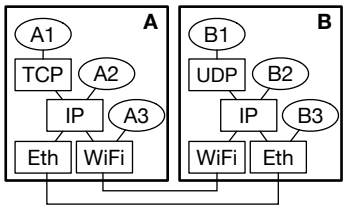
DMIF, Università degli Studi di Udine — I appello A.A. 2018-19 — 28 gennaio 2019

Esame di **Reti di Calcolatori**

Soluzione

1. Lo schema a lato rappresenta due host A e B connessi da due mezzi fisici e su cui sono in esecuzione le applicazioni A1, A2, A3 e B1, B2, B3 rispettivamente. Le applicazioni accedono ai vari protocolli come indicato. Si dica quali delle seguenti comunicazioni può avere luogo:
   a) A1–B1 b) A2–B2 c) A3–B3
   R: a) no; b) sì; c) no.



2. Si vuole realizzare una linea di trasmissione della capacità di 1 Mb/s di bitrate di dati senza errori, utilizzando un fascio di microonde in una banda di frequenza centrata a 10 GHz e di larghezza 500 kHz. Determinare il rapporto segnale/rumore (in dB) della linea in tali condizioni.

   R: Dal teorema di S-H è $1Mb/s \leq 500kHz \log_2(1+SNR)$ quindi $SNR \geq 3$ ossia $SNR \geq 4.7dB$

3. Sulla linea di trasmissione dell'esercizio precedente, viene utilizzato un Forward Error Coding che codifica 12 bit in pacchetti di 24 bit. Determinare il numero minimo di bit che deve venir codificato da un simbolo per baud, per avere un bitrate netto di 1 Mb/s.

   R: Con un bitrate netto di 1 Mb/s e un code rate di 12/24 = 0.5, il bitrate grezzo deve essere di 2 Mb/s. Dal teorema di Nyquist il baud rate è al massimo 500 kHz * 2 = 1MBaud, e quindi il numero di bit codificati per baud deve essere almeno 2Mb/s / 1 MBaud = 2.

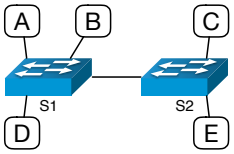
4. Una certa linea ha una probabilità di errore $p = 10^{-3}$ per ogni bit. Prima della trasmissione ogni 3 bit viene aggiunto un bit di parità. Qual è la probabilità che in un pacchetto di 4 bit così formato avvengano degli errori non rilevati?

   R: Affinché ci siano errori non rilevati dal bit di parità, gli errori devono essere pari. Su 4 bit, questo significa che ci devono essere o 2 o 4 bit errati. La probabilità che questo succeda è $P = \binom{4}{2}p^2(1-p)^2 + \binom{4}{4}p^4 = 6 * p^2(1-p)^2 + p^4 = 5.99 * 10^{-6}$.

5. Due stazioni Ethernet A e B hanno già tentato di trasmettere una volta, rilevando collisione. Al secondo tentativo, anche una terza stazione C prova a trasmettere (per la prima volta). Qual è la probabilità che la trasmissione avvenga senza collisioni?

   R: A causa del backoff esponenziale, A e B aspettano un tempo random compreso di 0 o 1 SlotTime ($= 51.2\mu s$), mentre C non aspetta niente (perché è il suo primo tentativo). Quindi affinché non ci sia collisione bisogna che sia A sia B scelgano di aspettare 1 SlotTime (altrimenti vanno in collisione con C). La probabilità che questo avvenga è $1/2 * 1/2 = 1/4$.

6. Nella rete a lato, gli switch S1 e S2 sono ad autoapprendimento. S2 ha le tabelle completamente popolate, mentre S1 è appena stato resettato. L'host A invia un frame indirizzato a C. (a) A quali host viene recapitato tale frame? (b) Se C risponde ad A, il suo frame a chi viene recapitato?

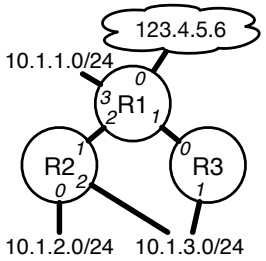


   R: (a) Agli host B, C, D. (b) Solo ad A (perché S1 ha imparato dove è A).

7. Un'azienda ha tre reti A, B, C con 100, 300 e 200 postazioni rispettivamente. Per ognuna di queste reti si dia una sottorete (minima) all'interno della rete 192.168.0.0/16.

   R: Per la rete A serve una rete /25, per la B serve una /23 e per la C serve una /24. Una possibilità è la seguente: A=192.168.0.0/25; B= 192.168.2.0/23, C=192.168.1.0/24.

8. Si dia la tabella di inoltro del router R3 della rete a lato, sapendo che le interfacce dei router hanno i seguenti indirizzi:

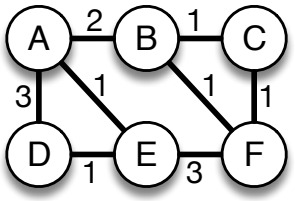


R1:if1=192.168.1.1 R2:if0=10.1.2.1
R1:if2=192.168.2.1 R2:if1=192.168.2.2
R1:if3=10.1.1.1 R2:if2=10.1.3.1
R3:if0=192.168.1.2
R3:if1=10.1.3.2

R:

dest	if	next hop
10.1.2.0/24	if1	10.1.3.1
10.1.3.0/24	if1	–
/	if0	192.168.1.1

9. I router in figura impiegano un algoritmo basato sul vettore delle distanze.
(a) Si dia la tabella di instradamento del router A.
(b) Cosa cambia se si interrompe il collegamento A-E?



R: (a)

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

(b)

Dest.	dist	next hop
A	0	-
B	2	B
C	3	B
D	3	D
E	4	D
F	3	B

10. Diversi servizi utilizzano gruppi multicast per la comunicazione tra processi vicini, ossia in esecuzione su host della stessa sottorete ma che non si conoscono a priori; ad esempio mDNS usa il gruppo 224.0.0.251 per risolvere gli hostname del dominio `.local`. (a) Come si può limitare la diffusione dei pacchetti multicast alla sola sottorete locale? (b) È necessario usare il protocollo IGMP? Perché?

R: (a) Impostando il TTL=1 (b) no, perché IGMP serve per comunicare il router gateway di quali gruppi siamo interessati, ma in questa situazione i gateway non hanno alcun ruolo.

11. Syslog è uno standard di logging remoto ampiamente utilizzato, in cui gli host possono inviare messaggi diagnostici ad un server (`syslogd`) in ascolto su una porta ben nota. Il server memorizza tali messaggi in un file (o li processa in altri modi); non è necessario che dia conferma di ricezione al mittente. Quale protocollo di trasporto può essere usato per implementare tale servizio su rete locale? Perché?

R: Va bene UDP, se la rete sottostante è abbastanza libera e affidabile. Così è scalabile e non richiede la creazione e mantenimento di una connessione.

12. Una socket TCP è appena entrata nello stato ESTABLISHED e, ancora prima che spedisca il primo segmento, riceve un segmento con ACK=1, Length=0. È corretto? Cosa deve fare TCP a fronte di tale segmento?

R: Sì, è legittimo: probabilmente è un duplicato dell'ultimo segmento che il client ha inviato al server alla fine della fase di handshake. Per essere certo è sufficiente vedere se l'Acknowledge corrisponde al valore fissato durante la fase di handshake. In tal caso il segmento può essere tranquillamente ignorato, e la comunicazione può continuare normalmente.

13. Una socket TCP ha inviato tre segmenti di 1400 byte ciascuno e con `SeqNum` pari a 1000, 2400 e 3800 rispettivamente. Riceve un segmento con `Acknowledgment`=2400, `AdvertisedWindow`=6000, e poi uno con `Acknowledgment`=1000, `AdvertisedWindow`=5000. A questo punto quanti byte può ancora inviare?

R: Il secondo segmento di ACK è stato consegnato in ritardo rispetto al primo, evidentemente, quindi bisogna fare riferimento al primo. In quel momento la finestra era di 6000 byte, ma 2800 sono già stati spediti e non ancora riconosciuti, quindi si possono invare ancora 6000-2800=3200 byte.

14. Una connessione TCP, che utilizza la ritrasmissione veloce e il recupero veloce, ha attualmente `CongestionWindow` = 10000. Dopo aver inviato 7 segmenti da 1 MSS (pari a 1000 byte) a partire dal numero di sequenza 0, ha ricevuto i seguenti `Acknowledgment`: 1000, 3000, 3000, 3000. (a) Quale numero di sequenza ha il prossimo pacchetto da inviare? (b) Quanto diventa `CongestionWindow`?

R: (a) 3000, per la ritrasmissione veloce. (b) L'incremento per ack è di MSS*MSS/`CongestionWindow`= 100 byte, quindi dopo quattro ack ricevuti `CongestionWindow` è pari a 10400. A questo punto viene dimezzato per il recupero veloce, e quindi diventa 5200 byte.

15. In che modo si può rendere confidenziale il traffico tra un client e un server che comunicano via TCP attraverso una rete insicura, nel caso in cui si disponga del codice sorgente del client ma non del server?

    R: Purtroppo non si può usare SSL/TLS, perché richiederebbe di intervenire anche sul codice del server che non abbiamo. Quindi non rimane che usare IPsec, o in trasport da host a host o in tunnel attraverso i router di frontiera.

16. Un flusso di pacchetti $M_1, M_2, \ldots$ viene cifrato usando RC4 in questo modo: $C_i = E_{K_i}(M_i)$ dove $K_i = H(K||i)$, H è una funzione di hash predefinita e K è una chiave master prefissata. Il contatore i è di n bit, e si riazzera quando supera il limite. Se il flusso è sufficientemente lungo, quale attacco si potrebbe condurre?

    R: Se la chiave master non viene cambiata, dato che i cicla dopo 2^n, i pacchetti M_{i+k*2^n} $(k = 0, 1, 2, \ldots)$ sono tutti cifrati con la stessa chiave. Quindi possono essere rimpiazzati l'uno con l'altro (attacco all'integrità). Inoltre, dato che sono cifrati con RC4, possono essere messi in XOR annullando così l'effetto della cifratura (attacco alla confidenzialità).

17. Nel protocollo a lato, A e B possiedono entrambi una chiave privata e corrispondente chiave pubblica, e N è una nonce generata da B. (a) Il messaggio M è confidenziale? (b) Si completi il passo 3. in modo da garantire puntalità e non ripudio di M (eventualmente usando una funzione di hash H).

    1. $A \to B : E_{PU_B}(M)$
    2. $B \to A : N$
    3. $A \to B : E_{PR_A}(?)$

    R: (a) sì, perché è cifrato con la chiave pubblica di B (b) 3. $A \to B : E_{PR_A}(N, H(M))$

18. In Kerberos: (a) Chi potrebbe avere interesse a modificare il contenuto dei ticket rilasciati da AS e da TGS? (b) in che modo si garantisce l'integrità di tali ticket?

    R: (a) L'utente stesso, ad esempio per estendere la durata del ticket o per usare un SGT presso un altro server. (b) Attraverso la cifratura del ticket con una chiave simmetrica nota soltanto a AS e TGS, o a TGS e server.

19. Un server email gestisce una mailing list "anonima e sicura": ogni utente può inviare una mail PGP all'indirizzo della mailing list (p.e. `spotted@uniud.it`) e il server si incarica di inoltrarla a tutti gli iscritti. Si vuole garantire l'autenticità del messaggio, ma non la sua segretezza né l'identità del mittente.
    (a) Quale chiave pubblica deve conoscere chi vuole inviare un messaggio? (b) Con quale chiave il server firma il messaggio che manda agli iscritti? (c) Cosa deve conoscere ogni iscritto alla mailing list?

    R: (a) Dato che non è necessario garantire la segretezza della mail, il mittente non deve necessariamente cifrare la mail, quindi non serve la chiave pubblica del server `spotted@uniud.it`. Però cifrando la mail si può raggiungere una maggiore anonimicità: terze parti possono vedere il messaggio in transito dal mittente al server, quindi capire chi scrive il messaggio ma non cosa scrive. (b) Con la propria chiave privata. (c) Solo la chiave pubblica del server, per verificare l'autenticità delle firme.

20. Un processo sta inviando un flusso di dati ad una velocità di 1MB/s, con segmenti lunghi mediamente 1000 byte su IPsec in modalità trasporto. I pacchetti vengono consegnati quasi tutti con un ritardo costante di 20 ms, tranne qualcuno che arriva con un ritardo di 100ms. Cosa succede a tali pacchetti "ritardatari"? (Suggerimento: si pensi alle misure antireply di IPsec.)

    R: Vengono inviati 1000000/1000= 1000 pacchetti al secondo, ossia un pacchetto ogni millisecondo. La finestra antireply scorre alla stessa velocità, per cui se un pacchetto arriva con un ritardo di oltre 64 ms rispetto al primo della finestra, cade fuori dalla finestra e viene scartato. I pacchetti ritardatari arrivano con un ritardo di 80ms rispetto ai primi, e quind vengono scartati.