Compito di Reti di Calcolatori

31-Luglio 2012

1. Network security (6 pts)

A. Cos'è la network security ? Ovvero, che problemi affronta la network security ? [Suggerimento: 4 problemi]

confidenzialità, autenticazione, integrità e disponibilità

B. Descrivere come un Public Key Cryptosystem con chiave pubblica (K+) e chiave privata (K-) può essere usato per garantire una comunicazione sicura e la correttezza del messaggio

Detto M il plaintext e C il ciphertext, la confidenzialità si ottiene inviando C=K+(M). Solo il ricevente ha K- e ottiene: M=K-(C).
La integrità la si ottiene spedendo C = K-(M). Solo il mittente ha K- pertanto il messaggio può essere stato scritto solo da lui.

C. Quali sono i vantaggi e svantaggi di un Public Key Cryptosystem (PKC) su un symmetric cryptosystem (shared secret key) dal punto di vista del networking? (2 pts)

PKC risolve il problema dello scambio della chiave su un canale sicuro prima che la comunicazione possa aver luogo: questo è particolarmente difficile se le due entità comunicano per la prima volta. Di contro un sistema simmetrico è più facile da implementare su HW di poco costo.

2. Indirizzamento IP (10 pts)

A. Sia assegnato l'indirizzo 135.12.1.200 con Netmask: 255.255.254.0 indicare (2 pts):

Network	**135.12.0.0/23**
Broadcast	**135.12.1.255**
HostMin	**135.12.0.1**
HostMax	**135.12.1.254**
Numero di Hosts	**510**

B. Dividere lo spazio in 4 subnets uguali e per ognuna indicare (8 pts)

Netmask: 255.255.255.128 = /25 11111111.11111111.11111111.1 0000000

	Subnet-1	Subnet-2	Subnet-3	Subnet-4
Network	**135.12.0.0/25**	**135.12.0.128/25**	**135.12.1.0/25**	**135.12.1.128/25**
Broadcast	**135.12.0.127**	**135.12.0.255**	**135.12.1.127**	**135.12.1.255**
HostMin	**135.12.0.1**	**135.12.0.129**	**135.12.1.1**	**135.12.1.129**
HostMax	**135.12.0.126**	**135.12.0.254**	**135.12.1.126**	**135.12.1.254**
Num.di Hosts	**126**	**126**	**126**	**126**

Numero complessivo di Hosts: 126 x 4 = 504

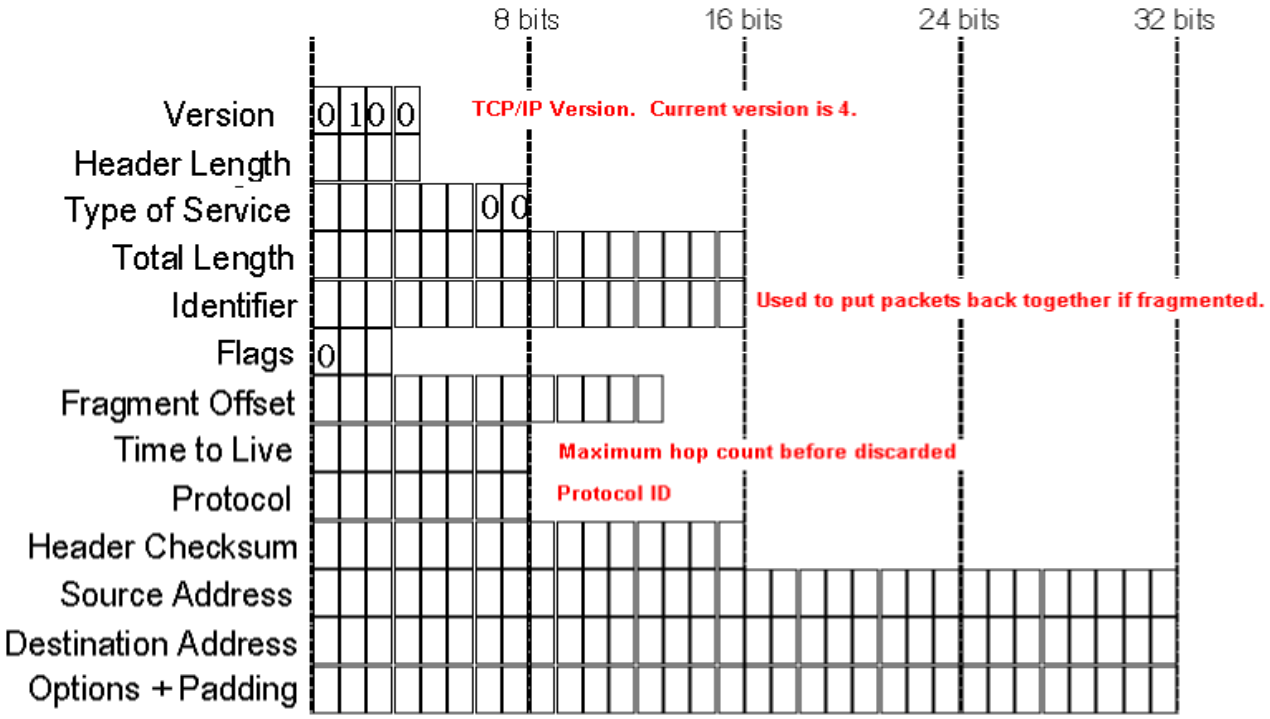
3. Protocollo IP (6 pts)

Avendo ricevuto i seguenti dati nella sezione IP

```
46 00 00 2E 00 00 40 00 01 01 35 A1 0A 0A 0A 01 0A 0A 0A 02 0C 0A 0F 0E 00 00 FF
FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Specificare

Version	(4)	4	# IP V4
Header Length	(4)	6	# 6x4=24 bytes
Type of service	(8)	00	# 0 = Best Effort
Total length	(16)	00 2E	# 46 (22 bytes di dati)
Identification	(16)	00 00	# 0
Flags	(3)	010	# Don't fragment
Fragment offset	(13)	0 00	# 0
Time to live	(8)	01	# 1
Protocol	(8)	01	# ICMP
Checksum	(16)	35 A1	# Correct
Source address	(32)	0A 0A 0A 01	# 10.10.10.1
Dest. Address	(32)	0A 0A 0A 02	# 10.10.10.2
Options+Padding	(x)	0C 0A 0F 0E	# Un caffè (op. inventate)

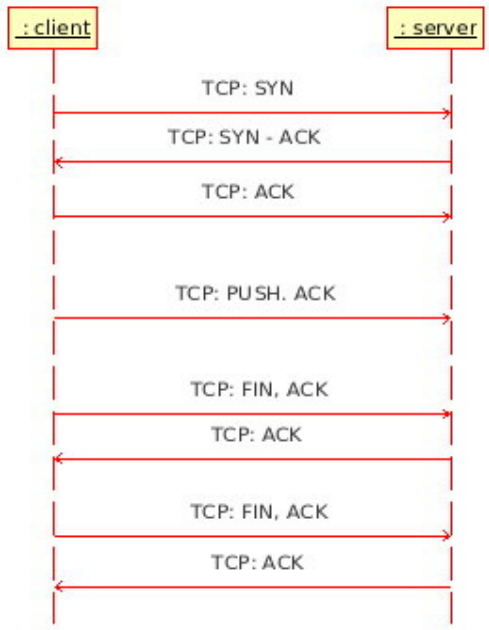


4. Dato il pacchetto di cui al punto precedente, dire se le seguenti affermazioni sono Vere o False (3 pts)

Il pacchetto è un frammento	**F (MF=0)**
Il pacchetto è l'ultimo frammento	**F (Offset=0)**
L'header ha delle options	**V (header da 24B)**
Sorgente e Destinazione sono nella stessa LAN	**V**
Ci sono Options e Padding	**V**
Il pacchetto viene scartato	**F**

5. TCP (3 pts)

Mostrare il diagramma temporale di una interazione TCP dall'apertura della connessione alla sua completa chiusura



6. Layer-2 bridging (2 pts)

Sotto è descritto l'algoritmo di "transparent bridging": l'algoritmo contiene uno o più errori. Trovare gli errori sapendo che SA=source address e DA=destination address

(1) Receive a frame
*(2) If (**SA** in table) and (**SA** local) then not forward else forward*
*(3) If (**DA** in table) check direction and update if needed*
*(4) If (**DA** not in table) add to table*

Dove c'è SA deve esserci DA e viceversa