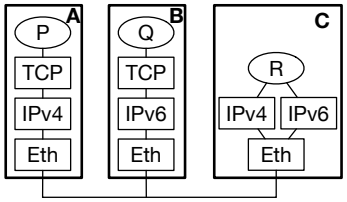
DMIF, Università degli Studi di Udine II appello A.A. 2018-19 — 18 febbraio 2019

Esame di **Reti di Calcolatori**

Soluzione

1. Nello schema a lato, i tre calcolatori sono collegati alla stessa rete Ethernet. I processi P e Q possono comunicare, eventualmente passando per C? A tal fine, cosa deve fare il processo R?
   R: Non possono comunicare direttamente, ma possono farlo passando per C. Il processo R deve tradurre pacchetti IPv4 in IPv6 e viceversa: toglie l'intestazione di un tipo e mette quell'altro, mantenendo il payload di livello 4. (Un po' come un NAT).



2. V.92 è uno standard per i modem analogici (quelli che si usavano sulle linee telefoniche, prima dell'ADSL) introdotto nel 1999. Determinare il bit rate grezzo di un modem V.92 che opera nella banda tra 0 e 4 kHz, con una modulazione in ampiezza di 128 livelli di segnale.

   R: Il numero grezzo di bit trasmessi per simbolo è $\log_2(128) = 7$, il baud rate è $2 * BW = 8kBaud$, per cui si ottiene un bit rate grezzo di $7 * 8 = 56kb/s$.

3. Nelle condizioni della domanda precedente, determinare il minimo rapporto segnale/rumore necessario per una trasmissione senza errori con un Forward Error Coding con code rate pari a 1/2.

   R: Con un code rate pari a 1/2 il numero di bit netti trasmessi per simbolo è $7 * 1/2 = 3.5$. Dal teorema SH si ha $3.5 \leq \frac{1}{2}\log_2(1 + SNR)$ da cui $SNR \geq 127$.

4. Un ricevitore Ethernet (a) come capisce quando inizia un frame? (b) E come capisce quando finisce?

   R: (a) Per il preambolo di 7 byte + il SDF (tecnica sentinel) (b) Per la mancanza di segnale.

5. In una certa cella Bluetooth (versione 2), l'accesso al mezzo è a divisione di tempo, con slot di $625\mu s$ e un bitrate grezzo di 3Mbit/s; il master trasmette negli slot pari, mentre gli slave negli slot dispari. Supponendo che un frame occupi un solo slot, e ricordando che ogni frame ha un'intestazione di 54 bit e un preambolo ("access code") di 72 bit, a quale bitrate massimo netto può trasmettere il nodo master?

   R: In uno slot ci stanno $625 * 10^{-6} * 3 * 10^6 = 1875$ bit, a cui bisogna togliere 54+72 bit di overhead, per cui i bit netti trasmessi sono 1749 bit , in ogni slot. Dato che il master può trasmettere solo negli slot pari, il bitrate complessivo con cui può trasmettere è $1749/(2 * 625 * 10^{-6}) = 1,4$ Mbps.

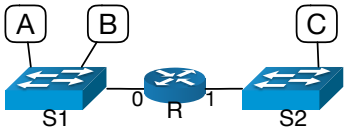
6. Per ognuna delle seguenti reti, si dica se l'indirizzo 192.168.7.14 vi appartiene o no: (a) 128.0.0.0/1; (b) 192.0.0.0/16; (c) 192.160.0.0/12.

   R: (a) sì; (b) no; (c) sì.

7. Un router riceve un pacchetto IP di 1500 byte, compresa l'intestazione di 20 byte, e deve inoltrarlo attraverso una interfaccia che ha una MTU di 520 byte. Quanto è lungo il payload del frammento che ha `MoreFragments`=0?

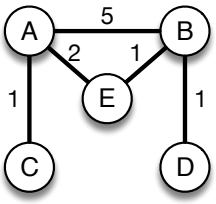
   R: Il primi due frammenti portano dei payload di 496 byte, perché 496 è il più grande numero inferiore a 520-20=500 e divisibile per 8 (perché l'offset va diviso per 8). Quindi il terzo ed ultimo frammento deve avere 1480-(496*2) = 488

8. Nella rete a destra, gli indirizzi assegnati alle varie interfacce sono i seguenti: R 0: 192.168.1.1; R 1: 192.168.2.1; A: 192.168.1.50; B: 192.168.1.200; C: 192.168.2.42. (a) Quale può essere il CIDR della rete di A e B? (b) Se A deve inviare un pacchetto IP a C, per quale indirizzo IP deve trovare il corrispondente MAC address, con ARP?



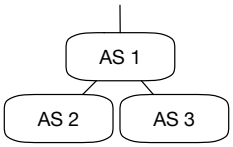
R: (a) 24 (b) Quello dell'interfaccia del router sulla sua rete, ossia 192.168.1.1.

9. I router a lato impiegano OSPF, un algoritmo di instradamento basato sullo stato dei collegamenti. Ad un certo punto il collegamento tra A e C viene interrotto, e poco dopo ripristinato. (a) È possibile che i pacchetti LSP generati da A vengano consegnati a D fuori ordine? (b) In tal caso, come fa B a capire quale è il pacchetto da utilizzare?



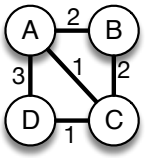
R: (a) Sì, perché OSPF diffonde i pacchetti in flooding appoggiandosi direttamente a IP, che si sa che non è affidabile; (b) Ogni pacchetto contiene l'identificatore di chi l'ha generato (A, in questo caso) e un numero progressivo. Il router B tiene traccia del più recente pacchetto LSP generato da A, cosicché se arriva un pacchetto (originato da A) con un numero più basso, viene scartato.

10. Gli autonomous system AS 2 e AS 3, le cui reti sono rispettivamente 130.7.1.0/24 e 130.7.2.0/24, sono conessi ad Internet attraverso un provider AS 1, il quale al suo interno ha anche le reti 130.7.0.0/24. (a) Che tipo di autonomous system è AS 1? (b) Quali reti vengono pubblicizzate dallo speaker di AS 1, al resto dell'Internet?



R: (a) Di transito. (b) 130.7.0.0/23 e 130.7.2.0/24.

11. I router della rete a lato usano DVMRP per instradare il traffico multicast. Sia A il core router di un certo gruppo G. (a) Quando viene inviato un pacchetto IP a tale gruppo, quanti pacchetti arrivano a C, e da quali router adiacenti? (b) Quale di questi viene inoltrato in flooding?



R: (a) 2, da A e da B. (b) Quello che viene da A, perché è quello che viene dal percorso più breve verso A.

12. Una applicazione sta producendo un flusso di dati su una socket TCP, alla velocità di 100 byte ogni 10 ms. La connessione TCP ha un MSS di 1460 byte e un RTT di 80ms. Si supponga che CongestionWindow e AdvertisedWindow siano abbondantemente grandi. (a) Quanto è grande il payload di ogni segmento inviato dall'host? (b) In percentuale, quanto è l'overhead introdotto dalle intestazioni IP e TCP?

R: (a) In un RTT il buffer accumula $100 * 80/10 = 800$ byte, inferiore al MSS. Quindi, per l'algoritmo di Nagle, ogni volta che arriva un ACK si invia un segmento di 800 byte. (b) L'overhead delle due intestazioni è di 40 byte, quindi $40/(40 + 800) = 4.76\%$.

13. Un'applicazione A ha scritto 8KB su una socket TCP il cui buffer di output è di 4KB. L'applicazione controparte B ha consumato 3KB, e il buffer di input della sua socket è di 2KB. Cosa succede all'applicazione A se prova ad eseguire tre scritture da 1KB l'una? (Si supponga che nel frattempo B non consumi altri dati).

R: La differenza tra i dati scritti sulla socket e dati consumati non può mai superare la somma dei buffer in gioco, perché altrimenti i dati andrebbero persi. Quindi, lo spazio ancora disponibile per le scritture di A è $(4 + 2) - (8 - 3) = 1$KB. Per cui, la prima scrittura da 1KB ha successo, ma la seconda si blocca in attesa che si liberi spazio nel buffer.

14. Un router applica la strategia RED alla coda di una linea che ha una velocità di 3 MB/s, mentre i pacchetti che devono essere accodati arrivano con un datarate medio di 10 MB/s. Sapendo che `MinThreshold`=50 kB, `MaxThreshold`=100 kB, `MaxP`=1, quant'è la lunghezza media della coda?

R: La lunghezza della coda si stabilizza quando i dati che vengono accodati equivalgono a quelli che escono dalla coda. Quindi la probabilità p di accodamento deve essere tale che $10p = 3$, e quindi $p = 0,3$. Pertanto la probabilità di eliminazione per ogni pacchetto che arriva è $q = 1 - p = 0,7$. Ricordando

che $q = (AvgLen - MinThreshold)/(MaxThreshold - MinThreshold)$, dobbiamo risolvere l'equazione $0,7 = (AvgLen - 50)/(100 - 50)$, che ci porta a $AvgLen = 85kB$.

15. Dal punto di vista della quantità di dati messi in sicurezza end-to-end, è meglio implementare i servizi di cifratura e/o autenticita dei dati a livello trasporto, a livello di rete, o a livello datalink?

    R: A livello trasporto o meglio ancora rete. A livello datalink i dati rimangono scoperti nei router.

16. Un certo programma utilizza AES-256 in modalità CBC per cifrare i propri dati. La chiave di 256 bit è generata calcolando lo SHA-256 di un PIN di 4 cifre decimali scelto dall'utente, concatenato con la sua data di nascita nel formato DD/MM/AAAA. Qual è la complessità di un attacco a forza bruta (ovvero, quante chiavi bisogna tentare in media), supponendo che gli utente abbiano da 0 a 100 anni?

    R: In 100 anni ci sono (365*4+1)*25=36525 giorni. Quindi le possibili combinazioni sono $10^4 * 36525 = 365,25 * 10^6$. In media bisogna provarne la metà, cioè circa 180 milioni—che è pochissimo. Naturalmente si può restringere ulteriormente il range se si hanno altre informazioni sull'età dell'utente.

17. Il protocollo a lato serve per generare semplici certificati di chiave pubblica. PU_A è una chiave pubblica generata sul momento da A, H è una funzione di hash prefissata, PR_{CA} è la chiave privata della CA, la cui chiave pubblica è ben nota a tutti i partecipanti.

    1. $A \to CA : A, PU_A$
    2. $CA \to A : E_{PR_{CA}}(A, H(PU_A))$

    (a) Viene garantita la correttezza del certificato, ossia l'associazione tra PU_A e identità di A?
    (b) Se questo non è il caso, si corregga il protocollo modificando solo il passo 1 e supponendo che A e CA abbiano precondiviso una chiave simmetrica K (e senza usare cifratura simmetrica).

    R: (a) No, perché al passo 1 chiunque può sostituirsi ad A e farsi rilasciare un certificato con una identità fasulla. (b) Ci sono diversi modi, ma il più semplice è aggiungere un HMAC, ad esempio come segue:
    1. $A \to CA : A, PU_A, H(K, PU_A)$

18. Nel protocollo a lato, K_A e K_B sono due chiavi simmetriche precondivise tra A e C e B e C rispettivamente, e K è una chiave di sessione generata da A sul momento. (a) La chiave K è puntuale? (b) A è autenticato per B? (c) B è autenticato per A?

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

    R: È una variante (più debole) del ben noto protocollo *wide mouthed frog*. (a) La chiave non è necessariamente puntuale: un attaccante può sostituire il primo messaggio con uno vecchio. (b) A non è autenticato per B, perché K non è puntuale (c) B è autenticato per A, se A vede arrivare un messaggio cifrato con la K che ha mandato poco prima: in pratica B sta rispondendo ad una challenge.

19. Alice manda a Bob una mail PGP cifrata, ma non firmata. Bob non si fida, e chiede ad Alice una firma non ripudiabile del messaggio. Può Alice soddisfare questa richiesta, senza reinviare l'intero messaggio? (Si supponga che Alice e Bob abbiano le rispettive chiavi pubbliche e private, come di consueto).

    R: Sì, perché è sufficiente che invii $E_{PR_A}(H(M))$.

20. Dei metodi di scambio chiave di SSL (e TLS), (a) quali garantiscono l'autenticazione del server per il client? (b) E quali quella del client per il server?

    R: (a) RSA, Ephemeral DH, Fixed DH. (a) Ephemeral DH, Fixed DH.