Ripasso di reti di calcolatori (esempio di esercizi) del 19 maggio 2023

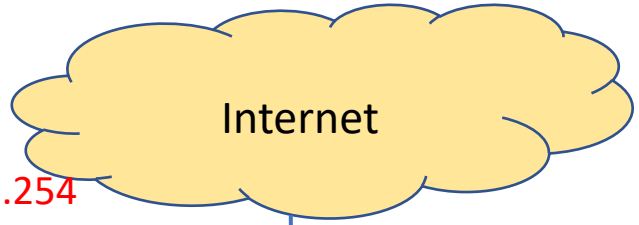
es. 1: quale è l'indirizzo di rete (e sottorete) e il router dell'host A : 97.14.18.27 / 11 ?
/11 : 255.224.0.0
97 ci dice che si tratta di un indirizzo IPv4 di classe A, quindi si tratta della rete 97.
Tuttavia abbiamo delle sottoreti. Il valore 224 indica 11100000 e quindi aggiunge 3 bit della sottorete, quindi 2^3 = 8 sottoreti)
il valore 14 si esprime in binario come 00001110, quindi il valore della sottorete è 000. La parte verde è l'host. La parte rossa è rete e sottorete.
Quindi, l'host 97.14.18.27 /11 appartiene alla rete e sottorete 97.0.0.0 / 11
Il router della rete e sottorete sarà quindi: (ultimo host prima del broadcast della rete/sottorete)
97.00011111.11111111.11111110 = 97.31.255.254 (indirizzo del router)

es. 2: quale deve essere la maschera di rete comune perchè l'host A e B: 97.18.11.127 appartengano alla stessa sottorete?

Per appartenere alla stessa rete e sottorete occorre che A e B abbiano indirizzo di rete e sottorete uguale.
La rete di classe A di entrambi A e B 97 è la stessa. Dobbiamo imporre che anche la sottorete sia la stessa.
host A : 97.14.18.27 = 97. 00001110 . ----------
host B : 97.18.11.127 = 97. 00010010 . ----------
La parte in comune della stessa subnet è data dagli stessi 3 bit della sottorete ottenuta con /11.
La maschera di rete richiesta è quindi /11 = 255.224.0.0

es. 3:

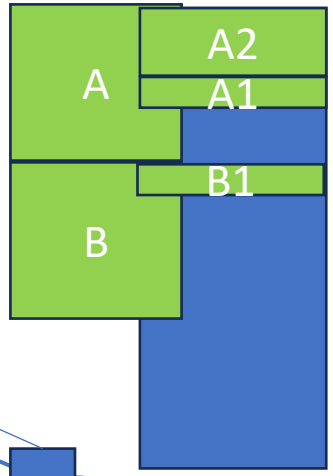
Network N che contiene host 128.129.127.0/23
Rete = 128.129.126.0/23
Router IP: 128.129.01111111.11111110 = 128.129.127.254
Netmask: /23 = 255.255.254.0
First host: 128.129.01111110.00000001 = 128.129.126.1
Last host: 128.129.01111111.11111101 = 128.128.127.253
Bcast: 128.129.01111111.11111111 = 128.129.127.255



N (512 host massimi)

Subnet A (max **120** host)
Default Gateway del router di A: 128.129.127.254
Router IP di A:128.129.126.126 (01111110)
Netmask: 255.255.255.128 (/25)
First host:128.129.126.1 (00000001)
Last Host: 128.129.126.125 (01111101)
bcast: 128.129.126.127 (01111111)

Subnet A



Subnet B (max **111** host)
Default Gateway del router di B :128.129.127.254
Router IP di B: 128.129.126.254 (11111110)
Netmask:255.255.255.128 (/25)
First host:128.129.126.129 (10000001)
Last host: 128.129.126.253 (11111101)
Bcast: 128.129.126.255 (11111111)

Subnet B

Subnet A1 of A (max **12** host)
Default Gateway del router di A1: 128.129.126.126 (01111110)
Router IP: 128.12.9.126.46 (00101110)
Netmask:/28 = 255.255.255.240
First host: 128.129.126.33 (00100001)
Last host: 128.12.9.126.45 (00101101)
bcast: 128.12.9.126.47 (00101111)

Subnet A1

Subnet A2 of A (max **27** host)
Default Gateway del router di A2: 128.129.126.126 (01111110)
Router IP: 128.12.9.126.30 (00011110)
Netmask:/27 = 255.255.255.224
First host: 128.129.126.1 (00000001)
Last host: 128.12.9.126.29 (00011101)
bcast: 128.129.126.31 (00011111)

Subnet A2

Subnet B1 of B (max **16** host) -> <u>32 host necessari!</u>
Default Gateway:128.129.126.254 (11111110)
Router IP: 128.129.126.158 (10011110)
Netmask: /27 (255.255.255.224)
First host: 128.129.126.129 (10000001)
Last host: 128.129.126.157 (10011101)
bcast: 128.129.126.159 (10011111)

Subnet B1

es. 4: Alice vuole spedire a Bob un messaggio M molto lungo con garanzia di Non replay e privacy
Non replay: NONCE (B manda a A un numero «once in a lifetime», es. 36 e A lo include nel msg.
per la privacy serve crittografia di M, ma quale? chiave pubblica/privata (RSA) o simmetrica (AES)?
Essendo M lungo, meglio cifrare con AES (simmetrica), quindi ad A serve generare e condividere Ks. Per condividere Ks devo usare RSA.

A ← nonce (36) B
A genera Ks e (KB+ ottenuta da CA) KB+(Ks) -> B ottiene Ks = KB-(KB+(Ks))
A spedisce Ks (M, 36) -> B ottiene Ks(M,36) = M, 36, e verifica che nonce = 36.

es. 5: e se volessimo aggiungere la garanzia di non ripudiabilità del mittente (firma digitale)?

Alice deve garantire la sua Id digitale e deve firmare il messaggio M e anche il trasf del Ks. Firmando i messaggi.
Si usa KA- (RSA).
A spedisce KA-(KB+(Ks)) -> B riceve e decripta KA+ (ottenuta da CA) KA+(KA-(KB+(Ks)) = KB+(Ks), e KB-(KB+(Ks)) = Ks
A spedisce Ks (M, 36) -> B ottiene Ks(M,36) = M, 36, e verifica che nonce = 36.

NB: se non avessi chiesto la privacy ma solo integrità: A genera H(M) e poi -> KA-(H(M)), M) -> e B calcola KA+(KA-(..) = H(M) e M

es. 6: e se il messaggio m fosse molto breve?
A ← nonce (36) B
In questo caso posso usare direttamente RSA per cifrare m piccolo.
Quindi
A ottiene KB+ da CA e genera KB+(m, 36) -> B ottiene m = KB-(KB+(m))
se serve anche garanzia mittente e firma digitale
A spedisce KA-(KB+(m,36)) ->>>>. B ottiene KA+ (da CA) e calcola KA+(KA-((KB+(m,36))) = (KB+(m,36)) e poi KB-((KB+(m,36)) = m, 36

es. 7: Se uso una OFDM da 40 subcarrier con QPSK con 1000 simboli al secondo, a quanto ammonta il bitrate nominale del canale?

40 subcarrier x 1000 simboli/s e 1 simbolo codifica 2 bit (QPSK ha 4 simboli, quindi Log_2(4) = 2).
Quindi il bitrate nominale sarà 40x1000x2 = 80Kbps (80 kilo bit al secondo).

es. 8: a quale distanza massima posso ricevere una comunicazione wireless se il link budget a 200 metri è di 8 dB?
se il link budget è 8 dB significa che il segnale che raggiunge il ricevente a 200 m è superiore di 8 dB al receiver sensitivity (RS) minimo per avere un link di comunicazione.
Se non possiamo rinunciare al Fade Operating Margin allora siamo già al di sotto del limite minimo di 10 dB e non possiamo aumentare la distanza.
Se possiamo rinunciare completamente (ciò rende il canale a rischio) allora possiamo arrivare vicino al limite > 0dB.
A 200 m abbiamo 8dB. La regola dei 6 dB (6 dB rule) dice che ogni volta che perdo 6 dB di segnale equivale a raddoppiare la distanza tra sender e receiver. Quindi avendo un margine di 8 dB posso rinunciare a 6 e raddoppiare a 400 m di distanza rimanendo con 2 dB di margine. Non posso raddoppiare fino a 800. Quindi la distanza massima sarà di poco superiore a 400 m e di certo inferiore a 800.

es. 9: e se usassi un'antenna con un guadagno di 3 dBi sia sul trasmittente che sul ricevente?
In questo caso il link budget guadagnerebbe 3+3 dBi (3 sul tx e 3 sul rx) = 6 dBi.
Quindi il link budget diventerebbe di 8+6 = 14 dB.
Quindi da 200 m posso salire a 400 rimanendo con 8 dB (14-6 = 8) e di nuovo a 800 m rimanendo a 2 dB (8-6 = 2)
Quindi riuscirei a aumentare la distanza di trasmissione fino a oltre 800 m.

es. 10: Se ho un router R con link di uscita a 100 MB/s, sul quale entrano K flussi ognuno da Y pacchetti/s, quale deve essere il limite massimo D di dimensione media dei pacchetti (in bit) per evitare la congestione?

100 MB/s = 800 Mbps

Il carico totale del router R si può esprimere come Cr= K*Y pacchetti/s

Per evitare congestione occorre garantire (L*a)/R < 1, tradotto Cr / capacità link di uscita sia < 1.

Quindi K*Y*D (numero total di bit in ingresso al router R) sia inferiore alla capacità del link di uscita 800 Mbps.

KYD < 800.000.000, quindi D < (800.000.000 / KY), (KY è positivo, quindi non cambia segno la disequazione).

D < (800.000.000 / KY) per non avere congestione.

es. 11: e se il router avesse un buffer da 50 MB?

Il buffer può tollerare degli «sforamenti» di ritmo di ingresso fino al suo limite, ma non può agire all'infinito in quanto è un buffer finito.

Quindi l'esistenza di un buffer arbitrariamente grande, ma finito, significa solo che prima o poi (più poi che prima) raggiungerò comunque la congestione.

Se vogliamo possiamo capire per quanto tempo reggerà il router senza perdere i pacchetti in questo modo:

se 50 MB = 400 Mb,

400 Mbit / (KYD – 800.000.000) è il numero di secondi di «resistenza» del buffer del router nel memorizzare i dati in eccesso rispetto a quelli smaltiti.

es. 12: quale è il valore EIRP di un intentional radiator (IR) che fornisce 2W di segnale a un antenna direzionale con guadagno di 18 dBi?

2000 mW sono forniti all'antenna. L'antenna ha guadagno 18 dBi (concentra energia 18 dB rispetto a isotropico).

Il valore EIRP (equivalente all'energia da fornire a antenna isotropica per avere stessa emissione radio) si ottiene dando all'antenna isotropica 18 dB di segnale in più. Quindi 2000 mW equivalgono a 1 mW = d dBm, ma 2000 = 1*10*10*10*2 che nella scala dB equivale a 0 dBm + 10 + 10 + 10 + 3 = 33 dBm.

Quindi l'EIRP dell'IR all'antenna isotropica sarà di 33 dBm + 18 dBi = 51 dBm = 1 mW * 2^17 = 2^17 mW = circa 128 W.

e se il limite EIRP fosse di 40 mW a quanto dovrebbe limitarsi il segnale IR in tale sistema?

Il limite equivale ad avere un max di 40 mW dati a un isotropica (con 0 dBi). Invece noi abbiamo una direzionale con +18 dBi. Di conseguenza, per stare nel limite dovremo ridurre di 18 dBi il segnale dell'IR dato all'antenna rispetto al limite EIRP di 40 mW.

40 mW = 1 *2 *2 *10 mW ⇔ 0 dBm +3+3+10 = 16 dBm (questo è il limite EIRP espresso in dB).

Non possiamo dare più di 16 dBm a un isotropico. Se l'antenna guadagna già da sola 18 dBi, significa che il max segnale dell'IR all'antenna non potrà superare i 16 – 18 = -2 dBm. Quindi la potenza massima da fornire all'antenna sarà di 0 dBm + 10 -3 -3 -3 -3 (= -2) che equivale a 1 mW * 10 / 2 /2 / 2/ 2 = 0,675 mW