DMIF, Università degli Studi di Udine I appello A.A. 2019-20 — 27 gennaio 2020

Esame di **Reti di Calcolatori**

Soluzione

1. Si considerino il multiplexing di un canale a divisione di tempo (TDM) e statistico (SM).
(a) Quale garantisce una banda minima per ogni flusso? (b) In quale/i un singolo flusso potrebbe utilizzare l'intero canale? (c) Quale garantisce un tempo di attesa massimo per accedere al canale?

   R: (a) TDM. (b) SM (c) TDM.

2. Un canale analogico di comunicazione opera nella banda di frequenza da 0 a 10kHz. (a) Determinare il numero minimo di campionamenti necessari per ricostruire senza ambiguità un segnale di durata 0.1 s. (b) Se il segnale ha un rapporto segnale/rumore di 0 dB, quale è la capacità massima di trasmissione del canale, in kbps?

   R: (a) Dal teorema NS, la frequenza di campionamento minima deve essere il doppio della massima frequenza trasmessa col segnale : $2 * 10$ kHz. In 0.1 s saranno quindi necessari $2 * 10^4 * 0.1 = 2000$ campionamenti.

   (b) SNR in decibel pari a 0 significa che il rapporto S/R è 1. Quindi, dal teorema SH, $C \leq B \log_2(1 + SNR)$ quindi $C \leq 10kHz \log_2(1 + 1) = 10kbps$.

3. Una scheda di rete rileva che in media un frame viene scartato con frequenza 10^{-4} a causa di errori di trasmissione. S apendo che i frame sono lunghi complessivamente 1000 byte (header e trailer compresi), qual è la probabilità di errore p per ogni bit?

   R: Un frame di 1000 byte di payload è lungo complessivamente 8000 bit. Se p è la probabilità di errore per bit, la probabilità che sia tutto giusto è $Q = (1 - p)^{8000}$, che per ipotesi deve essere pari a $1 - 10^{-4}$. Risolvendo per p si ottiene $p = 1 - (1 - 10^{-4})^{1/8000} = 1.25 * 10^{-8}$.

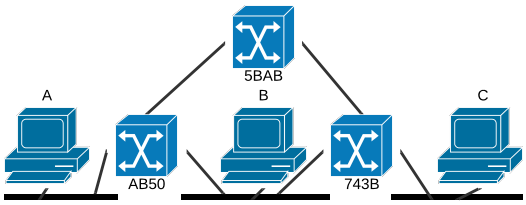
4. Se un frame Ethernet attraversa un hub o uno switch, è necessario ricalcolare il suo CRC? Perché?

   R: No, perché non c'è niente che cambi nel frame durante tale passaggio. Non ci sono TTL né altre informazioni modificate dallo switch.

5. I nodi di certa cella 802.11 stanno trasmettendo a 54 Mbps; SIFS= 10μs, RTS=20 byte, CTS e ACK=14 byte. Il nodo A inizia una trasmissione con B, mentre C è un nodo nel range di B ma nascosto per A. Dopo quanto tempo, dall'inizio della trasmissione, C è in grado di rilevarla?

   R: Appena B inizia a trasmettere il CTS, e quindi dopo il tempo di trasmissione di RTS (pari a $20 * 8/54 = 2,96\mu$s) e un SIFS; in totale circa 13μs.

6. Gli switch della rete a lato si sono autoconfigurati secondo l'algoritmo di spanning tree. (a) Quanti switch deve attraversare un frame di A per raggiungere B?
(b) Se il collegamento tra AB50 e 5BAB si interrompe, e dopo che la rete si è riconfigurata, quanti switch deve attraversare un frame di A per raggiungere C?



   R: (a) 3, perché bisogna passare per la root, che è 5BAB. (b) 2, perché non serve passare per 5BAB.

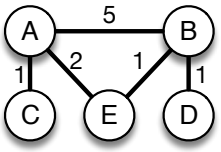
7. Si considerino le seguenti reti: (A) 192.168.4.0/22; (B) 192.168.4.0/23; (C) 192.168.3.0/24.
(a) A quali di queste reti appartiene l'indirizzo 192.168.6.10? (b) Quali di queste reti sono sottorete di 192.168.0.0/22? (c) Quanti indirizzi utili contiene la rete A?

   R: (a) Solo ad A. (b) La C. (c) $2^{32-22} - 2 = 1022$.

8. Un certo server DHCP, con indirizzo 10.0.0.1, assegna indirizzi nella sottorete 10.0.0.0/25. (a) Quanti client possono essere collegati alla rete, contemporaneamente? (b) Cosa può succedere se un host non rinnova il lease prima della sua scadenza (ma continua ad usare l'indirizzo)?

   R: (a) 125 (perché un indirizzo è usato dal server stesso) (b) il server potrebbe assegnare l'indirizzo ad un altro host della stessa rete, creando un conflitto.

9. I router della rete a lato utilizzano un algoritmo basato sullo stato delle linee, e hanno raggiunto la configurazione stabile. I valori rappresentano i ritardi introdotti dalle linee, in ms.
   (a) Si dia la tabella di instradamento di E. (b) Ad un certo punto il costo della linea B-E sale a 4. Dopo quanto tempo la rete raggiunge la nuova configurazione stabile?

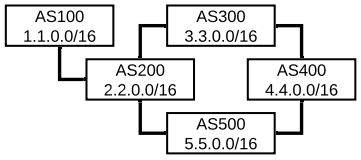


   R: (a)

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

   (b) Il tempo necessario affinché i pacchetti LSP di E e B raggiungano tutta la rete è 3 ms: B avvisa D in 1 ms, intanto E avvisa A in 2 ms. Poi A avvisa E in 1 ms.

10. Si considerino gli autonomous system a lato. AS100 è stub, AS400 multi-homed, e gli altri di transito.
    (a) Si dia la lista dei path pubblicizzati da AS400. (b) È possibile che si formino dei cicli nei path pubblicizzati da qualche AS?
    R: (a) Solo "4.4.0.0:AS400". (b) No, perché se AS400 è multihomed, in pratica il grafo è senza loop.



11. Un'applicazione client-server comunica mediante socket a datagrammi su UDP. (a) Qual è la dimensione massima teorica di un messaggio? (b) Il server deve collegare la sua socket ad una porta ("binding") prima di eseguire la receive? (c) E deve eseguire la accept prima di eseguire la receive?

    R: (a) 64KB (teoricamente). (b) Sì, altrimenti non si sa su quale porta viene messo in ascolto. (c) No, quella è per il TCP.

12. Durante la fase di handshake di TCP, il client (initiator) ha inviato un segmento con SYN=1, SeqNum=1232. Cosa deve fare, e in che stato deve portarsi, se:
    (a) riceve un segmento con SYN=1, ACK=1, SeqNum=4134, Acknowledge=4233?
    (b) oppure se riceve un segmento con SYN=1, ACK=0, SeqNum=4134?

    R: (a) Potrebbe essere un vecchio segmento, di una precedente incarnazione. Il segmento va scartato e si attende quello buono. Si rimane in SYN_SENT. (b) Questo caso è legittimo: è l'apertura attiva simultanea. Quindi risponde con ACK e si porta in SYN_RECEIVED.

13. Un host TCP, in cui `MaxRecBuffer`=16000, ha attualmente `LastByteRead`=2999, `LastByteRecv`=10000, `NextByteExp`=6000. (a) Quanto è attualmente la `AdvertisedWindow`? (b) Quanto è la `AdvertisedWindow` se arriva un segmento con `SeqNum`=8000, `Length`=1000?

    R: (a) Tutto il buffer meno la parte tra `LastByteRead`=2999 e `NextByteExpected`-1=6000-1, quindi `AdvertisedWindow` $= 16000 - (5999 - 2999) = 13000$. (b) Non cambia, perché il nuovo segmento non è quello immediatamente successivo alla parte contigua (SeqNum non è uguale a NextByteExp)

14. Un router applica l'accodamento FairQueing a tre flussi A,B,C, con attualmente pacchetti della seguente durata (in qualche unità di tempo): A: 100,200,100,1000; B: 300,200,500; C: 400. (a) A che istante termina la trasmissione del pacchetto di C? (b) Se all'istante 1200 arriva un altro pacchetto del flusso C di durata 100, quando inizia la sua trasmissione?

    R: Applicando l'algoritmo si vede che l'ordine e gli istanti di trasmissione sono: A1(0), B1(100), A2(400), C1(600), A3(1000), B2(1100), B3(1300), A4(1800). Quindi (a) C1 termina a 1000. (b) All'istante 1200 il pacchetto C2 viene etichettato con il timestamp max(400,1200)+100=1300, quindi potrà essere trasmesso dopo B3 ma prima di A4, all'istante 1800.

15. Per ognuno dei seguenti attacchi effettuabili ad una votazione, si dica se è passivo o attivo, a quale aspetto di sicurezza (confidenzialità, integrità, disponibilità), e se ai dati o ai metadati.
(a) Risalire all'identità dell'elettore; (b) Modificare un voto (broglio); (c) Votare due volte.

R: (a) attacco passivo, alla confidenzalità dei metadati; (b) attacco attivo, all'integrità dei dati; (c) attacco attivo, all'integrità dei metadati (replay).

16. Un certo programma cifra i file con AES-128 in modalità CBC, la cui chiave è ottenuta dalla hash di una parola inserita dall'utente. Come parola, l'utente inserisce stringhe alfanumeriche (26 lettere maiuscole, 26 minuscole, 10 cifre decimali e 20 simboli di punteggiatura) di lunghezza compresa tra 6 e 8 caratteri. Qual è il numero medio di tentativi per un attacco brute force ad un file cifrato?

R: L'uso dell hash è ininfluente sullo spazio di ricerca, perché è deterministica nelle parola chiava usata. L'alfabeto è $26+26+10+20=82$ caratteri. Lo spazio di ricerca è grande $82^6+82^7+82^8 = 2*10^{15}$. In media si devono tentare circa la metà, che è 10^{15}. (A 10^6 tentativi al secondo, servono 33 anni, comunque molto meno di quanto potrebbe garantire AES.)

17. Nel protocollo a lato, K_A, K_B sono chiavi simmetriche precondivise con C; M è un messaggio, e H è una funzione di hash prefissata. Per B: (a) M è integro? (b) è autentico? (c) è puntuale?

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

R: (a) sì, grazie alla hash cifrata con la chiave K_B. (b) sì, un attaccante non può modificarlo senza rigenerare il codice di controllo. (c) no, il messaggio al passo 1 o al passo 3 possono essere intercettati e sostituiti con vecchi messaggi.

18. (a) Quali sono i principali campi di un certificato X.509? (b) Alice ha ricevuto un certificato di Bob, che è stato rilasciato da una CA a lei nota ma la data di emissione è posteriore (ossia, nel futuro) rispetto alla sua ora attuale. Può Alice fidarsi di tale certificato?

R: (a) Identità del subject, chiave pubblica del subject, identità dell'issuer, data di emissione, data di scadenza, firma digitale dell'issuer. (b) Questo può succedere se l'orologio di Alice è "indietro", oppure se la CA ha veramente emesso un certificato "postdatato". Quindi Alice dovrebbe verificare il suo orologio, e se è corretto non può fidarsi ancora dell'identità di Alice. Oppure può succedere perché il certificato viene rinnovato prima della scadenza (e magari con la stessa chiave).

19. Nel protocollo a lato, A e B hanno precondiviso le chiavi simmetriche K_A, K_B con la terza parte fidata C, e N è una nonce. (a) A è autenticato per B? (b) B è autenticato per A? Perché?

1. $A \to B : Id_A$
2. $B \to C : Id_B, E_{K_B}(Id_A, N)$
3. $C \to A : E_{K_A}(N)$
4. $A \to B : N$

R: (a) Sì, perché risponde alla sfida di decifrare la nonce N (che gli arriva da C). Solo chi conosce K_A può averlo fatto. (b) No, non c'è niente che garantisca a A di star comunicando con B. Bisognerebbe modificare il messaggio al passo 3 come segue: $C \to A : E_{K_A}(Id_B, N)$.

20. In SSL (e TLS): (a) a cosa serve il Sequence Number? (b) è una informazione di sessione o di connessione? (c) è incluso nell'intestazione dei segmenti del protocollo SSL Record?

R: (a) Ad implementare il controllo anti-replay. (b) Di connessione. (c) No, è usato solo nel calcolo e nella verifica del MAC di ogni segmento di SSL Record.