandano un tempo casuale prima di ritrasmettare il frame. Tale tempo e' estratto casualmente secondo una d.d.p. uniforme, $U[0:M]$, ove M e' funzione del numero di collisioni consecutive. In particolare per lo standard Ethernet $M = min(2^{k-1}, s^10)$, ove k e' il numero di collisioni consecutive.

Questo meccanismo permette di separare nel tempo le ritrasmissioni, e di dilatare, nel caso di ripetuta collisione, la possibilit'a di un nodo di poter tentare di impossessarsi del canale.

4. *In una rete FDDI, scrivere la formula per calcolare il numero di pacchetti presenti nell'anello se: d = dimensione dell'anello in km; p = dimensione del pacchetto in byte; v = velocità della rete in Mbps. (c= velocità luce)*

$$N = \frac{d}{2/3c}\frac{v}{p}$$

5. *Discutere l'impatto delle dimensioni del pacchetto più piccolo in una rete Ethernet, Token-Ring e FDDI, in relazione al protocollo MAC adottato.* In una rete ethernet: più i pacchetti sono piccoli, più alta e' l'impatto delle collisioni. Infatti, a parit'ị traffico offerto, le stazioni devono contendere più volte per il possesso del canale, causando un incremento della possibilità di collisioni e quindi un aumento del traffico offerto a discapito di quello smaltito.

   In una rete Token Ring: i pacchetti non possono superare una lunghezza massima, dettata dal token holding time. L'impatto di pacchetti piccoli riduce il traffico smaltito, in quanto rende non trascurabile il tempo di trasmissione del token rispetto al tempo di trasmissione delle trame. Vengono invece ridotti i tempi di accesso al canale nel caso di tante stazioni collegate.

   In una rete FDDI: come in token ring, eccetto che il tempo di accesso massimo e' limitato comunque dal fatto che il Token Rotation Time è limitato.

   In tutti i casi, si ha un ovvio spreco di risorse dovuto all'incidenza maggiore dell'intestazione rispetto ai dati utili.

6. *In una rete Internet, si osservano le seguenti dimensioni di pacchetto: $L_1 = 40$ byte (con probabilità $p_1 = 2/3$) e $L_2 = 1500$ byte (con probabilità $p_2 = 1/3$). I Router sono connessi da una rete ATM, ove un circuito virtuale commutato permanente è usato come collegamento punto-punto usando AAL5. Calcolare valore medio di perdita di throughput dovuto alla segmentazione dei pacchetti in celle, considerando i contributi dovuti all'adozione di AAL5 e quindi di ATM.*

   I pacchetti di 40 byte sono incapsulati in una PDU AAL-5 aggiungendo 2 byte riservati, 2 byte di indicazione lunghezza, 4 byte di CRC 0 byte di padding, per un totale di 48 bytes. I 48 bytes sono poi trasformati in una cella ATM aggiungendo 5 byte di intestazioni. Totale 53 bytes.

   I pacchetti di 1500bytes sono incapsulati in x PDU AAL-5 aggiungendo 2 byte riservati, 2 byte di indicazione lunghezza, 4 byte di CRC, per un totale di 1508 bytes. Segmentando 1508 in payload non superiori a 48

byte si ottengono 32 celle, di cui 28 bytes di payload. A ciascuna cella vanno poi aggiunti 5 byte di intestazione ATM.

La perdita di throughput risulta quindi in

$$1 - \frac{1}{3}\frac{40}{40+8+5} + \frac{2}{3}\frac{1500}{1500+8+28+5*32}$$

7. *In quali protocolli di routing interno ed esterno può accadere il fenomeno di "counting to infinity"? Quali possibili soluzioni possono essere adottate per affrontare il problema? Come funzionano? Sono soluzioni sempre efficaci?*

   In fenomeno del Count to infinity è presente in tutti i protocolli Distance Vector. Quindi Rip-v1, Rip-v2, IGRP sono alcuni esempi di implementazioni di DV protocol che soffrono di questo problema.

   Non esistono soluzioni al problema, che puo' essere alleviato con meccanismi tipo "Split horizon" (non viene comunicato al vicino la raggiungibilità che il nodo vede attraverso il vicino stesso), e "Split horizon with poisonous reverse" (in cui si comunica al vicino destinazione irraggiungibile nel caso il next hop sia il vicino stesso).

8. *Descrivere il protocollo BOOTP, ponendo particolare attenzione alla costruzione degli indirizzi dei vari livelli di protocollo che devono essere indicati nei messaggi di richiesta e risposta.*

9. *Si consideri una rete wireless IEEE 802.11. Perchè in tale rete non si utilizza mai un protocollo CSMA con Collision Detection? Il Carrier Sense è sempre efficace?*

   Il protocollo CSMA/CD si basa sull'ipotesi che tutti coloro che hanno colliso siano in grado di individuare (i) canale libero (ii) eventuale collisione sul canale. Purtroppo nel caso di canale radiomobile, la presenza di terminali nascosti non permette il corretto funzionamento di CSMA/CD, in quanto entrambe le ipotesi NON sono verificate. E' infatti possibile che una stazione senta il canale libero, pur essendo presente un'altra stazione che stia gia' trasmettendo, a causa di segnali deboli o ostacoli lungo la proposagazione. Allo stesso modo non e' sempre possibile individuare le collisioni. Si usa pertanto una protocollo CSMA/Collision Avoidance, dove si fa precedere la trasmissione da una fase di prenotazione esplicita delle risorse.