ATTENZIONE: Manca l'esercizio 9, inoltre ho visto che ci sono poche prove sulla repo di reti, se ne avete alcune non uploadate vi prego di farlo

1[5]) Come è organizzata la struttura dell'intera rete Internet? E cosa la rende scalabile in termini di numero di collegamenti pur permettendo che tutti gli host siano connessi?

gerarchica
strutturata ad albero o piramidale, router siano gestori di rete locale, il fatto che esistano ISP (rete di accesso), poi ci sono IXP, diversi AS, dorsali di comunicazione nella parte core di Internet
rete a comm di pacchetto

2[5]) Quali sono le ragioni della perdita di pacchetti a livello 3 (Network) ? Esiste un modo per gestire pacchetti IPv4 sui router in modo da favorire pacchetti ad alta priorità? Spiegare.

congestione dei router (buffer limitato), errori nel routing (TTL limite o assenza di path tra mittente e destinazione), malfunzionamenti di HW (router),
Code a priorità differenziata: possono gestire inoltro di pacchetti a diversa priorità.

3[5]) Che cosa significa che un protocollo è Stateless? Il protocollo HTTP è stateless? Lo è sempre o è possibile renderlo non stateless? stateless e persistent sono la stessa cosa? spiegare

Stateless: è un protocollo che non mantiene informazioni sullo stato della relazione di comunicazione o servizio tra cliente e servente.

Nome e cognome (name and surname):_____(2)

4[15]) Alice vuole spedire oggi un messaggio segreto m (breve) a Bob e domani (non si sa a che ora esattamente) un messaggio molto lungo L a Charlie. In seguito Charlie vuole verificare che il messaggio m di Bob non sia contenuto nel messaggio L. Quindi Charlie chiede a Bob di inviare il messaggio m (ovviamente inviato in modo segreto).
Come si fa a essere sicuri che Charlie ottenga in modo privato (nessuno a parte Charlie e Alice conoscono sia m che L) e sicuro (nessuno ha modificato m o L in possesso di Charlie) esattamente i due messaggi inviati da Alice (m di ieri e L di oggi)?
Pensare a tutti i modi in cui Trudy potrebbe inserirsi generando problemi al raggiungimento dell'obiettivo e cercare di prevenirli, spiegando azioni e motivazioni.

Da ora in poi, tutte le chiavi pubbliche RSA saranno ottenute da CA.

ALICE che invia a BOB: KB+(m , KA-(H(m))) oppure **[KB+(m) , KA-(H(m))]**
per garanzia mittente da Alice, segretezza di m, non modificabilità di m.

ALICE che invia a CHARLIE L: genera chiave Ks, e poi [KA-(KC+(Ks)) , Ks(L) , KA-(H(L))]
per garanzia mittente da Alice, segretezza di L (efficiente), non modificabilità di L.

BOB che invia a CHARLIE m: KC+[m , KA-(H(m))] oppure [**KC+(m) , KA-(H(m))**]
si noti che serve garantire che BOB sia mittente, in quanto la garanzia è data da firma digitale di ALICE su H(m) e per ipotesi BOB e ALICE sono gli unici a possedere tale informazione (m, H(m)). Notare che me rimane segreto e firmato digitalmente (quindi non modificabile) da ALICE (garanzia del mittente essere ALICE)

Non serve necessariamente NONCE in quanto ALICE invia sia m che L firmando digitalmente, e si assume che ALICE non sia un attaccante.
Replay attack è svelabile da H(), senza ricorso a NONCE R, essendo m e L unici.

TRUDY potrebbe fare un attacco DOS modificando bit in transito oppure impedendo la ricezione di bit.
TRUDY può come sempre realizzare attacco forza bruta.

ALICE

BOB

5[10]) un Web Proxy Server (WPS) contiene in memoria circa 10.000 documenti web scaricati di recente ed è collocato all'interno di una rete locale a 1 Gbps. Ognuno dei 100 client della rete locale fa X richieste di documenti Web al secondo. La rete locale è connessa a Internet da un link di accesso a 250 Mbps. Trascurando la dimensione delle richieste (molto piccole) e considerando tutti i documenti richiesti di dimensione costante pari a 1 MB (8 Mbit), a) quale deve essere il cache hit rate minimo del WPS per non generare un collo di bottiglia sul link di accesso? b) Nella distribuzione di richieste del punto a, Se X=1, quale sarà il throughput medio al secondo generato sulla rete locale dai soli documenti scaricati dalla cache del WPS?

Scrivere qui il procedimento e i calcoli

a) cache hit rate minimo?
100*X/s, abbiamo limite 1000 Mbps capacità di rete locale.

vincolo impegno link accesso = % cache miss * Size Richiesta * NumRichiesteTot/s < 250 Mbps
quindi
(1-CacheHit) * 8*(100*X) < 250 Mbps
(1-CacheHit) < 250 / 800X = 1/(3.2*X)
quindi 1 - cache hit < 1/(3.2*X)
cache hit > **1 - 1/(3.2*X)**

b) X = 1 , throughput medio al secondo generato sulla rete locale dai soli documenti scaricati dalla cache del WPS?

se X=1 allora (1 - cache hit) = 0,3125 o 31,25%, quindi il cache hit necessario è 68,75%

In media, quindi, delle 100 richieste/s almeno 68,75 vanno a finire cache generando un carico di rete locale di 8Mb * 68,75 / sec = **550 Mbps**

6[10]) Ragionando solo a livello 1 (fisico), se volessi trasmettere un file da 36 MB usando un canale WiFi IEEE 802.11g (OFDM a 48 subcarriers) ma la condizione di rumore del canale fosse tale da impedirmi di usare ogni forma di QAM, quanto tempo impiegherei per completare la trasmissione del file? Trascurare tutti gli overhead MAC e gli errori di trasmissione, ma argomentare su eventuali possibilità di scelta dei subcarrier da usare per la protezione (convoluzione 1/2 o 3/4).
Spiegare:

La tabella di codifica IEEE 802.11g indica che sono disponibili (D)BPSK, **QPSK,** QAM. Escludendo la QAM, la codifica più veloce disponibile è QPSK (4 simboli, codifica 2 bit/simbolo).
Il symbol rate è 250.000 SYM/sec, e abbiamo 48 subcarrier totali.
Quindi avremo 48 subcarrier * 250.000 sym/sec * 2 bit = **24 Mbps**
Tuttavia con convoluzione 1/2 oppure 3/4 avremmo:
24 Mbps con 1/2 = **12 Mbps**
24 Mbps con 3/4 = **18 Mbps**

Quindi per trasmetter 36 MB = 36 * 8 Mbit = 288 Mbit impiegheremmo:

288 / 12 = 24 sec (con 1/2)
288 / 18 = 16 sec (con 3/4)

7[5]) Cosa sono e a cosa servono le CDN? Quale può essere un esempio del loro uso?

Content Distribution Networks
Scopo : distribuire contenuti in modo ridondante rispetto alla architettura fisica di rete con server distribuiti geograficamente aumentando prossimità rispetto ai client.
Lo scopo è ridurre la banda e il ritardo di collegamento per distribuire contenuti molto richiesti a un numero di clienti scalabile, senza generare colli di bottiglia nella architettura di rete.
es. NETFLIX, Google, ecc.

8[10]) rispondere con evidenza di procedimento e risultati alle seguenti domande:
a) E' o non è possibile fare il super-netting delle reti IPv4:

rete A : 179.106.0.0/16
rete B : 179.107.0.0/16

in caso affermativo quale sarebbe l'indirizzo e netmask della Super-rete ottenuta?:
Indirizzo Super-rete :_____
Netmask Super-rete. :_____

b) a aggiungendo anche la rete C: 179.105.0.0/16 è possibile fare super-netting delle 3 reti A, B e C? Spiegare.

Calcoli [procedimento richiesto]

a)
rete A: 10110011 . 0110101 0 . 00000000 . 00000000
rete B: 10110011 . 0110101 1 . 00000000 . 00000000
Siccome gli indirizzi di rete A e B / 15 sono identici, è possibile fare supernetting in rete unica /15 come da esempio.
In questo caso esprimeremo la rete risultato come: 179.106.0.0 / 15 (255.254.0.0)

10[10]) Un sistema di comunicazione wireless ha un dispositivo ricevente R con receiver sensitivity RS = -96 dBm.
a) Assumendo che l'intentional radiator del trasmettitore T fornisca la potenza di segnale Ptx = 200 mW a un'antenna isotropica, uguale a quella del ricevente R, e che il path loss in dB dovuto alla distanza di X miglia sia pari a *Free space Loss (in dB) = 36.6 + (65,10) + 20*log10(X))*, a quale frequenza avviene la comunicazione?

65,10 = 20 Log10(F), quindi abbiamo 65,10/20 = Log10(F), quindi F(Mhz) = 10^(54,1/20) = F (Mhz) = 1800 Mhz

b) Come nel caso precedente, a che distanza massima X in miglia esiste ancora un link di comunicazione, garantendo un Fade Operating Margin almeno pari a +10 dB?

Per garantire Fade Operating Margin = +10 dB, allora deve essere il Link Budget >= 10, quindi

Prx-RS >= 10, quindi Prx - (-96) >= 10, quindi Prx + 96 >= 10, quindi Prx >= 10 - 96 = - 86
Prx >= -86

imponiamo che Prx >= -86 .
Sostituendo i dati: assumendo la frequenza F = 1800 Mhz calcolata al punto a
Total Loss = Free Space loss (in dB) = 36,6 + (65,10) + 20 Log10(X) = 101,7 + 20Log10(X)
Total Gain = zero gain per le antenne (isotropica = 0dBi), per cui abbiamo solo i 200 mW di Ptx.
Total Gain = 200 mW (ma serve espresso in dB!!!), quindi converto in dBm.
200 mW = 1 mW * 10 * 10 * 2 <=> 0 dBm + 10 + 10 +3 = **23 dBm**