DMIF, Università degli Studi di Udine IV appello A.A. 2018-19 — 15 luglio 2019

Esame di **Reti di Calcolatori**

Soluzione

1. A quali livelli dello stack OSI operano i seguenti componenti?
   (a) router; (b) hub; (c) server HTTP; (d) amplificatore di segnale elettrico.

   R: (a) livello 3 (b) livello 2 (c) livello 7 (d) livello 1

2. Nell'ultimo standard ADSL (ADSL2+M) la banda riservata al flusso in download è tra 276 kHz e 2208 kHz. Il massimo bitrate dichiarato (comprensivo dell'overhead del protocollo) in download è di circa 24 Mbit/s, per distanze fino a 600 metri. In tale situazione, quanti bit sono codificati per simbolo?

   R: Il baud rate complessivo di tutta la banda di download è pari a $2 * (2208 - 276)$ kHz = 3864 kBaud e quindi ogni baud deve codificare 24 Mbit/s / 3864 kBaud = 6.2 bit per Baud (accettabile anche 6)

3. Nelle condizioni dell'esercizio precedente, che rapporto segnale rumore minimo è richiesto?

   R: Dal teorema di Shannon-Hartley avremo $C = BW \log_2(1 + SNR)$ quindi 24 Mbit/s = (2208-276) kHz $\log_2(1 + SNR)$, ossia $24 * 10^6 / 1932 * 10^3 = 12.422 = \log_2(1 + SNR)$ da cui SNR = 5487 (all'incirca, causa approssimazioni).

4. Un pacchetto di 100 bit contiene un codice di controllo che permette di rilevare fino a 2 bit errati. Se il Bit Error Ratio è $p = 10^{-3}$, qual è la probabilità P che il pacchetto arrivi con errori non rilevati?

   R: Bisogna calcolare la probabilità che ci siano 3 o più errori, ovvero $P = 1 - (P(\#errori = 0) + P(\#errori = 1) + P(\#errori = 2))$. Ora: $P(\#errori = k) = \binom{N}{k} p^k (1-p)^{N-k}$, dove $N = 100$. Sostituendo abbiamo $P(\#errori = 0) = (1 - 10^{-3})^{100} = 0.9047921$, $P(\#errori = 1) = 100 * 10^{-3} * (1 - 10^{-3})^{99} = 0.0905697$, $P(\#errori = 2) = 100 * 99/2 * 10^{-3*2} * (1 - 10^{-3})^{98} = 0.00448765$, quindi $P = 1 - (0.9047921 + 0.0905697 + 0.00448765) = 0.00015 = 0.15 * 10^{-3}$.

5. Una certa cella 802.11n sta funzionando a 100 Mb/s, con SIFS=16μs, DIFS=34μs. Ricordando che ogni frame dati ha un header di 30 byte e un CRC di 4 byte, i frame ACK e CTS sono di 14 byte e il frame RTS è di 20 byte, si dica il tempo minimo necessario per trasmettere un payload di 1500 byte.

   R: I dati complessivi da trasmettere sono $1500 + 30 + 4 + 14 + 14 + 20 = 1582$ byte = 12656 bit, che prendono 126.56 μs. A questo bisogna aggiungere 3 SIFS e un DIFS = 3*16+34=82 μs, per un totale di 208.56 μs. (Quindi il bitrate netto è 12000/208.56 = 57,54 Mb/s)

6. Quanto deve essere il CIDR x minimo affinché 192.168.168.0/x sia un indirizzo di rete valido? Quanti indirizzi utili ha tale rete?

   R: Convertendo 168 in binario si ottiene 10101000. Ci vogliono 8+8+5 bit per coprire fino all'ultimo 1, quindi $x = 21$. Rimangono $32 - 21 = 11$ bit per l'host, quindi ci sono $2^{11} - 2 = 2046$ indirizzi utili.

7. (a) Il campo TTL viene utilizzato nel calcolo del checksum dell'intestazione di IPv4?
   (b) Tale campo TTL è necessario anche nei sistemi a commutazione di circuito? Perché?

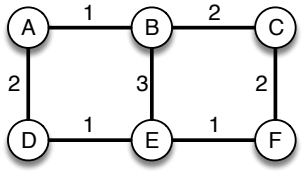
   R: (a) Serve a capire se un pacchetto è finito in loop. Ogni router lo decrementa, e quando va a 0 il pacchetto viene scartato. (b) No, perché il circuito viene creato senza loop, durante la fase iniziale.

8. Un utente esegue il comando a lato, ottenendo la risposta mostrata. (a) L'host di destinazione potrebbe essere spento? (b) Se è acceso e funzionante, dove potrebbe essere il problema?

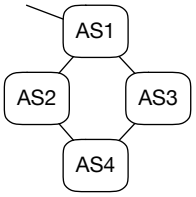
```
$ ping 123.45.67.89
PING 123.45.67.89 (123.45.67.89): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
...
```

   R: (a) Sì, anche se sarebbe più preciso un altro errore (Host Unreachable) (b) In un router intermedio, che filtra il pacchetto ICMP senza dare risposta.

9. I router della rete a lato utilizzano un algoritmo di routing basato sul vettore delle distanze. (a) Si diano i percorsi da A a F, e da D a C, con i rispettivi costi. (b) Ad un certo punto, il costo del collegamento B-E diventa 1. Come cambiano i percorsi da A a F e da D a C?
R: (a) A-D-E-F, costo 4; D-E-F-C, costo 4. (b) Da A a F cambia e diventa A-B-E-F. Invece da D a C non cambia, o potrebbe diventare D-E-B-C.



10. Nella rete a lato, tutti gli AS sono di transito, tranne AS4. Sia N una rete di AS4. (a) Quali sono i percorsi pubblicati dallo speaker di AS1 per la rete N? (b) Quando AS1 comunica questi percorsi allo speaker di AS2, vengono accettati o rifiutati?
R: (a) AS1-AS2-AS4 o AS1-AS3-AS4. (b) AS1-AS2-AS4 viene rifiutato da AS2, perché vi riconosce un loop con se stesso. Invece AS1-AS3-AS4 viene accettato, ma tenuto solo come alternativa al collegamento AS2-AS4



11. Un processo intende inviare dei dati ad un gruppo IP multicast. (a) Quale protocollo di trasporto deve utilizzare? (b) Se il gruppo comprende host al di fuori della rete locale, cosa deve inviare l'host prima di iniziare ad inviare i dati, e a quale indirizzo?

    R: (a) UDP. (b) Prima deve fare il join al gruppo, mediante il protocollo IGMP. Un messaggio IGMP Report viene mandato dall'host allo stesso indirizzo del gruppo, ma viene ricevuto dagli switch e da eventuali router.

12. Durante la fase di handshake di una connessione TCP, il client (che esegue l'apertura attiva) misura un tempo di 50 ms tra l'invio del SYN e la ricezione del SYN+ACK. Dopo aver inviato il primo segmento dati, l'ACK corrispondente arriva dopo 80 ms. A questo punto, quanto valgono `EstimatedRTT` e il Timeout, se si usa l'algoritmo standard con $\alpha = 0.8$?

    R: EstimatedRTT = 0.8*50 + 0.2*80 = 56 ms. Il timeout è il doppio, ossia 112 ms.

13. Un host sta inviando dei segmenti TCP da 1000 byte l'uno. Finora ha inviato quattro segmenti a partire dal `SeqNum`=500, e ha ricevuto i seguenti `Acknowledgment` (in questo ordine): 500, 2500, 1500. Non ci sono stati timeout, e la finestra è > 1000. Quale `SeqNum` ha il prossimo segmento da inviare, e perché?

    R: I quattro segmenti inviati hanno `SeqNum` pari a 500, 1500, 2500, 3500. Dato che non c'è bisogno di rimandare pacchetti vecchi, e la finestra lo consente, si invia il segmento con `SeqNum`=4500.

14. Una connessione TCP, con MSS=1400 e recupero veloce, si trova nella fase additiva, e inizia il round con `CongestionWindow` = 10000. Dopo aver inviato un po' di segmenti e ricevuto 5 ACK, scade il timout di un segmento inviato in precedenza. Quanto diventa `CongestionWindow`?

    R: L'incremento ricevuto per ogni ACK è di MSS*MSS/CW = 196 byte. Quindi, dopo 5 segmenti riscontrati, CW è diventato 10000+196*5 = 10980. A questo punto scade il timeout, e quindi CW viene dimezzata diventando 5490.

15. Per ognuno dei seguenti meccanismi di sicurezza
    (a) cifratura simmetrica dei dati; (b) firma digitale; (c) protocollo di challenge-response;
    si dica a quali servizi di sicurezza seguenti si applica: 1. confidenzialità dei dati; 2. dei metadati; 3. integrità dei dati; 4. dei metadati; 5. autenticazione delle parti; 6. non ripudio.

    R: (a) 1. 3. (confidenzialità e integrità dei dati). (b) 3. 6. (integrità dei dati, non ripudio) (c) 5. (autenticazione delle parti)

16. Il modo di cifratura Output Feedback (OFB) può essere definito formalmente come segue (dove IV è un vettore di inizializzazione e P_i è l'i-esimo blocco del testo in chiaro):
    $O_0 = IV, O_i = E_K(O_{i-1}), C_i = P_i \oplus O_i$, e corrispondentemente la decifratura è $P_i = C_i \oplus O_i$.
    (a) Se durante la trasmissione un bit di C_i viene alterato, quanti bit verranno alterati nel testo decifrato?
    (b) Cosa succede se lo stesso IV viene usato per cifrare due diversi flussi?

    R: (a) 1 solo bit, perché c'è lo XOR. (b) disastro, si può condurre il solito attacco sui cifrari a flusso.

17. Quali delle seguenti informazioni sono presenti in un certificato X.509: (a) Chiave pubblica del soggetto (subject); (b) Chiave pubblica dell'emittente (issuer); (c) Hash di tutti i campi del certificato; (d) Chiave privata del soggetto.

R: (a) sì (b) no (c) sì (d) no

18. Nel protocollo a lato, PU_B è la chiave pubblica di B (nota ad A), K è una chiave di sessione generata sul momento da A, N è una nonce generata da B. (a) A è autenticato per B? (b) B è autenticato per A? (c) K è puntuale?

1. $A \to B : E_{PU_B}(K)$
2. $B \to A : E_K(N)$
3. $A \to B : E_K(N+1)$

R: (a) No, perché non c'è nessuna challenge a cui possa rispondere A usando qualche informazione solo ad essa nota (in altre parole, A può essere chiunque); (b) Sì, perché riesce a decifrare K dal primo messaggio, e solo chi possiede PR_B può farlo. (c) Sì, perché un attaccante non può riproporre il primo messaggio senza conoscere la chiave K, in quanto gli serve K per rispondere correttamente al passo 3.

19. Una mail S/MIME o PGP cifrata può essere descritta in astratto come $A \to B : E_{PU_B}(K), E_K(M)$.
(a) Cosa deve conoscere A? (b) B è sicuro dell'integrità del messaggio M? E dell'autenticità?
(c) Il destinatario come può ottenere una prova della puntualità del messaggio (eventualmente con lo scambio di altre 1 o 2 mail $B \to A$ e $A \to B$)?

R: (a) La chiave pubblica del destinatario.
(b) Sì dell'integrità. Non dell'autenticità, perché non c'è niente che distingua il mittente.
(c) Sì, ad esempio come segue: 2. $B \to A : N$; 3 $A \to B : E_{PU_B}(H(M, N))$

20. Un browser si collega ad un server mediante HTTPS (ossia, HTTP su TLS o SSL), in cui lo scambio chiavi è avvenuto mediante RSA. (a) L'indirizzo IP del server è segreto? (b) La porta del server è segreta? (c) Il server è autenticato per il browser? (d) Il browser è autenticato per il server?

R: (a) no (b) no (c) sì (d) no