



Tentativo di trovare un link fra le domande di reti

- modulazione OFDM
- IP unicast
- payload pacchetto IPv4
- differenze Pings e traceroute
- send/sendto() o socket bloccante e non
- TIME\_WAIT in TCP, perché?
- es routing
  - relazione max bit/s di mezzo trasmissivo e la sua latenza
  - bitrate e bandrate di canale link ADSL cod QAM 16 o 20 mb/s
  - Collisione = broadcast in eth?
  - situazioni IEEE 802.1 o .2 gestiscono mac. spedizione frame?
  - domande su switch e telefonia, ritardo filter ecc.
- Source routing IP
- ICMPv6 VS ICMPv4
- Timer principali TCP
  - raggi infrarossi
  - Piggybacking
  - problema frame fatale
  - risoluzione inversa DNS
- ALOHA
- elg backoff
  - qualità IPv6
  - RTO in TCP. elg backoff Korn
  - schema pacchetti SRTP
  - capacità max (bps) canale e segnale/rumore
  - esadecimale
  - bit-stuffing
  - congestione, SACK
  - JPEG - campi MIME
  - elg generazione chiavi RSA / chiave pub e cert x.509
  - QAM
- backoff  $\rightarrow$  CSMA
  - maximum size segment
  - IPv6
  - differenze tra CSMA/1 e CSMA/1
  - intradonneau ATM

esercizio

- network, routing IP, reti
- diagrammi spazio tempo
- routing

# PROVE ANNI PASSATI:

19/12/2013

1) tecnica modulazione QAM: cosa coeviste e che impieghi lì?

E' una modulazione sia di ampiezza che di fase. E' impiegata principalmente nelle reti di sistemi telefonici e nella telefonia in generale. Ha un diagramma chiamato "a costellazione" e ha diverse variazioni come la QAM16 e QAM32. Vedi reti wireless.

2) Cosa è e quando viene usato l'algoritmo di backoff nei protocolli CSMA?

Dovranno implementare ethernet.

In CSMA un algoritmo di backoff serve per calcolare tempo di attesa in caso di collisioni rilevate ( $n$ ) fra terminali. In ethernet dopo  $n$  collisioni rilevate fa partire un tempo di attesa prima di ritrasmettere il dato. Il tempo è  $\max(10 \text{ slot}, \text{formula } 0 - 2^n - 1 \text{ slot})$ . Si chiama esponenziale binario.

3) Un router deve annunciare che gli indirizzi da 10.10.0.0 a 10.10.50.255 e da 10.10.64.0 a 10.10.127.255 sono raggiungibili tramite interfaccia 1.

Gli indirizzi tra 10.10.60.0 e 10.10.63.255 raggiungibili interfaccia 2.

Aggregare usando minor numero di reti.

1)  $10.10.0.0 \rightarrow 10.10.50.255$        $2^{\text{host}} = 32 - 1 = 21 \rightarrow 10.10.0.0/21$   
 $\dots \rightarrow 00110010.111111$

2)  $10.10.64.0 \rightarrow 10.10.127.255$

$\dots /01000000.00000000 \rightarrow \dots /01111111.1111111$        $2^{\text{host}} = 32 - 15 = 17 \rightarrow 10.10.64.0/17$

3)  $10.10.60.0 \rightarrow 10.10.63.255$

$\dots /0011100. \dots \rightarrow 0011111.111111$        $2^{\text{host}} = 32 - 10 = 22 \rightarrow 10.10.60.0/22$

4)  $10.10.0.0 \rightarrow 10.10.127.255$

$\dots /0101111.1111111$        $2^{\text{host}} = 32 - 15 = 17 \rightarrow 10.10.0.0/17$

indirizzi 1° contenuti in 2  
interfaccia 1: un host sceglie 2° perché netmask più lungo

interfaccia 2

$10.10.0.0/17$

4) Cosa è e come viene determinato MSS di uno in TCP?

L'MSS ottimale è l'MTU minimo fra tutti gli MTU incontrati nel tracitto. Non c'è modo a inizio trasmissione e potrebbe variare nel tempo.

5) Schema possibile pacchetto IPv6 con intestazioni estese:



IPv6 header      ext header      dati

Nelle trame IPv6 vengono opposte intestazioni trovate campo next header dove si inserisce un numero che corrisponde al codice delle opzioni. Opzioni principali →

- info per router attraversati      Hop-by-Hop
- liste router da visitare ordine stabilito routing header
- fragmentation option
- ESP      AH      Dest. option      ICMPv4 - ICMPv6      TCP - UDP

6) Il client 172.28.64.100 (IP privato) effettua una query iterativa al DNS server di default 160.78.48.10 per conoscere l'indirizzo dell'host www.kernel.org. Disegnare lo schema con tutti i server coinvolti e i messaggi scambiati. Per ogni messaggio indicare le principali info contenute nei pacchetti DNS (question, answer, authorities).

No!!!

26/2/2015

1) In cosa consiste la modulazione OFDM? quali tecnologie per le trasmissioni detti lo utilizzano?

La OFDM è un caso speciale di mod FDM, che divide lo spettro in bande di sequenze. La OFDM fa lo stesso caso ma le frequenze sono ortogonalib fra di loro. Viene usata per esempio in ADSL o fibra ottica ma anche in wireless 3G/4G/LTE e WiMax.

2) Cosa sono e a cosa servono gli indirizzi IP anycast?

Gli IP anycast sono metodi di routing per cui una singola destinazione ha più routing paths o due o più end points. Viene spesso usata per la distribuzione di movie di contenuto (CDN).

3) In linea teorica quale è la max e min dim per un payload in IPv4? In pratica come viene determinata?

La dimensione minima di un payload in IPv4 è di 20 bytes mentre la massima è di 64 kb.

4) piag vs traceroute. Entrambi passano attraverso liste router ma usano tecniche diverse. descrivere e descrivere i modi che conoscete per tracciare i router attraverso

Il comando ping spedisce dei pacchetti al destinatario, i quali attraversano i vari router, ma il suo ruolo primario non è contare gli hops, bensì verificare se un host è raggiungibile. Il comando traceroute invece conta gli hops, attraversando i vari router per poi comunicarlo all'host. E' anche il suo ruolo primario.

5) Differenze di chiavette ed une primitive di output nel caso di socket bloccante e non.

La send() è per default bloccante. Si blocca quando il buffer è pieno e ritorna quando si libera spazio sufficiente. Se il socket è impostato come non bloccante ed il buffer è pieno, ritorna -1 e l'errore EINVAL

6) In quale fase TCP l'host entra in TIME\_WAIT? A che serve?

Il TIME\_WAIT arriva dopo le chiamate di close() per chiudere la connessione. Per garantire no errori durante la chiusura dopo il close dell'host (che entra in TIME\_WAIT) ospello il FIN del server per poi mandare ACK+RST e chiudere

7) 2 switch A / B con supporto VLAN. Host 1 invia broadcast.

- 1) in che modo 802.1Q consente di gestire la VLAN?
- 2) chi ripristina interazione modificata?
- 3) host 3 riceve e scatta o non riceve?
- 4) frame da 1 a 4 ha interazione eth std o mac?



1) l'802.1Q consente di configurare dest addr, source addr, vlan pri, tag, length, type, pid e check sum di frame eth.

Lo VLAN può essere configurato con gli switch modificando le porte delle VLAN.

2) Non ne ho idea 4) Neanche

3) l'host 3 riceve il frame ma lo scatta.

8) Un router deve creare le tabelle di routing per le seguenti dest:

10.0.0.0	$\rightarrow$	10.0.0.0.127	$\rightarrow$	if 1	1
10.0.0.128	$\rightarrow$	10.0.0.0.159	$\rightarrow$	if 2	2
10.0.0.160	$\rightarrow$	10.0.0.0.175	$\rightarrow$	if 1	3
10.0.0.192	$\rightarrow$	10.0.0.0.255	$\rightarrow$	if 2	4

1) 0000 0000  $\rightarrow$  01111111 7 bit combinano 2<sup>7</sup> host  $32-7 \rightarrow 25 \rightarrow 10.0.0.0/25$  if 1

2) 1000 0000  $\rightarrow$  10011111 5 bit  $\rightarrow$  2<sup>5</sup> host  $32-5 \rightarrow 27 \rightarrow 10.0.0.128/27$  if 2

3) 1010 0000  $\rightarrow$  1010 1111 4 bit  $\rightarrow$  2<sup>4</sup> host  $32-4 \rightarrow 26 \rightarrow 10.0.0.160/26$  if 1

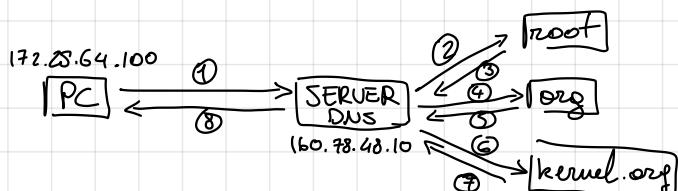
4) 1100 0000  $\rightarrow$  1111 1111 8 bit  $\rightarrow$  2<sup>8</sup> host  $32-8 \rightarrow 24 \rightarrow 10.0.0.192/24$  if 2

Per supernetting

supernet mask	New NID	32-8 = 24
10.0.0.0/25	255.255.255.0	10.0.0.0.0000 0000 if 1
10.0.0.128/27	255.255.255.0	10.0.0.1000 0000 if 2
10.0.0.160/26	255.255.255.0	10.0.0.1100 0000 if 1 NID = if 2 $\rightarrow 10.0.0.0/25$
10.0.0.192/24	255.255.255.0	10.0.0.1110 0000 if 2 router sceglierà if 2
supernet mask		10.0.0.0
255.255.255.0		

Esempio: il client 172.28.64.100 (privato) effettua una query iterative al DNS di default 160.78.48.10 per conoscere l'IPV4 dell'host www.kernel.org.

Disegnare lo schema con i server coinvolti e i messaggi scambiati. Indicare le info dei pacchetti.



1,2,4,6 mandano solo la richiesta Q  
3,5 sono le autorities Auth  
7,8 sono le risposte Answe

# Domande del primo appello:

20/1/20

1) Indicare i parametri che concorrono a quantificare bit-rate linea ADSL

Si utilizzano per quantificare il bitrate la velocità di trasmissione e la quantità di dati da trasportare  $\rightarrow T = \frac{S \cdot t}{n \cdot m \cdot b}$

Altrimenti si possono usare il teorema di Nyquist o quello di Shannon

$N = 2B \log_2 M$  (bit/s) con  $B$  lunghezza banda,  $M$  valori distinti che può assumere ogni simbolo trasmesso

$$S = B \cdot \log_2 \left( 1 + \frac{S}{N} \right) \text{ (bit/s)} \quad S = \text{potenza canale} \quad N = \text{disturbo}$$

2) Come si comporta il protocollo eth se il trasmettente deve trasmettere per la prima volta un frame ma trova il canale occupato?

Se il trasmettente trova il canale occupato aspetta fino a quando la linea diventa inattiva e poi trasmette immediatamente (csma/ca -1 persistente)

3) Nel protocollo TCP quali dati sono contenuti nel buffer del mittente? Quelli dinamici ne modificano il contenuto?

Sono contenuti dati spediti non ancora riscontrati, dati ancora da spedire e spazio libero. Può modificare il contenuto un ACK, che elimina dati non riscontrati (perché vengono riscontrati), dati spediti e rimossi dal buffer o dati aggiunti per spedire.

6) Cosa è un DNS forwarder? Come gestisce una richiesta iterative?

Un DNS forwarder differisce dal DNS normale perché risolve le query non direttamente ma interrogando un server ricorsivo.

A una richiesta iterativa il client invia una query al Local Name Server, che verifica se il nome può essere convertito, rispondendo al client con l'IP nel caso, altrimenti si limita a comunicargli il nome del server che secondo lui può farlo, la procedura si ripete verso il nuovo server.

7) In quali messaggi di una richiesta HTTP viene utilizzato il corpo (body) dopo l'intestaz.? Cosa contiene?

Il campo body in una richiesta HTTP può contenere un POST, che si utilizza quando si vogliono mandare al server molte informazioni, senza un limite sulla quantità e tipo di dati che si vogliono trasmettere, in modo non visibile all'URL.

8) openssl rsautl -sign -inkey rsa-key.pem -in text.txt -out signed.txt

In openssl rsautl può firmare, verificare, crittare e decrittare dati.

Così -sign si vuole firmare il txt in input con -in che genera il txt in -out firmato e -sign prende come chiave (-inkey) la chiave rsa-key.pem per svolgere l'operazione.

9) Come funziona un DDoS con amplificazione come per esempio NTP reflection?

Nel NTP reflection l'attaccante esplora Network time protocol server ed accesso pubblico per intasare il bersaglio con traffico UDP. L'NTP è un protocollo vecchio che sincronizza gli orologi dei computer in rete.

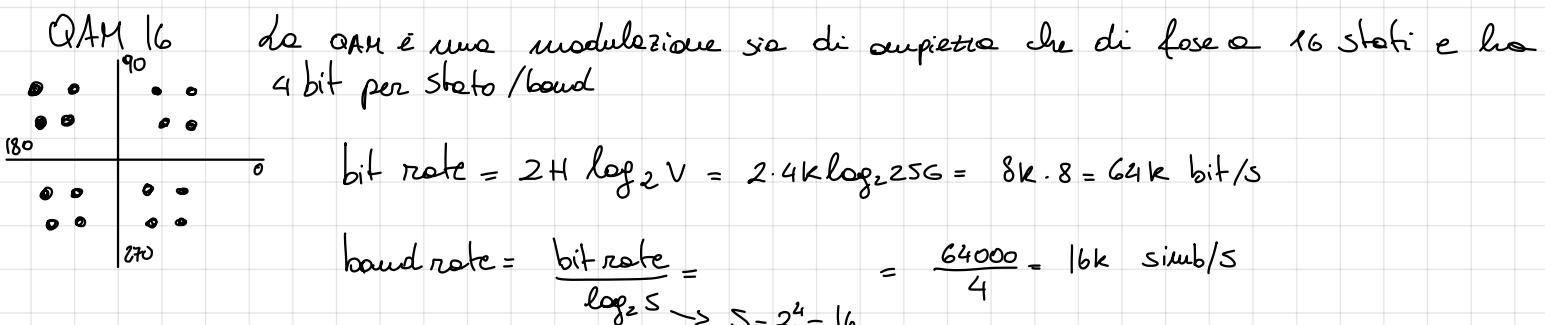
Un DDoS è come un DOS ma utilizza molteplici macchine infettate per amplificare le potenze dell'attacco.

29/1/2015 ——

1) Quale è la relazione fra max r. (bit/s) di un mezzo trasmissivo e la sua lunghezza?

Max rango che la lunghezza del mezzo determina la velocità massima ottenibile per via dell'annuncio del rumore. Per calcolare la velocità ci sono due modi:  $H \log_2(1 + S/N)$

2) Un link ADSL in cui i canali sono codificati in QAM 16 può trasmettere a 20 mb/s. Determinare bit-rate e band-rate



3) Per quali operati eth il dominio di collisione coincide con il dominio broadcast?

Non esistono operatori di rete il cui dominio di collisione coincide con il dom. broadcast

4) Esistono situazioni in cui gli standard IEEE 802.3 e 802.11 gestiscono in modo diverso i meccanismi di priorità nella spedizione dei frame?

No

5) Si consideri un flusso di pacchetti da host A a host B attraverso switch cut-through e uno switch store and forward in doppio telefonico. Cosa può incidere su filter, throughput, affidabilità, ritardo in caso di 1) rete scarsa e 2) vicina alla congestione?

↓

A → switch → R → switch → B

	throughput	off. isol.	ret.	gett.
A	Max	Max	Min	Min
B	Min	Min	Max	Max

6) Cosa è / cosa serve il source routing in IP? Come funziona?

S'intende una lista di router da percorrere per arrivare a destinazione. Il mittente ottiene le informazioni tramite meccanismi di route location oppure tramite richieste ad un intermedio system e le inserisce nel campo options delle trame IP.

Si usa quando ci sono problemi di intrasistemi.

7) IPv4 VS IPv6 !?

IPv4 e IPv6 sono fondamentalmente uguali, ma IPv6 aggiunge delle novità:

- path MTU discovery → per ottenere MTU ottimale
- neighbor discovery → sostituisce ARP per determinare l'indirizzo LAN.
- router discovery → quando un host entra in link manda un "router solicitation" in multicast e ogni risponde con un "router advertisement" che contiene l'indirizzo + other stuff necessarie per il routing.

8) Elencare i timer più usati in TCP

I timer TCP sono:

1 timer di persistenza → attivato quando la finestra di ricezione viene chiusa. Se il pacchetto che riapre viene perso, quando scade il mittente invia una secca.

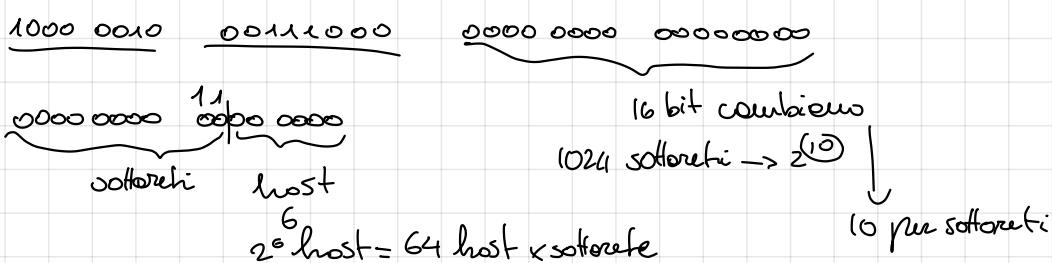
2 timer wait → prima di rilasciare le connessioni, per gestire pacch. ancora in transito.

3 timer di keepalive → attivato quando la linea è inattiva. A zero il TCP manda ACER e se non torna risposta → connessione chiusa

4 RTO → per decidere quando un pacchetto va considerato perduto. Questo valore deve essere pari almeno al RTT ma deve aggiornarsi dinamicamente e gestire situaz. di congestione

9) blocco IP 130.56.0.0/16 → voglio 1024 sottoreti con subnet mask fissa.

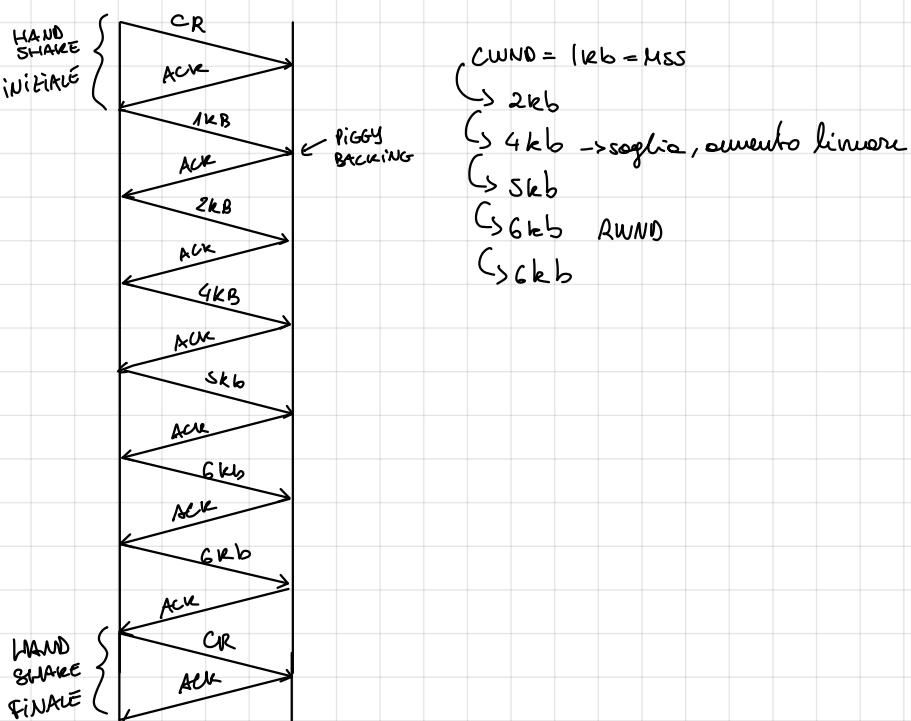
- subnet mask
- n host × sottorete
- indirizzo rete e broadcast × 1° e ultimo sottoret



maschere sottorete  $\rightarrow$  255.255.255.192  
 $\downarrow$   
 11000000  
 6 cambiare

indirizzo broadcast 1° 130.56.0.127  
 2° 130.56.255.255

10) Diagramma spazio tempo TCP - file 24 kB slow start 4 kB MSS = 1 kB  
 RWND = 6 kB



27/2/2014 — |

1) I raggi infrarossi funzionano a breve distanza, ma sono disturbati dalla luce solare. Sono molto sicuri perché non sono intercettabili, ma sono dirizzabili e non possono superare ostacoli. Vengono usati per la costruzione di telecomandi e impulsi in fibra ottica.

2) I due campi del piggybacking sono: 1) options e 2) bitcode.

Se modifico il primo con parametro sack verrà usato il Selective Ack anziché il go-back-n.

Se modifico il secondo con flag SYN viene indicato al suo interno il sack permitted per indicare le capacità di gestire lo sack.

3) Descrivere la finestra futile (silly window syndrome) di TCP e come ottenerlo.

È un problema di prestazioni, che accade quando il mittente perde dati lentamente o quando il ricevente consuma dati lentamente. Le possibili soluzioni per ottenere il problema possono essere: Alg. di Nagle per il mittente o alg. di Clark per il ricevente.

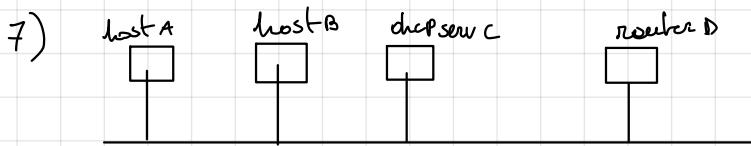
4) Cosa è e come funziona la risoluzione inversa dei nomi in una infrastruttura DNS?

La risoluzione inversa dei nomi in DNS è una tecnica che converte l'IP al nome del dominio. Serve per identificare un host e per leggere il risultato di un browser.

Consiste nell'invio dell'IP dell'host e viene richiesto al DNS nell'ordine inverso dei byte es: IP 1.2.3.4 → nome host ottengo richiedendo al DNS 4.3.2.1

$$6) \quad T = L/\text{bit-rate} \quad 200/200 \cdot 10^3 = 1 \mu\text{s}$$

$$G = \frac{1 \mu\text{s} \cdot 1000}{1 \text{s}} = \frac{10^{-3} \cdot 10^3}{1} = 1 \quad G = 1 \text{s} \quad \text{Throughput} = S = Ge^{-2G} = 1 \cdot e^{-2} = 0,13 \text{ kbps} \times \text{distanza puro}$$



1. host A Arp req. broadcast con IP<sub>B</sub>
  2. host B arp replay unicast
  3. host A ICMP MAC<sub>B</sub> MAC<sub>A</sub> IP<sub>B</sub> IP<sub>A</sub> => ping
  4. host B ICMP MAC<sub>A</sub> MAC<sub>B</sub> IP<sub>A</sub> IP<sub>B</sub> => risposta ping
- }] Liv 3

30/1/2014

- 1) In una rete locale 1-persistente con backoff esp. le stazioni A, B, C hanno dati da trasmettere. A ha già avuto 2 collisioni, B inizia ora, C 1 collisione. Quale è la prob. di collisione al prossimo tentativo?

La probabilità di collisione è bassa (molto) perché essendoci già state 3 collisioni totali l'alg. di backoff è già stato eseguito ed il prossimo tentativo sarà una volta finito il timer, che volge proprio a evitare altre collisioni.

- 2) Discutere le qualità del servizio fornito in IPv6

IPv6 permette future evoluzioni. Offre meccanismi di sicurezza e ottima qualità di servizio. Gestisce miliardi di host semplificando il routing. Consente la mobilità e garantisce retrocompatibilità.

- 3) A che serve l'RTO in TCP? Quando e come interviene l'algoritmo di backoff di Kern?

L'RTO in TCP serve per decidere quando un pacchetto è da considerarsi perduto. Deve essere almeno uguale al RTT ma aggiornarsi di nuovi eventi e gestire situazioni di congestione. Se RTO scade, significa che la rete è congestionata e l'algoritmo di Kern raddoppia l'RTO fin quando i segnali non arrivano a destinazione al primo tentativo.

- 4) Collegamento punto-punto fibra ottica 100km. Quale ampiezza di banda rende (bit/s) un ritardo di proporzione uguale al tempo di trasmissione per pacchetti di 100byte?

$$t_{TR} = n \cdot \text{bit} / \text{bit rate} \Rightarrow \parallel \\ t_{PR} = l / n \cdot c \quad (v)$$

$$t_{TR} = n \cdot \text{bit} / \text{bit rate} \\ t_{PR} = l / v$$

$$T_{TR} = T_{PR} \quad \frac{n \text{ bit}}{\text{bit rate}} = \frac{l}{v} (2 \cdot 10^8) \rightarrow \frac{\text{bit rate}}{n \text{ bit}} = \frac{v}{l} \rightarrow \text{bit rate} = \frac{v \cdot n \text{ bit}}{l}$$

$$\text{bit rate} = \frac{2 \cdot 10^8}{\frac{10^9 \cdot 10^3}{12 \text{ s}}} \cdot \frac{1000}{800} = \frac{1600,000}{1600} \text{ kbit/s} \rightarrow \text{ampiezza di banda}$$

## Correzione esame (passato bitches!)

- 1) Satellite geosaziale a 30000 km a 1Mbps e frame 1KB. Quali frame manca il mittente prima di ricevere il 1° ACK? ?
- 2) data la rete 192.135.11.0 suddividerla in 3 cifre usando tutti gli indirizzi della 1a. ?
- 3) Due eth. 256B trasmettono con N e collisione. % collisione è N+1? X
- 4) freq. luce visibile usata nelle trame dati etere? ✓
- 5) Host A invia datagramme IPv4. Ricava pacchetti errori. Descrivere 2 possibili errori. ✗
- 6) Vantaggi proxy web server? ✓
- 7) Obiettivi sic hardware? ✓
- 8) Cosa sono e perché i record MX vengono inseriti in DNS? X

$$1) 1 \text{ Mbps} \text{ connessione} \quad 1 \text{ KB frame} \quad v = 2 \cdot 10^8 \quad l = 30000 \text{ km}$$

$$T_{TR} = n \text{ bit} / v$$

$$T_{PR} = l/v$$

$$T_{TR} = \frac{1000}{1000000} = 1 \cdot 10^{-3} \quad (0,001)$$

$$T_{PR} = \frac{30000000}{2 \cdot 10^8} = \frac{3 \cdot 10^7}{2 \cdot 10^8} = 0,15 \text{ s}$$

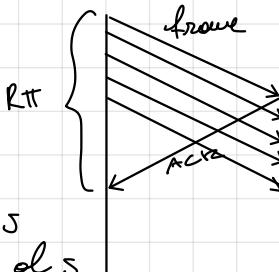
$$T_c = T_{PR} + T_{TR} = 0,155 + 0,001 = 0,156 \text{ s}$$

$$RTT = T_c \cdot T_{PR} = 0,151 \cdot 0,15 = 0,0241 \text{ s}$$

$$\text{Ack arriva dopo} = 0,0241 \text{ s}$$

A frame di 1KB a 1Mbps ovvero 1000 KB/s  $\rightarrow$  1000 frame/s quanti frame in 0,0241 s

1000 frame/s  
Prima di ricevere 1° ACK sono 226 frame inviate 24 frame



2) 192.135.11.0 Suddividere in 3 sottoreti CIDR

192.135.11.0

11000000.10000111.0001011.00000000 per 3 sottoreti bastano 2 bit

$$2^2 = 4 \text{ (3) subnets } 32 - 2 = 30$$

$$2^{4+2} = 26$$

192.135.11.xxxxxx  
  |  
  host

2^6 host per sottoretto

192.135.11.0 - 192.135.11.86

192.135.11.86 - 192.135.11.170

192.135.11.171 - 192.135.11.255

$$\text{netmask} = 255.255.255.192$$

3) Collisione a N. N+1?

Dopo la prima collisione, ho il 50% di avenire immediatamente (0 slot) e il 50% allo slot N+1. Dopo la seconda collisione la prob è del 25% per i 4 casi (0,1,2,3) e così via.

4) N. de luce visibile fra 0.4 e 0.7. Le 3 bandole misurano l'IR fra 0.8 e 1.6 + Hz

5) Errori checksum (header). TTL scritto, Manca route per la ruta destinazione.

TTL scritto: time to live meccanismo che determina il tempo di vita di un pacchetto in rete. Nel caso particolare IP determina il numero di volte per cui un router può trasmettere prima che venga distrutto. Viene messo fra 1 (255) e si riduce x ogni router che attraversa.

Errore checksum: è la somma in complemento a 1 delle sequenze di 16 bit del segmento. Se il checksum del ricevente è ≠ da quello del mittente c'è stato un errore.

6) Un proxy web server agisce da server intermediario fra l'utente e il traffico web.

Offre diversi livelli di sicurezza, tra cui l'autenticazione, ma soprattutto può anche funzionare da firewall intermediario.

7) Un SSL handshake avviene quando un utente naviga su un sito tramite HTTP e il browser pone delle query al db del server origine.

L'handshake inizia la fase di comunicazione protetta e crittata tramite SSL. Durante l'handshake le parti si verificano, scambiano ACK e decidono gli alg. da usare per la sessione.

8) Il record MX è un mail exchange record, specifica il mail server responsabile per l'invio e ricezione di email. E' contenuto nel DNS e se ne possono avere diversi.