DMIF, Università degli Studi di Udine IV appello A.A. 2017-18 — 9 luglio 2018

Esame di **Reti di Calcolatori**

Soluzione

1. Un server TCP/IP, prima di mettersi in ascolto passivo, deve associare una socket ad un certo indirizzo. Quali informazioni sono contenute in tale indirizzo? Quale invece non è necessario specificare?

   R: Ci sono l'indirizzo di livello 4 (porta) e l'indirizzo di livello 3 (indirizzo IP). Non è necessario mettere l'indirizzo di livello 2 (MAC address) perché è gestito dal livello 3.

2. Nello standard IEEE 802.15.7, il canale fisico wireless più avanzato è realizzato impulsando un segnale ottico (prodotto da un LED) con una banda di 24 MHz e modulazione 16-Colour Shift Keying (cioè in ogni baud si trasmette un simbolo preso da una costellazione di 16 simboli distinti codificati con un colore della luce trasmessa). Quale è il rapporto segnale/rumore minimo per avere la massima capacità di canale possibile?

   R: Il teorema di Shannon dice che $R = B \log_2(1 + SNR)$, dove B è la banda base e R è la velocità di trasmissione (bitrate). Per Hartley, $R = 2B \log_2 M$, ove M è la molteplicità del simbolo trasmesso per baud. Sostituendo abbiamo $2 \log_2 M = \log_2(1 + SNR)$, cioè $M^2 = 1 + SNR$. In questo caso abbiamo $M = 16$ e quindi SNR = 255.

3. Sui dati grezzi trasmessi sul canale fisico di cui all'esercizio precedente, viene utilizzata una codifica di correzione in avanti (FEC) in cui vengono usati pacchetti di 64 simboli, di cui 32 sono di parità. Determinare il bit rate effettivo del canale, ignorando l'overhead dovuto alla struttura dei frame.

   R: Ad una banda base di 24 MHz corrisponde un baudrate di 48 Mbaud La codifica 16-CSK implica 4 bit codificati per ogni simbolo, per cui il bit rate grezzo è 2*24*4 = 192 Mb/s. Il bit rate viene ridotto di un fattore 32/64 dalla FEC, quando si passa a considerare la parte utile per il payload. Il bit rate netto è quindi di 96 Mb/s.

4. Nei protocolli che usano caratteri sentinella per indicare l'inizio e la fine del payload di un frame, cosa succede se, a causa di un errore di trasmissione, il carattere di "fine dati" ETX viene modificato (e quindi non è più ETX)? Quanti frame posso essere scartati?

   R: Il ricevitore potrebbe continuare a leggere dati anche oltre la fine del frame, includendo anche quelli del frame successivo, fino all'ETX. Dopodiché il CRC segnala l'errore, e tutti i dati vengono scartati. Quindi si perdono 2 frame.

5. Si vuole trasmettere la sequenza di bit 101001110 aggiungendo un codice CRC-4-ITU, il cui polinomio generatore è $x^4 + x + 1$. Come è fatto il messaggio complessivo?

   R: Il messaggio complessivo è 101001110*1001*. Qui sotto il calcolo.

```
101001110 0000  | 10011
10011
 01111110 0000
  10011
  0110010 0000
   10011
   010100 0000
    10011
    00111 0000
      100 11
      011 1100
```

```
10 011
01 1010
 1 0011
   1001
```

6. Si dica quali sono il primo e l'ultimo indirizzo utile per ognuna delle seguenti reti: a) 10.0.0.0/8; b) 143.220.0.0/15. c) 192.168.128.0/18.

   R: a) 10.0.0.1 – 10.255.255.254; b) 143.220.0.1 – 143.221.255.254; c) 192.168.128.1 – 192.168.191.254.

7. Un router riceve due pacchetti IP, da inviare su un collegamento che ha MTU=576. Il primo pacchetto ha Offset=200, Length=400; il secondo ha Offset=0, Length=800. (a) Quanti pacchetti vengono inviati? (b) Per ogni pacchetto si diano i valori di Length e Offset.

   R: Il primo pacchetto ha una dimensione complessiva di 400 byte, quindi non deve essere frammentato ulteriormente. Il secondo pacchetto non entra nell'MTU, quindi deve essere spezzato in due ulteriori frammenti. Togliendo 20 (dimensione dell'header di IP) dall'MTU e dividento per 8, si vede che il numero massimo che si può mettere in Offset è la parte intera di (576-20)/8 = 69,5, ossia 69. Quindi il secondo pacchetto viene spezzato in due frammenti: uno con un payload di 69*8=552 byte, e quindi una Length=552+20=572, Offset=0; l'altro con un payload di 780-552=228 byte, e quindi Length=228+20=248, Offset=69.

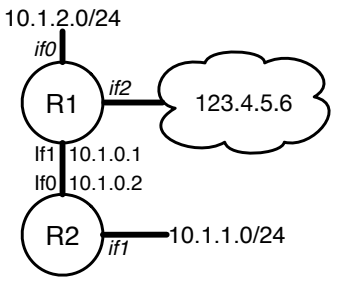
8. Le tabelle di inoltro dei router della rete a lato sono come segue:

   R1:

Net/CIDR	if	next hop
10.1.0.0/24	if1	-
10.1.2.0/24	if0	-
/	if2	123.4.5.6

   R2:

Net/CIDR	if	next hop
10.1.0.0/24	if0	-
10.1.1.0/24	if1	-
/	if0	10.1.0.1

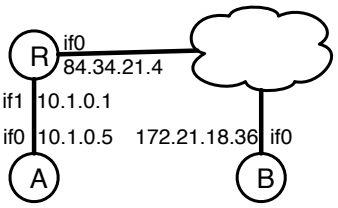
   

   L'host 10.1.1.7 può "pingare" (ossia inviare un pacchetto ICMP e ricevere la risposta) un host con indirizzo 10.1.2.2? Perché?
   R: No: il pacchetto ICMP arriva all'host 10.1.2.2, ma la risposta non raggiunge 10.1.1.7 perché da R1 viene mandato a 123.4.5.6, invece di R2. Il problema è nella tabella di inoltro di R1.

9. Un calcolatore utilizza DHCP per la propria configurazione di rete. (a) A quale indirizzo viene inviata la richiesta? (b) Quali informazioni minime sono contenute nella risposta?

   R: (a) Al broadcast 255.255.255.255. (b) Indirizzo IP da usare per l'interfaccia, netmask, gateway e possibilmente anche indirizzo DNS.

10. Il router R in figura implementa NAT per collegare la rete privata 10.0.0.0/8 al resto della rete. (a) Se l'host A invia un pacchetto IP all'host B, questo che indirizzo di mittete vede? (b) Può B eseguire una apertura attiva TCP con A (ossia inviare per primo un segmento SYN)?
    R: (a) Quello pubblico del router: 84.34.21.4 (b) Sì, a patto che il router abbia configurato il port forwarding.

11. Un host intende inviare un pacchetto ad un gruppo IP multicast. (a) Deve conoscere gli indirizzi degli host appartenenti al gruppo? Di un host in particolare? (b) Come può limitare la diffusione del messaggio all'interno della propria rete aziendale?

    R: No. No. Scegliendo il TTL opportunamente.

12. Una certa socket TCP sull'host A, dopo aver ricevuto un segmento SYN, si trova nello stato SYN_RCVD. A questo punto riceve un segmento con SYN=1, e i cui indirizzo IP e porta mittente sono gli stessi del segmento ricevuto in precedenza. Come deve comportarsi l'host A (ossia, cosa fa del nuovo segmento e in che stato si porta)?

    R: Dipende dal valore di SeqNum che c'è nel segmento. Se è lo stesso di quello ricevuto precedentemente, allora il segmento è un duplicato e può essere scartato senza problemi. Se è diverso, può essere una nuova connessione (la precedente è stata abortita per qualche motivo), per cui fa finta di rifare l'ack a tre vie da capo: rimanda SYN+ACK nuovo (con il nuovo SeqNum), e si rimette in SYN_RCVD.

13. Due processi stanno comunicando attraverso una certa connessione TCP, il cui RTT è di 50ms. Se il MSS è di 1460 byte, a quale velocità un processo deve produrre dati per massimizzare l'efficienza di trasferimento (ossia, massimizzare il payload in ogni segmento)?

    R: In base all'algoritmo di Nagle, il produttore deve produrre abbastanza dati da riempire una MTU prima che arrivi l'ACK del segmento precedente. Quindi 1460 byte / 50 ms = 29200 byte/s.

14. Un host TCP impiega la ritrasmissione veloce con recupero veloce, con numero massimo di duplicati pari a 3, con MSS=1000, CongestionWindow=8000 e si trova in fase additiva. Inizia a trasmettere i segmenti, e riceve i seguenti ACK: 11000, 12000, 13000, 13000, 13000, 13000. A questo punto, (a) Quanto vale la CongestionWindow? (b) Qual è il numero di sequenza del prossimo segmento che verrà inviato?

    R: Increment=MSS*MSS/CW = 1000*1000/8000 = 125. Quando vengono ricevuti gli ACK 11000, 12000, 13000, che sono corretti, la CW viene incrementata di 125 byte ogni volta; quindi a questo punto è 8375. Alla ricezione degli altri ACK=13000, non viene incrementato. Al terzo ACK duplicato, la CW viene dimezzata, e quindi diventa 4187. Il segmento che viene inviato a questo punto è quello con SeqNum=13000.

15. Molte persone telefonano in pubblico senza prestare troppa attenzione a chi gli sta intorno. Supponendo che gli astanti sopportino in silenzio il fastidio causato dalla telefonata, si dica se il canale bocca-microfono è soggetto ad attacchi passivi e/o attivi, e se ai dati o ai metadati.

    R: E' soggetto ad attacchi passivi, ma non attivi. L'attacco è sui dati (si ascolta cosa dice), e parzialmente anche ai metadati (si conosce ora e durata della telefonata, ma non identità dell'altra persona, in generale).

16. Si vuole trasmettere dei dati cifrati su un canale soggetto ad errori, usando un cifrario a blocchi tipo AES. Se un errore coinvolge fino a 2 bit consecutivi, quanti bit vengono alterati usando i modi ECB, CBC e CTR, rispettivamente?

    R: Il peggiore è CBC perché se i 2 bit sbagliati cadono a cavallo dei due blocchi, vengono rovinati 3 blocchi in tutto. Con ECB si rovinano al max 2 blocchi, e con CTR si rovinano al massimo 2 bit.

17. Un utente vuole ottenere un certificato X.509 per la firma digitale. (a) Quale informazione deve fornire l'utente alla CA? (b) E' possibile che il certificato emesso abbia una data di inizio validità nel futuro (ad esempio, uno o due giorni dopo)?

    R: (a) Essenzialmente la propria identità e la chiave pubblica appena creata. (b) Sì, questa è la normale situazione in cui un certificato viene rinnovato / sostituito.

18. Si consideri il protocollo a lato, dove K_A, K_B sono segreti precondivisi tra A e KDC e B e KDC, rispettivamente, e K è una chiave di sessione random generata da A. (a) B è autenticato per A? (b) A è autenticato per B?

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

    R: (a) Sì, perché cifrando M con K dimostra di conoscere K_B (b) No, c'è un attacco, in cui Eva può riusare una vecchia chiave ricevuta da B durante una precedente sessione con A.

19. Oggigiorno per accedere alla posta elettronica si utilizzano sempre più "web client", ossia applicazioni web accessibili via browser senza installare niente sul calcolatore. Alcuni di questi web client permettono di decifrare messaggi ricevuti in S/MIME e inviare messaggi S/MIME firmati. Se le mail rimangono solo sul server, cosa significa questo riguardo la sicurezza delle chiavi private?

    R: Per avere queste funzionalità è necessario che il server abbia accesso alle chiavi private. Se queste sono memorizzate sul server, è un problema serio per la loro sicurezza.

20. Nella prima fase di handshake SSL un server ha selezionato lo scambio RSA, ma nella seconda fase ha inviato un certificato X.509 rilasciato da una CA non nota al client. Il client può continuare l'autenticazione? Se sì, con quali conseguenze?

    R: Può continuare, ma al prezzo di non essere certi dell'identità del server. È quello che succede quando ci si collega ad un server, e il browser dice che il certificato non è riconosciuto.