DMIF, Università degli Studi di Udine — II appello A.A. 2020-21 — 16 febbraio 2021

Esame di **Reti di Calcolatori**

Soluzione

1. Si supponga di realizzare una rete a commutazione di pacchetti usando una tecnologia di collegamento punto-punto che garantisce la consegna affidabile a livello datalink, a meno di guasti completi del collegamento. (a) Cosa può fare un nodo se si accorge che un collegamento è guasto? (b) È necessario implementare altri meccanismi di gestione errori ai livelli superiori (es. trasporto)?

   R: (a) può cambiare le proprie tabelle di inoltro in modo da trovare un'altra strada per i pacchetti. (b) sì, è necessario gestire il riordinamento, perché i pacchetti possono arrivare fuori ordine facendo strade diverse, e comunque possono andare persi lo stesso a causa di rotture dei nodi.

2. Nei sistemi radio DAB e DAB+, i dati sono codificati mediante simboli (OFDM); ogni simbolo porta 3072 bit e dura 1,246 ms. Ogni frame contiene 76 simboli, e i frame sono separati da una pausa di 1,304 ms. (a) A quanto equivale il bitrate grezzo di tale trasmissione? (b) Se il canale usato ha una larghezza di banda di 1536 kHz, quanto dev'essere il rapporto S/N minimo per una trasmissione senza errori?

   R: (a) La durata di un frame è $1,246 * 76 + 1,304 = 96$ ms. Il bitrate è 3072*76/96=2432 kbps=2,432 Mbps. (b) Per SH è $C = B \log_2(1 + S/R)$. Quindi $2,432 * 10^6 = 1,536 * 10^6 * \log_2(1 + S/R)$ da cui $2^{1,583} = 3 = 1 + S/R$ da cui S/R = 2, ovvero 3 dB.

3. Un certo dispositivo di rete utilizza il CRC FOP-4, il cui polinomio generatore è 10111. Riceve la sequenza di bit 110101101010. È corretto (e in tal caso, qual è la parte dati) o contiene degli errori?

   R: Basta fare la divisione, e si vede che il resto non è zero, quindi è sbagliato.

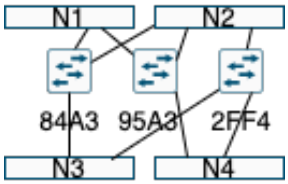
```
11010110 1010 | 10111
10111
=====
 11011
 10111
 =====
  11001
  10111
  =====
   11100
   10111
   =====
    1011 1
    1011 1
    ======
         0010
```

4. Una certa linea viene utilizzata con il protocollo *sliding window*. Le finestre di ricezione e invio hanno dimensione RWS = SWS = 8 frame. Quanti bit bisogna utilizzare per l'etichetta di ogni frame?

   R: RWS e SWS devono essere strettamente minore della metà del massimo numero assegnabile alle etichette più 1; ossia, il numero massimo assegnabile alle etichette deve essere almeno 2*RWS-1. In questo caso, 2*8-1 = 15, per cui servono 4 bit.

5. In una piconet Bluetooth c'è solo un master e uno slave che stanno trasmettendo in modalità multislot, a 3 slot alla volta. Ricordando che un bit dura 1μs, uno slot 625μs, c'è una pausa di 16 bit tra un frame e l'altro, e ogni frame ha 126 bit di intestazione, si calcoli la banda utile massima da master a slave.

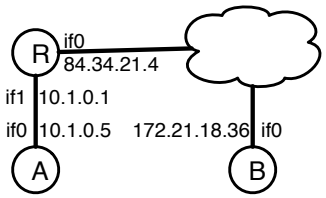
R: Ogni frame occupa 3*625 μs = 1875 μs, e porta 1875-(16+126)=1733 bit di payload. La banda è quindi di 1733/1875 = 924 kb/s, ma che va divisa per 2, arrivando a 462 kb/s.

6. Nella rete a lato è composta da 4 segmenti di rete, connessi da tre switch che implementano lo spanning tree. (a) Quando si raggiunge la stabilità, ci sono switch disattivati? se sì quali? (b) Se 2FF4 si guasta, quali rami rimangono connessi tra loro (fino a nuova stabilizzazione)?


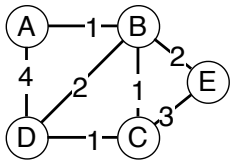
R: (a) Sì, 95A3 si disattiva. (b) N1 e N3 attraverso 84A3, mentre N2 e N4 rimangono sconnessi .

7. Un router riceve un pacchetto IP con un payload di 1000 byte, che deve essere trasmesso su una linea con MTU=256 byte. (a) Quanti pacchetti vengono trasmessi, complessivamente? (b) Qual è l'overhead aggiunto dalla framentazione, in percentuale?

   R: (a) Il maggiore multiplo di 8 inferiore a 256-20=236 è 232. Quindi si mandano 4 frammenti da 232 byte di payload, più uno con 72 byte di payload. Totale 5 pacchetti. (b) visto che ci sono 4 intestazioni in più, abbiamo 80 byte di overhead, ossia 80/1020=7,8%.

8. Il router R in figura implementa NAT per collegare la rete privata 10.1.0.0/24 al resto della rete. L'host A, porta 43234, ha stabilito una connessione TCP con B, porta 80. (a) Qual è la porta destinatario che l'host B deve usare nei pacchetti che invia? (b) Se un altro host C con indirizzo 151.65.34.2 invia un pacchetto IP alla stessa porta, tale pacchetto viene recapitato a A?


R: (a) Quella assegnata dinamicamente da router R alla connessione (che può essere diversa da quella usata da A) (b) No, perché il NAT tiene memoria dell'indirizzo IP della controparte, quindi un pacchetto con mittente sbagliato viene scartato.

9. I router della rete a lato utilizzano un algoritmo di routing basato sullo stato delle linee; i numeri rappresentano il ritardo introdotto dalla linea (p.e. in ms). (a) Quante entry contiene la tabella LSP di ogni nodo? (b) Dopo che si è stabilizzato, qual è la distanza tra A e D? (c) Se la linea D-C si interrompe, dopo quanto tempo A lo viene a sapere?


R: (a) Per poter applicare Dijkstra bisogna conoscere l'intero grafo, quindi bisogna conoscere lo stato di ogni collegamento. Quindi servono 7 entry. (b) 3 (c) 2 (lo sa da C via B).

10. Nel routing interdominio con BGP: (a) che differenza c'è tra un AS "stub" e uno "multihomed"? (b) È possibile che uno stub diventi multihomed, e viceversa?

    R: (a) Lo stub è connesso ad un solo altro AS, quindi è una foglia della rete degli AS. (b) Uno stub diventa multihomed se si aggiunge un nuovo collegamento verso un altro AS (e lo speaker annuncia di conseguenza). Analogamente se si toglie un collegamento e ne rimane uno solo.

11. Un'applicazione sta ricevendo un flusso di 15 datagrammi UDP al secondo, con payload medio di 1000 byte. (a) Quant'è il bitrate utilizzato dai pacchetti IP di tale trasmissione? (b) Se si vuole avere 2 secondi di tempo per farsi rispedire eventuali pacchetti perduti, l'applicazione quanti kbyte deve bufferizzare?

    R: (a) 1000+8+20=1028 byte = 8224 bit per pacchetto IP, da cui 123.360 b/s = 123,4 kb/s. (b) 2*15*1000=30.000 byte = 30 kB.

12. Un host TCP ha appena ricevuto un segmento con `SYN`=1, `SeqNUm`=12345. (a) Se si trova nello stato LISTEN, cosa deve inviare e in che stato si porta? (b) E se si trova nello stato SYN_RCVD? (c) Quali dovrebbero essere i flag a 1 del prossimo segmento che si aspetta di ricevere?

    R: (a) SYN=1, ACK=1, Acknowledgment=12346; si porta in SYN_RCVD. (b) Vuol dire che deve ritrasmettere l'ultimo che ha mandato. (c) ACK=1 e basta, con il quale va in ESTABLISHED

13. Durante una connessione TCP, A ha inviato a B i seguenti segmenti: `SequenceNum`=1000, `Length`=1000; `SequenceNum`=2000, `Length`=500; `SequenceNum`=2500, `Length`=700. A questo punto riceve da B un segmento con `AdvertisedWindow`=3000, `Acknowledge`=2000. Quanti byte può ancora spedire A?

R: B ha sicuramente ricevuto fino a 1999; del resto non sappiamo niente, ma evidentemente il segmento con SequenceNum=2000 non è arrivato; siccome potrebbe essere solo in ritardo, A deve ritenere che sia ancora in viaggio, come il suo successore. Quindi la EffectiveWindow è $AdvertisedWindow - (LastByteSent - LastByteAck) = 3000 - (3199 - 1999) = 1800$.

14. Un router che applica l'accodamento FairQueing deve gestire i flussi A, B, C, con i seguenti pacchetti in coda (in qualche unità di tempo): A: 100, 50, 80, 100; B: 80, 200, 80; C: 50, 250, 50. (a) Quando inizia la trasmissione del flussi A? (b) A che istante inizia la trasmissione del terzo pacchetto di C?

    R: Applicando l'algoritmo si vede che l'ordine e gli istanti di trasmissione sono: C1(0), B1(50), A1(130), A2(230), A3(280), B2(360), C2(560), A4(810), C3(910), B3(960). Quindi (a) 130. (b) C3 inizia a 910.

15. Un programmatore deve mettere "in sicurezza" un'applicazione client/server, ossia garantire confidenzialità e integrità dei dati trasmessi. Avendo a disposizione il codice sorgente, (a) a che livello dello stack potrebbe intervenire? (b) Se deve garantire anche la mutua autenticazione, cosa si deve fornire al client e al server? (c) È necessario avere i diritti di amministratore di sistema?

    R: (a) 5 (sessione) - 6 (presentazione) con TLS (b) Certificati X.509 (e aggiornarli) (c) No, si può fare tutto in user space.

16. Un certo sistema costruisce la chiave "master" per ogni utente giustapponendo la sua data di nascita (nel formato YYYYMMDD) ad un codice di 4 cifre scelto dall'utente stesso. (a) Sapendo che gli utenti sono nati dal 1/1/1940 al 31/12/2019, quant'è grande lo spazio delle chiavi? (b) Avendo a disposizione un calcolatore che può fare 10.000 tentativi al secondo, in quanto tempo in media si può trovare la chiave?

    R: (a) dal 1940 al 2020 (escluso) ci sono 80 anni, per un totale di $80 * 365 + 20 = 29220$ giorni (contando anche i 20 giorni bisestili). Quindi le chiavi sono $29220 * 10^4 = 292200000 = 292,2 * 10^6$ (b) $292,2 * 10^6/(2 * 10000) = 14620s \approx 4$ ore.

17. Si consideri il protocollo a lato, dove K_A è una chiave simmetrica precondivisa tra A e la terza parte fidata C, e analogamente per K_B tra B e C; K è una chiave casuale generata da C sul momento. Il messaggio M è (a) segreto? (b) autentico, ossia B è sicuro della sua provenienza? (c) puntuale, ossia non soggetto ad attacchi replay?

    1. $A \to C : A, B$
    2. $C \to A : E_{K_A}(A, B, K, E_{K_B}(A, B, K))$
    3. $A \to B : E_{K_B}(A, B, K), E_K(M)$

    R: (a) sì, un attaccante non riesce a rubare la chiave K. (b) sì (c) No, si può rimandare a B un vecchio messaggio senza problemi.

18. Nel meccanismo anti-replay implementato da IPSec: (a) è possibile che un pacchetto venga scartato pur essendo valido? Perché? (b) Se succede, come viene risolto questo problema, e da quale protocollo? (c) Questi fatti sono rilevanti per il programmatore di una generica applicazione?

    R: (a) sì, perché la finestra anti-reply è limitata (b) si lascia ai protocolli superiori, tipo TCP, se dovesse essere necessario (c) Solo se l'applicazione è real time; in tal caso le perdite in più potrebbero essere problematiche. Altrimenti può ignorare il problema (è gestito ai livelli sottostanti).