Scritto 26 Maggio 2023

1) [5 punti] A cosa serve e come funziona il meccanismo di Fragmentation and Reassembly IPv4

2) [5 punti] Come posso riconoscere l'indirizzo IP di un server SMTP di dominio al quale spedire un messaggio di posta elettronica indirizzato a nome.cognome@dominioX.it?

3) [5 punti] A cosa servono gli indirizzi di Broadcast a livello MAC e livello Rete? Non basterebbe disporre dell'indirizzo di Broadcast solo a livello MAC o solo a livello Rete?

4) [15 punti] Alice deve spedire separatamente un messaggio m1 (breve) a Bob e un messaggio m2 (breve) a Charlie in modo che sia Bob che Charlie possano leggere m1 e m2, e poi vadano a scambiare tra loro i due messaggi m1 e m2, ma con le garanzie di confidenzialita' (trudy non legge m1 e m2), garanzia del mittente (Bob e Charlie sono certi che il messaggio proviene da Alice), integrita' (m1 e m2), garanzia del mittente (Bob e Charlie sono certi che il messaggio proviene da Alice), integrita' (m1 e m2 non sono stati modificati rispetto a queanto spedito da Alice). In che modo l'attaccante (Trudy) puo' ancora attaccare la comunicazione tra Alice e Bob? Spiegare.

   - Uso chiave pubblica e privata in quanto i messaggi sono brevi entrambi.
   - A chiede alla CA la chiave pubblica di B e C (`Kb+` e `Kc-`) per evitare man in the middle
   - A spedisce `Kb+(m1, Ka-(H(m1)))` -> solo Bob possiete `Kb-` e apre `m1`, poi con `KA+` (chiesto alla CA) apre `H(m1)` e verifica che `H(m1)` ricevuto da A sia uguale a `H()` calcolato su `m1` ricevuto nel messaggio
   - A spedisce `Kc+(m2, Ka-(H(m2)))` -> solo Charlie possiete `Kc-` e apre `m2`, poi con `KA+` (chiesto alla CA) apre `H(m2)` e verifica che `H(m2)` ricevuto da A sia uguale a `H()` calcolato su `m2` ricevuto nel messaggio
   - Ora avviene lo scambio di messaggi tra Bob e Charlie
   - Bob spedisce a Charlie `Kc+(m1, Ka-(H(m1)))` -> Solo Charlie possiede `Kc-` e apre la busta, scopre `m1` e verifica che `m1` provenga da Alice grazie a `Ka+`, e verifica l'integrita' di `m1` grazie a `H()`
   - Charlie spedisce a Bob `Kb+(m2, Ka-(H(m2)))` -> Solo Bob possiede `Kb-` e apre la busta, scopre `m2` e verifica che `m2` provenga da Alice grazie a `Ka+`, e verifica l'integrita' di `m2` grazie a `H()`
   - Trudy puo' ancora attaccare tramite attacco DOS o Replay, e per risolverlo servirebbero rispettivamente "i militari" e il nonce

5) [10 punti] Le seguenti quattro regole di tabella OpenFlow che tipo di gestione di traffico di rete SDN locale implementano sul router sul quale sono

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	100.2.3.4	*	*	*	80	drop
*	*	*	*	12	*	100.2.3.5	*	*	25	port3
*	*	*	*	*	100.2.3.6	100.2.3.7	*	3918	4233	drop
*	*	FF:FF:FF:FF:FF:FF	*	*	*	*	*	*	*	port5

programmate?

1) Blocca tutti i pacchetti provenienti da IPv4 `100.2.3.4` e indirizzati a porta 80 (web server)
2) Manda su porta 3 (fisica) i pacchetti su VLAN 12 se destinati a IPv4 `100.2.3.4` e SMTP server (port 25)
3) Blocca tutti i pacchetti da socket `<100.2.3.6, 3918>` a socket `<100.2.3.7, 4233>`
4) Manda su porta fisica 5 tutti i broadcast di livello MAC sul segmento locale

6) [10 punti] Se un canale radio OFDM ha 18 sub-carrier e un symbol lrate di 500.000 simboli/sec quanti simboli della codifica digitale PSK deve adottare per riuscire a trasferire un file da 54 Mbit in non piu' di 4 secondi, massimizzando la resistenza all'errore di canale? Quanto tempo impiegherebbe esattamente a completare il trasferimento? (trascurare tutti gli overhead e gli errori di transmissione)

   - prestazione canale = 18 * 500.000 symbols/sec = 9.000.000 symbols/sec
   - requisito: 54 Mbit/s / 4 = 13.500.000 bit/s (bitrate minimo nominale del canale)
   - Si evince che serve almento una QPSK (una BPSK non basterebbe a soddisfare il requisito)
   - QPSK definisce una prestazione di canale pari a 9.000.000 symbols/s * 2 bit/symbols = 18.000.000
   - Il tempo necessario per completare il trasferimento e' pari a 54.000.000 / 18.000.000 = 3 secondi

7) [5 punti] Che cosa sono le fasi di Slow Start e Congestion Avoidance del protocollo TCP e a cosa servono?

8) [10 punti] Quali dovrebbero essere gli indirizzi IPv4 di Bradcast del router (con ultimo indirizzo IP valido) della rete che contiene l'host `54.205.211.33` se la maschera di rete fosse `255.248.0.0`? E se la

maschera di rete fosse /21?

- Netmask /13:
  - `255.248.0.0` = `11111111.11111 000.00000000.00000000`
  - `54.205.211.33` = `00110110.11001 101.11010011.00100001`
  -
  - Rete: `00110110.11001 000.00000000.00000000` = `54.200.0.0/13`
  - Router: `00110110.11001 111.11111111.11111111` = `54.207.255.254/13`
  - Broadcast: `00110110.11001 111.11111111.11111110` = `54.207.255.255/13`
- Netmask /21:
  - `255.255.248.0` = `11111111.11111111.11111000.00000000`
  - `54.205.211.33` = `00110110.11001101.11010 011.00100001`

9) [25 punti] Esercizio di programmazione di rete

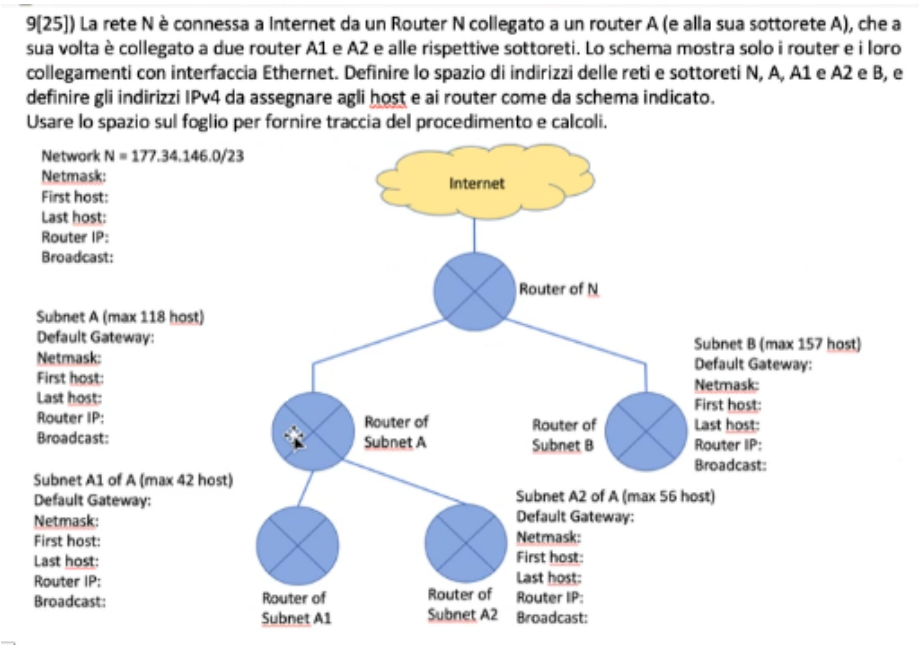

Figure 1: Disegno

10) [10 punti] Un sistema di comunicazione wireless ha un dispositivo ricevente R in grado di garantire le seguenti prestazioni:

Bitrate nominale possibile	se in presenza di Link Budget minimo
1 Mbps	5 dB
2 Mbps	8 dB

Bitrate nominale possibile	se in presenza di Link Budget minimo
4 Mbps	14 dB
8 Mbps	20 dB
16 Mbps	26 dB
32 Mbps	32 dB
64 Mbps	38 dB

1) Assumendo che l'Intentional radiator del trasmettitore T fornisca la potenza di segnale Ptx = 25mW a un'antenna con guadagno di 8 dBi e che il ricevitore abbla un'antenna omnidirezionale con guadagno di 3 dBi, e che il path loss dovuto alla distanza di un miglio sia pari a -80 dB, a quale velocità avviene la comunicazione se la Receiver Sensitivity di R è pari a -75 dBm?
   - Ptx = 25 mW Converto in dBm: `(1 mW == 0 dBm) <=> (1*10*10/2/2 == 0+10+10-3-3) <=> 25 mW == 14 dBm`
   - `+8 dBi`
   - `+3 dBi`
   - `-80 dB`
   - Link Budget = `(14 + 8 + 3 - 80) - (- 75) = - 55 + 75 = +20 dBm`
   - Quindi abbiamo la situazione: 8 Mbps (20 dB)
2) E se la distanza tra T e R si riducesse a 1/3 di miglio?
   - Se la differenza tra T e R si riduce di 1/3 di miglio (1/3 del valore precedente) significa che il link budget si modifica come segue: per la regola dei 6 dB ogni volta che dimezzo la distanza tra T e R aumento di 6 dB il link budget. Quindi i `-80 dB` di Loss a distanza 1/2 diventano `-74 dB` e il link budget diventa `+26 dBm`
   - Di conseguenza se dimezzo di nuovo a distanza 1/4 di miglio il Loss diventa `-68 dB` e il link budget diventa `+32 dBm`
   - Essendo ad 1/3 mi trovo a meta' tra 1/2 e 1/4, quindi il link budget sara' compreso tra `+26 dBm` e `+32 dBm` esclusi, quindi posso prendere il livello con `+26 dBm` con velocita' 16 Mbps