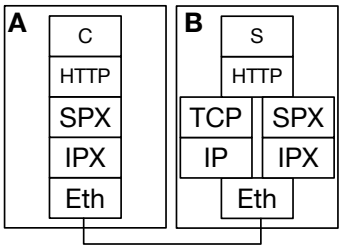
DMIF, Università degli Studi di Udine V appello A.A. 2017-18 — 17 settembre 2018

Esame di **Reti di Calcolatori**

Soluzione

1. IPX/SPX ("Internetwork Packet Exchange/Sequenced Packet Exchange") era uno stack di rete diffuso fino alla fine del secolo scorso (e che si può ancora incontrare in qualche azienda); IPX è un protocollo di rete, e SPX è un protocollo di trasporto orientato alla connessione. Nella figura a lato sono rappresentati un calcolatore A con il singolo stack IPX/SPX, e un calcolatore B con il doppio stack. (a) L'applicazione C può stabilire una connessione con l'applicazione S? (b) Quando riceve un frame (da A, ma anche da altri calcolatori), come fa lo strato Ethernet di B a scegliere il protocollo di rete a cui passare il payload?



R: (a) Sì, passando per lo stack IPX/SPX. (b) In base al campo EtherType nell'intestazione del frame Ethernet (IPX è rappresentato da 0x8137, IP da 0x0800)

2. Intel HEX è un modo per rappresentare dati binari in un formato testuale, in cui ogni byte è rappresentato da un coppia di caratteri esadecimali ASCII. La struttura dati è organizzata in linee delimitate da un carattere ASCII ":" all'inizio e da LF (linefeed) alla fine; ogni linea contiene un header di 4 byte, un blocco dati (payload) di lunghezza specificata nell'header, e un byte di checksum del blocco dati. Ad esempio, questa è una linea con un blocco dati di 16 byte:

	header	blocco dati	cs	
:	10010000	21460136012147013600 7EFE09D21901	40	(LF)

Si determini il bit rate netto del payload se si trasmettono in questo formato, con blocchi dati di 32 byte, su un canale fisico di baud rate 1kBaud/s, nel quale ogni simbolo codifica 1 carattere ASCII utile.

R: Ogni linea consta di 1+4*2+32*2+1*2+1 = 76 caratteri e codifica 32*8 = 256 bit. Poiché il numero di caratteri trasmessi per secondo è 1000, vengono trasmesse 1000/76 = 13,2 linee al secondo e quindi con un bit rate netto di 256*1000/76 = 3.4 kb/s.

3. Se nella domanda precedente un carattere ASCII trasmesso è codificato con 7 bit, determinare il rapporto S/N minimo necessario per una trasmissione senza errore.

R: Dal teorema SH $\log_2(M) = 1/2 \log_2(1 + SNR)$ ove $M = 2^7$ e quindi si ha in condizioni ideali SNR = 42 dB o SNR =16383.

4. Nella codifica 4B/5B, i bit 0100 vengono rappresentati come 01010. La codifica della sequenza 01000100 viene trasmessa su un canale che, a causa di un disturbo, inverte uno dei bit (ma non si sa quale). Qual è la probabilità che tale errore venga rilevato dal decodificatore?

R: La sequenza codificata è 0101001010. La regola di buona formazione della codifica 4B/5B richiede che non ci siano mai più di tre 0 consecutivi; quindi un errore per essere rilevato deve portare almeno 4 zeri consecutivi. Questo succede solo per i bit 4 e 7, quindi 2 possibilità su 10, quindi la probabilità è 20%.

5. Due stazioni 802.11n hanno negoziato un bitrate grezzo di 240 Mbps. Sapendo che SIFS = 9μs e DIFS = 34μs, il frame RTS è di 20 byte e ACK e CTS sono di 14 byte, il frame dati ha una intestazione di 30 byte e un CRC-32 di 4 byte, si dica quale bitrate netto massimo si può ottenere con payload di 1500 byte (trascurando i tempi per la contesa del canale).

R: Per trasmettere un frame di dati servono 1 DIFS e 3 SIFS, più un RTS, un CTS e un ACK alla fine. I byte trasmessi complessivamente sono 20 + 14 + 30 + 1500 + 4 + 14 = 1582 byte, che impiegano

$1582 * 8/240 = 52,73\mu s$. A questo bisogna aggiungere $34 + 9 * 3 = 61\mu s$, per un totale di $113,73\mu s$. Quindi bitrate netto è quindi 1500*8/113,73= 105,51 Mbps.

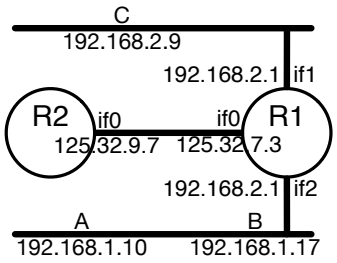
6. Tre host, collegati alla stessa LAN, hanno indirizzi IP A=12.10.0.7, B=12.70.7.7, e C=12.110.7.23. (a) Se il CIDR è /10, a quali reti appartengono? (b) Quali host possono comunicare direttamente senza passare per un router (a meno di configurazioni ad hoc)?

   R: (a) A: 12.0.0.0/10; B: 12.64.0.0/10; C: 12.64.0.0/10. (b) Solo B e C.

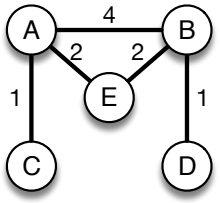
7. Un'azienda ha bisogno di 300 indirizzi IP. Se gli viene assegnata una singola rete, qual è l'utilizzo percentuale di tale spazio di indirizzamento? E se invece le vengono assegnate tre reti più piccole?

   R: La più piccola rete che contiene 300 indirizzi è una /23, ossia 9 bit di host, per totali 512-2 = 510 indirizzi utili. La percentuale di utilizzo è 300/510 = 58,8%. Se invece possiamo usare tre reti /25 da 126 indirizzi l'una, abbiamo 300/(3*126) = 79,4%. Si può fare anche di meglio, con due reti /25 euna /26, per totali 320 indirizzi e un'efficienza del 95%.

8. Nella rete a lato, il router R2 è quello di frontiera, ed è connesso al resto dell'Internet. L'host A deve inviare un pacchetto IP all'indirizzo 123.45.67.89. (a) Quale indirizzo deve risolvere con il protocollo ARP? (b) Chi gli risponderà, e con quale informazione?
   R: (a) L'indirizzo 192.168.2.1, in broadcast. (b) Il router R1, con il MAC address della sua interfaccia if2.



9. I router a lato utilizzano un algoritmo di instradamento basato sullo stato delle linee. Si dia la tabella di instradamento di B (a) a regime, e (b) dopo che viene aggiunto un collegamento tra C e D di peso 1.



R: (a)

Dest.	dist	next hop
A	4	A
B	0	-
C	5	A
D	1	D
E	2	E

(b)

Dest.	dist	next hop
A	3	D
B	0	-
C	2	D
D	1	D
E	2	E

10. (a) Perché nel routing interdominio non si utilizza un algoritmo basato sul vettore delle distanze? (b) Supponiamo che AS1 sia connesso ad AS2 stub e ad AS3 che è di transito. Che tipo di AS è AS1?

    R: (a) per i soliti motivi: impossibile definire una singola metrica, difficile raggiungere la stabilità, bisogno di tenere sotto controllo i percorsi per scegliere il percorso con criteri politici. (b) Di transito.

11. IPv6 offre varie funzionalità avanzate, come il supporto per il real-time e il Quality of Service. (a) A questo scopo, quale informazione è presente nell'intestazione del pacchetto? (b) Cosa succede a tale informazione se IPv6 viene incapsulato in un tunnel IPv4?

    R: (a) Il TrafficClass per la priorità e la FlowLabel per identificare i flussi all'interno dei router. (b) non è più utilizzabile dai router IPv4, che quindi non possono implementare il servizi real-time richiesti.

12. Lo strato TCP di un host A ha appena inviato un segmento con SYN=1, ACK=0, SeqNum=31541 ad un altro host B. Poi riceve da B un segmento con SYN=1, ACK=1, SeqNum=53628, Acknowledgement=23143. (a) È corretto? Perché? (b) Cosa deve fare A?

    R: (a) no, non è corretto, perché Acknowledgement dovrebbe essere 31542. Probabilmente è un vecchio segmento appartenente alla fase di handshake di una connessione precedente. (b) Scartare il segmento appena ricevuto, e aspettare (fino al timeout) quello con l'Acknowledgement corretto.

13. Una rete è realizzata con degli switch Ethernet e router a 1Gbps. (a) Supponendo che una connessione TCP tra due host riesca a sfruttare il 50% del bitrate grezzo, qual è il tempo di wraparound? (b) Cosa

potrebbe succedere se un pacchetto IP viene consegnato (o reinviato da un router o un attaccante) con un ritardo maggiore di tale tempo?

R: (a) Il bitrate netto è 500 Mbps, ossia 62,5 MB/s. A questa velocità, il wraparound avviene dopo $2^{32}/(62,5 * 10^6) = 68,72$ secondi. (b) Potrebbe essere scambiato per buono durante un nuovo ciclo del contatore di sequenza. Ossia, un segmento portante dati vecchi verrebbe preso al posto di quelli nuovi, se arriva quando la finestra copre proprio il suo numero di sequenza.

14. Un router inizia a servire due flussi secondo la politica di accodamento equo (Fair Queueing); il flusso A ha in coda 2 pacchetti di lunghezza A1=100, A2=300; il flusso B ha in coda 3 pacchetti di lunghezza B1=200, B2=100; B3=300. Inoltre all'istante 800 arriva un pacchetto A3=100. In che ordine vengono trasmessi i sei pacchetti?

    R: A1, B1, B2, A2, B3, A3. (A3 finirebbe prima di B3, ma quando arriva in coda B3 è già in trasmissione e non c'è prelazione).

15. Nel modello Dolev-Yao del canale insicuro, a volte si assume l'esistenza di una "terza parte fidata". (a) Come sono le connessioni tra le controparti (A e B) e questa terza parte? (b) Perché normalmente non si utilizza tale parte come intermediario per lo scambio dei veri messaggi tra A e B?

    R: (a) Sicure, non attaccabili dall'attaccante. (b) Si potrebbe in teoria, ma solitamente questi canali sicuri sono lenti, costosi, o fuori tempo (non esistono nel momento in cui A e B devono comunicare).

16. Un maldestro programmatore utilizza DES per cifrare dei dati, e come chiavi utilizza le targhe delle auto, scritte come stringhe della forma "AB123CD" (che sono esattamente 56 bit). Sapendo che nelle targhe le lettere sono prese da un alfabeto di 22 caratteri, quanto è grande lo spazio delle chiavi del nostro sventurato programmatore?

    R: $22^4 * 1000 = 234.256.000$. Un niente.

17. Si consideri il protocollo di scambio chiave a lato, variante del Diffie-Hellman, dove y_A e y_B sono le due mezze chiavi pubbliche, K_A è un segreto precondiviso tra A e la terza parte fidata C, e analogamente per K_B. (a) Il protocollo è soggetto all'attacco man-in-the-middle? (b) C è in grado di calcolare la chiave di sessione D-H stabilita tra A e B?

    1. $A \to C : A, y_A, H(K_A, A, y_A)$
    2. $C \to B : A, y_A, H(K_B, A, y_A)$
    3. $B \to C : B, y_B, H(K_B, B, y_B)$
    4. $C \to A : B, y_B, H(K_A, B, y_B)$

    R: (a) No, perché i messaggi scambiati sono autenticati da C, grazie alla hash con i segreti precondivisi. Se un attaccante prova a sostituire il messaggio con una propria mezza chiave, C se ne accorgerebbe. (b) No, non ha nessuna informazione in più degli attaccanti.

18. Si consideri il protocollo a lato, dove PU_A è la chiave pubblica di A (che B non conosce ma che gli viene inviata al passo 1), mentre K è una chiave random generata da B. (a) Il messaggio M è confidenziale? (b) A è autenticato per B?

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

    R: (a) No, un attaccante può facilmente fare un MITM mandando la propria PU al primo passo, spacciandola per quella di A, così inganna B, può ottenere la chiave K usando la sua chiave PR_E, inviarla a A, e poi intercettare il messaggio di risposta.

    1. $A \to E : A, PU_A$
    1'. $E \to B : A, PU_E$
    2'. $B \to E : E_{PU_E}(K)$ 2. $E \to A : E_{PU_A}(K)$
    3. $A \to E : E_K(M)$ 3'. $E \to B : E_K(M)$

    (b) no: se al primo passo un attaccante E sostituisce PU_A con PU_E, B non ha modo di accorgersene.

19. Il protocollo a lato schematizza il caso in cui un client invia una email con la sua firma digitale al server di posta S, e poi il server inoltra la mail al destinatario B aggiungendo il suo timestamp. (a) Il messaggio M è non ripudiabile? (b) È puntuale?

    1. $A \to S : A, B, M, E_{PR_A}(A, B, H(M))$
    2. $S \to B : A, B, M, E_{PR_A}(A, B, H(M)), E_{PR_S}(T, H(M))$

    R: (a) sì, è firmato da A. (b) no, un attaccante può intercettare il primo scambio da A a S, e rimandarlo più tardi quante volte vuole.

20. Un host riceve un pacchetto IP con un payload IPsec, ma nel suo SADB di ingresso non c'è una entry corrispondente a quel Security Parameter Index. (a) Cosa deve fare l'host di quel pacchetto? (b) Può fare qualcosa per rimediare alla situazione?

    R: (a) Non può processarlo, quindi deve per forza scartarlo. (b) Può mandare un messaggio al mittente (con ICMP ad esempio) che il pacchetto è stato scartato. Il mittente vedrà se è il caso di ricreare una SA (perché potrebbe essere andata perduta per un reset del ricevente).