DMIF, Università degli Studi di Udine IV appello A.A. 2020-21 — 9 luglio 2021

Esame di **Reti di Calcolatori**

Soluzione

1. Il Controllo Missione della NASA sta comunicando con un rover su Marte, che dista circa 60 milioni di km dalla Terra, su un canale con una capacità di 250 kbps. (a) Ricordando che $c = 3 * 10^8$ m/s, quant'è il RTT? (b) Periodicamente il rover scatta una foto, che pesa 5MB, e la trasmette su tale canale. Dopo quanto tempo, dal momento dello scatto, tale foto è disponibile presso il Controllo Missione?

   R: (a) Il delay è $60 * 10^9/3 * 10^8 = 20 * 10^1 = 200$ s, quindi il RTT è 400 s = 6 minuti 40 secondi. (b) 5MB = 40Mbit, che a 250 kbps prende 40.000/200 = 160 secondi la trasmissione. Quindi in totale il ritardo è 160+200=360 secondi=6 minuti.

2. ll sistema DVB-T2 prevede diversi "profili" a livello fisico. Uno di questi definisce una modulazione 64-QAM (quindi un alfabeto di 64 simboli), con una FEC 3/5, su un canale largo 8 MHz; si codifica un simbolo per ciclo. Sapendo che circa l'8% della banda viene consumato da traffico di servizio, quant'è il bitrate utile per ogni canale?

   R: Attenzione che nell'esercizio è specificato che si codifica un simbolo per ogni ciclo di clock, quindi il baudrate è 8*1=8 Mbaud.. 64 simboli corrispondono a 6 bit per simbolo, quindi il bitrate grezzo è 8*6= 48 Mbps, che dopo la FEC diventano 28,8 Mbps. Togliendo l'8%, rimangono 26,5 Mbps netti.

3. Su una certa linea di trasmissione, i dati vengono inviati in frame composti da una intestazione di 10 byte, comprensiva di CRC, e un payload di 1000 byte. Se un frame è errato, viene scartato e ritrasmesso. La probabilità di errore per ogni bit è $p = 10^{-5}$. Se questi frame vengono usati per trasferire un file da 10KB, qual è la probabilità che si debba effettuare almeno una ritrasmissione?

   R: 1010 byte = 8080 bit; probabilità che arrivi un frame correttamente è $(1-p)^{8080} = 0,922 = 92,2\%$. Probabilità di ritrasmissione = 1 - probabilità di nessun errore su 10 frame. Probabilità di nessun errore su 10 frame = $0,922^{10} = 0,4457$. Quindi probabilità di ritrasmissione = 55%.

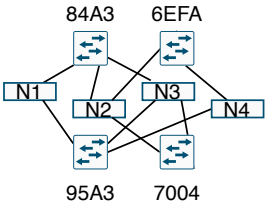
4. In una rete Ethernet classica, ci sono due host A, B. L'host A ha una serie di frame da trasmettere $A_1, A_2, \ldots$; analogamente B. Ad un certo istante, entrambi provano a trasmettere A_1 e B_1, collidendo. (a) Qual è la probabilità che al secondo tentativo ci sia di nuovo una collisione? (b) Se al secondo tentativo A riesce a trasmettere il frame A_1, qual è la probabilità che riesca ad inviare A_2 immediatamente dopo?

   R: (a) 2 casi su 4, quindi 50%. (b) Dopo la seconda collisione, B ha impostato il suo numero massimo per il backoff esponenziale a 4, quindi quando tenta di trasmettere B_1 per la terza volta aspetta da 0 a 3 slot time. Invece A, per trasmettere A_2, non aspetta niente, perché è il primo tentativo per quel frame. Per cui la trasmissione di A_2 avviene senza collisioni se a B non esce da aspettare 0 slot, e questo succede con probabilità 75%.

5. In una certa cella Bluetooth ci sono 3 slave A,B,C e un master M. Ricordando che gli slot sono di $625\mu s$, se uno slave deve trasmettere dei dati (che stanno in uno slot) ad un altro slave, qual è il ritardo massimo dall'inizio della trasmissione alla completa ricezione?

   R: Tutta la comunicazione passa attraverso il master, che può trasmettere solo negli slot pari; ad esempio la sequenza di trasmissione può essere AMBMCMAMBMCM ecc. Il massimo ritardo si ha quando A deve trasmettere a C (passando per M), per cui bisogna aspettare 6 slot (AMBMCM), ossia 6*625=3750 μs = 3.75 ms.

6. Gli switch della rete a lato implementano l'algoritmo di spanning tree. (a) Ci sono switch che si disattivano? (b) Quali switch deve attraversare un frame per andare da N1 al N3?



R: (a) La root è 6EFA. Si disattiva 95A3 (b) 84A3 e 7004.

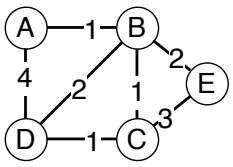
7. Si considerino tre host con indirizzi A=158.0.2.3, B=158.5.3.5, C=158.7.1.4. (a) Qual è la rete più piccola (ossia con il minor numero di indirizzi) che li comprende tutti e tre? (b) Qual è l'indirizzo di broadcast per tale rete?

   R: (a) Bisogna vedere il massimo prefisso comune. 158.0=10011110.00000000, 158.5=10011110.00000101, 158.7=10011110.00000111, quindi il più lungo prefisso comune è 10011110.00000xxx, ossia 158.0.0.0/13. (b) 158.7.255.255.

8. (a) Il protocollo ICMP si appoggia a quale altro protocollo? (b) Cosa significa se un host riceve un pacchetto ICMP con codice "Network Unreachable"?

   R: (a) A IP. (b) Che un router non sa come instradare un pacchetto IP che l'host ha inviato.

9. I router della figura a lato adottano un protocollo basato sul vettore delle distanza, con *split horizon*. (a) Si mostri la tabella di instradamento di C. (b) Si mostri il vettore inviato da C a B.



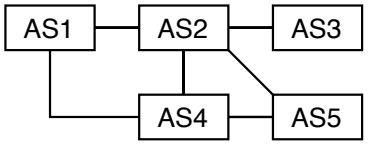
R: (a)

dest	d	n.h.
A	2	B
B	1	B
C	0	-
D	1	D
E	3	E

(b)

dest	d
C	0
D	1
E	3

10. Si considerino gli autonomous system a lato. (a) Ci sono AS stub? (b) Quale/i AS deve/ono essere di transito per garantire la connettività completa? (c) Quale/i AS deve/ono essere multi-homed per garantire l'assenza di loop?



R: (a) sì, AS3. (b) AS2 (c) AS4.

11. (a) Quali informazioni vengono utilizzate per il calcolo del checksum UDP? (b) Cosa succede al checksum se il datagramma attraversa un router che implementa NAT?

    R: (a) il datagramma, più lo pseudoheader IP: protocollo, indirizzi IP mittente e destinatario. (b) bisogna ricalcolarlo.

12. Una certa socket TCP si trova nello stato SYN_SENT. (a) Che tipo di apertura sta effettuando? (b) Se riceve un segmento con `SYN`=1, `SeqNUm`=12345, cosa deve inviare e in che stato si porta? (c) E se invece riceve un `SYN+ACK`, in che stato si porta?

    R: (a) Attiva. (b) SYN=1, ACK=1, Acknowledgment=12346; si porta in SYN_RCVD (simultanea) (c) ESTABLISHED, ed invia ACK.

13. Un'applicazione sta scrivendo su una socket TCP una stringa di 300 byte ogni 10 ms. La connessione TCP ha un MSS di 1460 byte e un RTT di 50ms. Si supponga che CongestionWindow e AdvertisedWindow siano sufficientemente grandi. (a) Quanto è grande il payload di ogni segmento inviato dall'host, in media? (b) Cosa succede se il RTT scende a 30ms?

    R: (a) In un RTT il buffer accumula 1500 byte, superiore al MSS. Quindi, per l'algoritmo di Nagle, vengono inviati segmenti di 1460 byte. (b) In tal caso il buffer accumula 900 byte, inferiore al MSS. Quindi vengono inviati segmenti con un payload di 900 byte, ogni volta che arriva un ACK.

14. Un router implementa RED su una certa interfaccia con MinThreshold=20KB e MaxThreshold=100KB. Si osserva una perdita media di pacchetti pari al 5%. Quanto è lunga la coda di quell'interfaccia?

    R: Probabilità di scarto nell'intervallo: $Q(l) = (l - 20)/(100 - 20) = (l - 20)/80$. Quindi se $0.05 = (l - 20)/80$ risolvendo si ha $l = 24$ KB.

15. Per ognuna delle seguenti azioni, si dica se è un attacco attivo o passivo, e a quale aspetto di sicurezza. (a) Modificare il MAC address della scheda di rete del proprio PC. (b) Intercettare le richieste al DNS. (c) Scambiare porzioni di due file cifrati con la stessa chiave.

    R: (a) Attivo, integrità dei metadati, masquerade. (b) Passivo, confidenzialità dei metadati. (c) Attivo, integrità dei dati.

16. Un certo sistema di trasmissione usa AES in modo OFB, ma in cui il vettore di inizializzazione è di 2 byte e il feedback considera solo gli ultimi 2 byte dell'output del cifrario, azzerando tutti gli altri bit; formalmente, $KS_0 = IV, KS_{i+1} = E_K(KS_i \;\&\&\; 0xFFFF), C_i = P_i \oplus KS_i$. (a) Quale vulnerabilità presenta questo sistema, anche all'interno dello stesso flusso di dati? (b) Come si potrebbe mitigare (senza estendere l'IV, ovviamente)?

    R: (a) Che dopo $2^{16} = 64kB$ il keystream si ripete. (b) Se non si può estendere l'IV, bisogna cambiare la K (rekeying) prima di arrivare al limite.

17. Nei ticket Kerberos, c'è un timestamp e una durata. (a) Chi inserisce questi timestamp e durata? (b) Chi li controlla? (c) L'utente può modificarli? Perché?

    R: (a) Chi rilascia i ticket: AS o TGS. (b) TGS o Server (c) No, perché sono cifrati con una chiave che non conosce.

18. Alice invia a Bob una mail S/MIME firmata con la sua chiave privata, ma non cifrata; in astratto, questo si rappresenta con $A \to B : M, E_{PR_A}(H(M))$. (a) Cosa deve conoscere Bob per verificare la mail? (b) Come potrebbe Charlie, dopo aver intercettato tale mail, modificarla e mandarla a Bob facendogli credere che è sua e non di Alice? (c) Si proponga una modifica al protocollo (eventualmente con un passaggio in più, e con nonces ma non con timestamp), che impedisca tale attacco.

    R: (a) La chiave pubblica di Alice. (b) Sì: toglie la firma di Alice (è un semplice attachment) e mette la propria. $1'.C \to B : M, PR_C(H(M))$ (c) Senza introdurre altre chiavi o funzioni crittografiche, un modo semplice è introdurre una nonce che diventa una challenge da B per A e garantisce puntualità e autenticità di M: $1.B \to A : E_{PU_A}(N); 2.A \to B : M, N, E_{PR_A}(H(M, N))$.