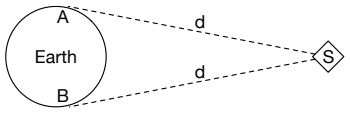
DMIF, Università degli Studi di Udine V appello A.A. 2018-19 — 23 settembre 2019

Esame di **Reti di Calcolatori**

Soluzione

1. Un collegamento dati tra A e B impiega come ripetitore di livello 1 un satellite S in orbita geostazionaria. Sapendo che la velocità del segnale radio nel vuoto è pari a $c = 3 * 10^8$ m/s, e la distanza d è circa 41.000 km, quanto è il Round Trip Time tra A e B?



R: La distanza totale da A a B è $82 * 10^6$ m, che vengono coperti in $82 * 10^6/(3 * 10^8) = 0,273s = 273$ ms. Siccome nel RTT dobbiamo tenere conto anche del tempo di ritorno, $RTT = 2 * 273 = 546$ ms.

2. Un canale fisico di trasmissione ha una larghezza di banda di 1 MHz e un rapporto segnale/rumore in potenza di -30 dB. Determinare il bit rate senza errori massimo possibile (mostrando il procedimento).

R: Un rapporto SNR in potenza di -30 dB equivale a $S/R = 10^{-3}$, perché $SNR = 10 * \log(S/R)$. Dal teorema di Shannon-Hartley, $C \leq B \log_2(1 + S/R)$ quindi $C \leq 1MHz \log_2(1 + 10^{-3}) = 1.44kbps$.

3. Nel canale dell'esercizio precedente, quanti simboli devono essere trasmessi per bit senza errore? Illustrare brevemente il procedimento seguito.

R: Il baude rate massimo è di $2 * 1MHz = 2$ MBaud, e quindi il numero di simboli per codificare un bit è 2 MBaud / 1.44 kbps = 1388.

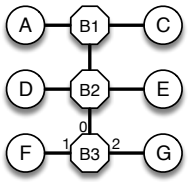
4. Ricordiamo che un frame 802.11 ha un header di 30 byte, seguito dal payload, ed infine un CRC-32. Il frame RTS è di 20 byte e CTS e ACK sono di 14 byte. Se il payload è di 1500 byte, quanti byte complessivamente deve trasmettere il nodo trasmittente?

R: RTS+Frame Dati = 20 + 30 + 1500 +4 = 1554 byte. CTS e ACK sono trasmessi dalla stazione ricevente.

5. Consideriamo una rete Ethernet classica con due stazioni A, B. All'istante 0, A e B provano a trasmettere i rispettivi frame A_1 e B_1 per la prima volta, collidendo. Di conseguenza, al turno successivo A e B provano a ritrasmettere gli stessi frame A_1, B_1 aspettando ognuna un tempo casuale secondo la regola del backoff esponenziale. A questo secondo tentativo, A risulta vincitrice e riesce a trasmettere i dati, mentre B rileva ancora collisione. Terminata questa trasmissione, A prova a trasmettere immediatamente un nuovo frame A_2. Qual è la probabilità che A riesca a trasmettere A_2 senza collisioni?

R: 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 senza collisioni avviene se a B non esce da aspettare 0 slot, e questo succede con probabilità 75%.

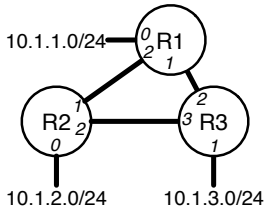
6. Nella rete a lato, B1, B2 e B3 sono switch ad autoapprendimento. B1 e B2 hanno già completato il loro apprendimento, mentre B3 è appena stato resettato.
(a) Se A manda un frame a E, come diventa la tabella di inoltro di B3?
(b) Se A manda un frame a F, quali host lo ricevono?
R: (a) Non cambia: il frame non gli arriva.
(b) F e G, perché B3 non sa dove mandarlo e quindi lo manda in flooding.



7. Si dica a quali delle seguenti reti appartengono gli indirizzi A=192.168.1.190, B=192.168.172.5:
(a) 192.168.0.0 netmask 255.255.0.0; (b) 192.168.0.0/24; (c) 192.168.0.0/17.

R: A appartiene ad (a) e (c), B appartiene a (a). Oppure, dualmente: (a) contiene A, B; (b) nessuno dei due; (c) solo A.

8. La rete a lato (non connessa con l'esterno) ha tre router, le cui tabelle di inoltro sono riportate qui sotto; per comodità, l'interfaccia y del router Rx ha l'indirizzo IP 10.2.x.y.
Uno di questi router è configurato in modo errato (ossia, porta a dei gravi malfunzionamenti, non semplici inefficienze): quale, e perché?



R1:

dest	if	next hop
10.1.1.0/24	0	-
10.1.2.0/23	2	10.2.2.1

R2:

dest	if	next hop
10.1.2.0/24	0	-
10.1.3.0/23	2	10.2.3.3

R3:

dest	if	next hop
10.1.3.0/24	1	-
10.1.0.0/23	2	10.2.1.1

R: Il router R2, perché così com'è non può instradare la rete 10.1.1.0/24.

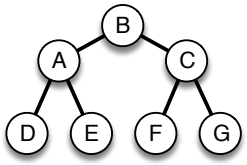
9. In una certa rete i router B e C sono collegati direttamente, mentre A è un altro router della rete. Tutti adottano un algoritmo di instradamento a stato delle linee, come OSPF. (a) È possibile che ad un certo punto il router A riceva contemporaneamente un LSP originato dal router B che dice che il collegamento $B - C$ è interrotto, e un LSP originato dal router C che dice che il collegamento $C - B$ è attivo?
(b) In tale situazione, cosa dovrebbe fare C con i pacchetti ricevuti (ricordiamo che i pacchetti LSP non contengono timestamp)? Cosa potrebbe aspettare?

R: (a) Sì, per vari motivi: ritardo nella trasmissione dello stato del collegamento dopo il guasto o dopo il ripristino, oppure linee asimmetriche. (b) Buttarne via uno, e aspettare che arrivi la conferma da A o da B, in un senso o l'altro.

10. (a) È possibile che un'interfaccia abbia contemporaneamente un indirizzo IPv4 e uno IPv6? Perché?
(b) A livello di applicazione, una socket può usare entrambi gli indirizzi contemporaneamente?

R: (a) Sì, per la tecnica del dual stack. (b) No, si deve scegliere a quale famiglia di indirizzamente associare la socket, e quindi a quale stack.

11. Per gestire il multicast, i router della rete a lato utilizzano un algoritmo di instradamento ad albero condiviso (tipo PIM-SM). Un host collegato a D invia un messaggio ad un gruppo il cui router rendezvous-point è B e i membri sono E, F, G.
(a) Qual è il traffico complessivo generato (ossia, quanti messaggi vengono creati sulla rete comprendendo anche quelli da un router all'altro)?
(b) Quanti messaggi verrebbero inviati se si usasse l'unicast invece del multicast?



R: (a) 2 per la trasmissione unicast da D fino a B, poi 2 per tornare a E, e 3 per raggiugnere F e G. Totale 7. (b) 2 da D a E, 4 da D a F, 4 da D a G. Totale 10.

12. Una certa implementazione di TCP utilizza un generatore di numeri casuali per definire il `SequenceNumber` iniziale ma, a causa di un bug in tale generatore, i numeri effettivamente generati sono solo una decina. A causa di questo bug, quale problema potrebbe verificarsi durante la fase di comunicazione?

R: Potrebbe succedere che un pacchetto in ritardo, duplicato, appartenente ad una precedente incarnazione, si infili in una nuova connessione, perché ha un numero di sequenza che rientra nella finestra ammissibile. Questo porterebbe ad inserire dati scorretti nel flusso di dati appena stabilito.

13. Un certo host TCP, con `NextByteExpected`=3000 e spazio libero nel buffer pari a 10000, riceve i seguenti segmenti, in questo ordine: `SequenceNum`=2000, `Length`=1000; `SequenceNum`=4000, `Length`=1500; `SequenceNum`=3000, `Length`=500. Quale valore di `Acknowledge` e `AdvertisedWindow` vengono inviati dopo il terzo segmento, se nel frattempo l'applicazione non consuma dati?

R: Il primo segmento porta dati duplicati, e viene scartato (ma viene comunque inviato un Ack). `NextByteExpected`=3500 (manca un pezzo tra 3500 e 4000), quindi `Acknowledge`=3500, `AdvertisedWindow`=10000-(3500-3000)=9500.

14. Un router applica la politica Round Robin tra quattro flussi, i cui pacchetti sono di 100, 200, 1200, 1400 byte ciascuno. (a) Quanto è l'indice di equità di questa situazione? (b) Come diventa se il flusso di pacchetti da 1400 byte termina? La situazione è migliorata o peggiorata?

R: (a) Dividendo tutto per 100 per semplicità (il risultato non cambia), è: $F = \frac{(1+2+12+14)^2}{4*(1^2+2^2+12^2+14^2)} = 0.61$.
(b) $F = \frac{(1+2+12)^2}{3*(1^2+2^2+12^2)} = 0.5$, quindi è peggiorata (meno equa).

15. Per ognuna delle seguenti affermazioni, si dica se è vera o falsa. (a) È inutile usare connessioni HTTPS se il nostro dispositivo si collega alla rete mediante una connessione Wi-Fi cifrata WPA2. (b) In una VPN su IPSec, il programmatore delle applicazioni deve gestire direttamente la creazione delle associazioni di sicurezza. (c) I meccanismi di sicurezza a livello trasporto non coprono gli indirizzi IP dei due estremi.

    R: (a) falso. (b) falso. (c) vero.

16. Si consideri il protocollo a lato, dove K è una chiave simmetrica precondivisa, K_S una chiave di sessione generata fresca da A, N una nonce generata da B. (a) Il messaggio M è autentico per B? (b) È non ripudiabile? (c) È puntuale (ossia non soggetto ad attacchi replay)?

    1. $A \to B : E_K(K_S)$
    2. $B \to A : E_{K_S}(N)$
    3. $A \to B : M, H(M, N)$

    R: (a) Sì: l'unico che può generare la hash al passo 3 è chi conosce K_S, ossia solo A e B. (b) No, per sopra: A e B hanno la stessa conoscenza, entrambi potrebbero aver generato M. (c) Sì: in caso di attacco replay, l'attaccante non potrebbe ottenere la nonce fresca per ricostruire la hash.

17. I certificati X.509 possono essere utilizzati anche per distribuire chiavi pubbliche Diffie-Hellman: al posto della chiave pubblica RSA (o simili), c'è la chiave pubblica DH. (a) Per quale scopo tali certificati possono essere utili? (b) Se A e B vogliono implementare uno scambio chiavi DH con le chiavi contenute nei loro rispettivi certificati, cosa devono concordare *ancora prima* di farsi rilasciare i certificati da una CA?

    R: (a) Per evitare l'attacco MITM. (b) Il numero primo p e la radice prima g per il calcolo della mezza chiave.

18. I ticket di Kerberos, ad esempio quelli rilasciati da AS, contengono un timestamp. (a) Cosa succede se l'orologio del client non è sincronizzato con quello di AS? Ci può essere un attacco? (b) E se quello del Ticket Granting Server non è sincronizzato con AS?

    R: (a) non succede niente, è normale. (b) è un problema, perché il TGT deve confrontare il timestamp.

19. Il protocollo a lato vuole implementare il *code signing*: lo sviluppatore A carica il suo programma sullo store S, da cui l'utente C può scaricarlo. K_A è una chiave simmetrica precondivisa specifica per lo sviluppatore A (rilasciatagli dallo store al momento della sua iscrizione), e PR_S è la chiave privata di S. (a) Cosa deve conoscere il client C per poter verificare il codice? (b) C è sicuro dell'integrità del codice? (c) C è sicuro dell'autenticità del codice (ossia, del fatto che provenga da A)?

    1. $A \to S : P, A, H(K_A, P)$
    2. $S \to C : P, A, E_{PR_S}(H(P))$

    R: (a) La chiave pubblica di S. (b) Sì, perché che la hash firmata. (c) No, un altro sviluppatore può intestarsi l'identità del codice di A, ad esempio cambiando A con B nel secondo messaggio.

20. In SSL, si dica quali delle seguenti informazioni sono di sessione e quali di connessione: (a) Master secret (b) Informazione segreta per l'autenticazione dei dati dal server (c) Numero di sequenza (d) Certificato X.509 della controparte (se c'è).

    R: Di sessione: (a), (d) Di connessione: (b), (c).