

PISSIR: ESERCIZI IN PREPARAZIONE DELL'ESAME DI TEORIA

1. Data link layer

Esercizio 1

Elencate almeno tre servizi/funzionalità che possono essere offerti da un protocollo di collegamento.

Esercizio 2

Cos'è l'indirizzo MAC e quando viene utilizzato? Esattamente un indirizzo MAC a cosa è associato in modo univoco? Quali differenze esistono tra l'indirizzo MAC e l'indirizzo IP, in particolare rispetto alla struttura (o formato) dell'indirizzo e rispetto alla mobilità di un nodo.

Esercizio 3

Data la sequenza di bit sottostante:
S=00101010101000011111

Indicate una possibile sequenza di bit trasmessa su un canale di comunicazione non affidabile nel caso si adotti una tecnica di controllo di parità pari:

- a) a singolo bit;
- b) bidimensionale.

Quale vantaggio fornisce la tecnica bidimensionale?

Esercizio 4

A cosa serve un protocollo di accesso al mezzo? Descrivete le caratteristiche ideali che dovrebbe avere un tale protocollo. Elencate almeno tre protocolli (o loro classi) e specificate per ognuno quali caratteristiche ideali possiede.

Esercizio 5

Considerate due stazioni A e B che comunicano a 1 Gbps adottando il protocollo 802.3. In questo caso quanto vale il bit-time?

Assumendo l'occorrenza di tre collisioni consecutive, descrivete una possibile sequenza temporale di scambio dei messaggi tra i nodi.

2. Wireless Networks

Esercizio 1

Illustrate le differenze fra le modalità *infrastruttura* e *senza infrastruttura* (ad-hoc network).

Esercizio 2

Quali sono le differenze fra i seguenti tipi di deterioramenti di segnali trasmessi su canali wireless:

1. path loss;
2. multipath propagation;
3. interferenze con altre sorgenti.

Esercizio 3

Supponete ci siano due ISP che forniscono accesso WiFi dove ogni ISP adotta il suo access point con il proprio blocco di indirizzi IP.

1. Assumete che accidentalmente ciascun ISP ha configurato il proprio access point per operare sul canale 11. In tal caso la comunicazione tramite il protocollo 802.11 è totalmente compromessa? Discutete cosa accade quando due stazioni associate a differenti ISP tentano di trasmettere contemporaneamente.
2. Ora assumete che gli access point operino su canali diversi. Come cambia la precedente risposta?

Esercizio 4

Illustrare le similitudini e le differenze fra i protocolli 802.3 e 802.11.

Esercizio 5

Considerate due stazioni A e B che comunicano su un canale condiviso tramite la tecnica CDMA.

1. Se la chip sequence di A è $S_A = \{1, -1, 1, -1, 1, -1, 1, -1\}$ come risulterà la codifica della sequenza di bit 101?
2. Assumendo che A e B vogliono trasmettere contemporaneamente sullo stesso canale e che A usi la chip sequence S_A precedentemente indicata, indicate una possibile chip sequence S_B valida per la stazione B.

3. Mobility in Networks

Esercizio 1

Descrivete nel dettaglio i passi numerati nella Figura 1. Quale tipo di instradamento è rappresentato nella figura? Specificate i/il punto/i nella comunicazione dove si utilizza la tecnica di tunneling.

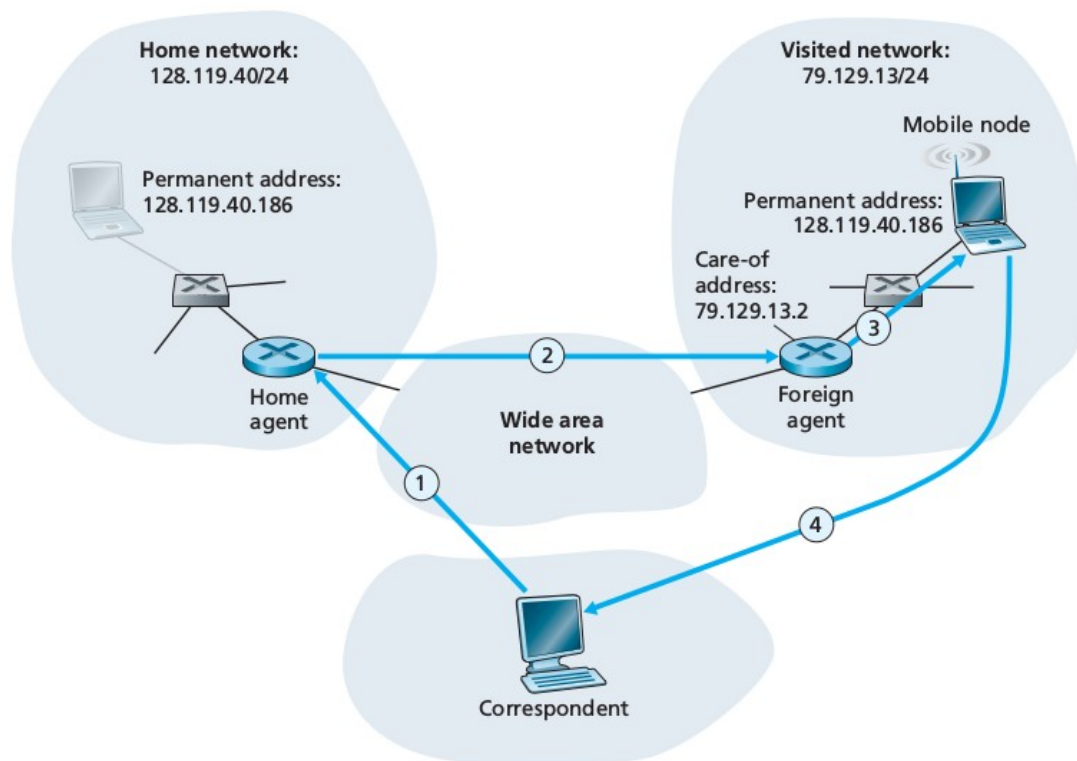


Figura 1 Instradamento ad un nodo mobile.

Esercizio 2

Descrivete come cambia la Figura 1 se ipotizziamo che anche il nodo corrispondente sia mobile, connesso ad una visited network e usi un instradamento diretto.

Esercizio 3

Quali sono le funzionalità/servizi forniti dal protocollo IP mobile? Riuscite a trovare delle analogie tra (alcuni) servizi di IP mobile e le modalità attivo/passiva del protocollo 802.11?

Esercizio 4

Spiegate cos'è la procedura di handoff, quando può essere richiesta ed in quali condizioni permette di non interrompere una connessione stabilita a livello di trasporto.

4. Multimedia networking

Esercizio 1

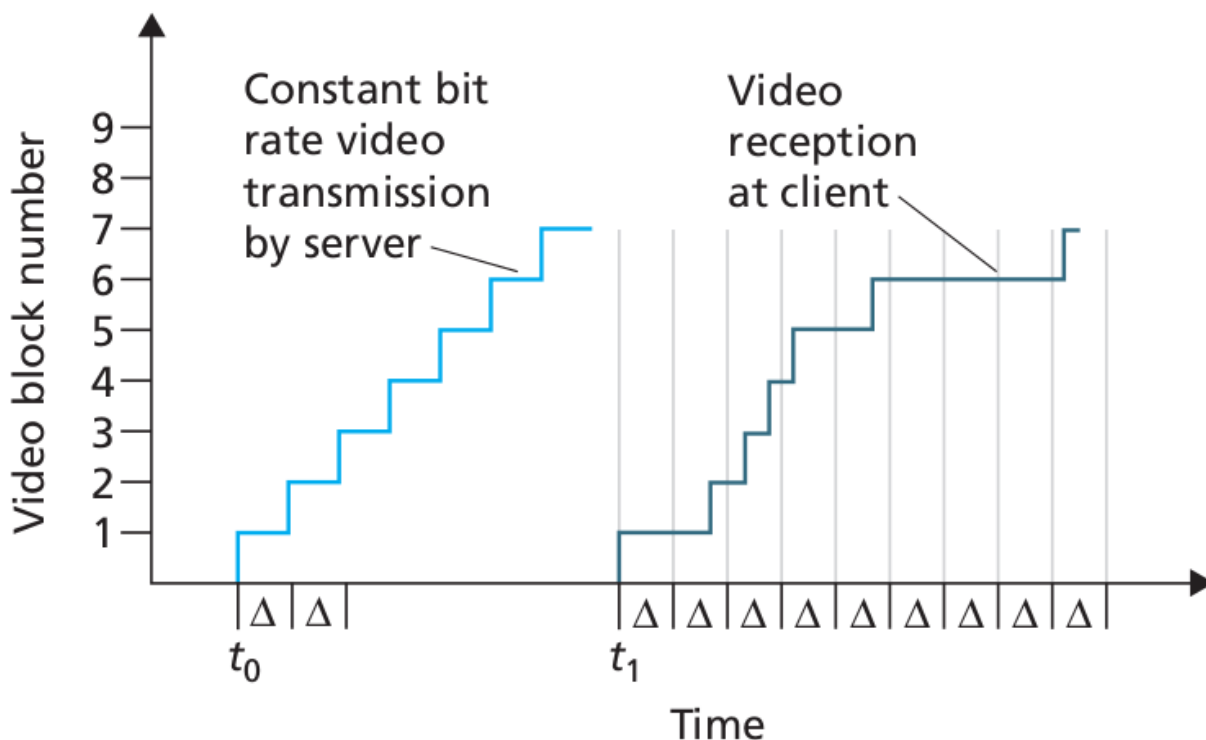
Si assuma che Victor Video guardi un video di 4 Mbps, Facebook Frank una nuova immagine da 100 Kbyte ogni 20 secondi e Martha Music stia ascoltando audio in streaming a 200 kbps. Calcolare il consumo di banda delle diverse applicazioni multimediali durante un periodo complessivo di 4000 sec.

Esercizio 2

Considerate la figura riportata di seguito. Supponete che il video sia codificato a un bit rate fisso e che quindi ogni blocco del video contenga frame che vengono riprodotti nella stessa quantità di tempo, Δ . Il server trasmette il primo blocco video al tempo t_0 , il secondo blocco al tempo $t_0 + \Delta$, il terzo a $t_0 + 2\Delta$ e così via. Quando il client inizia la riproduzione, ogni blocco dovrebbe essere riprodotto Δ unità di tempo dopo quello precedente.

(a) Supponete che il client inizi la riproduzione non appena arriva il primo blocco al tempo t_1 . Nella figura sottostante, quanti blocchi video, compreso il primo, arriveranno al client in tempo per essere riprodotti? Spiegate il ragionamento che avete fatto.

(b) Supponete ora che il client inizi la riproduzione al tempo $t_1 + \Delta$. Quanti blocchi video, compreso il primo, arriveranno al client in tempo per essere riprodotti? Spiegate il ragionamento che avete fatto.



Esercizio 3

Riprendete il semplice modello di streaming HTTP mostrato nella Figura 7.3 del libro, nel quale B denota la grandezza del buffer dell'applicazione client e Q denota il numero di bit che deve essere memorizzato nel buffer prima che l'applicazione client inizi la riproduzione. Sia r inoltre il tasso di consumo del video. Assumete che il server invii bit a un tasso costante finché il buffer del client non sia pieno.

(a) Supponete $x < r$. Come discusso nel testo, in questo caso la riproduzione avrà periodi alternati di continuità e di blocco. Determinate la lunghezza di questi due tipi di periodi, in funzione di Q , r , e x .

(b) Supponete ora $x > r$. A quale tempo t_1 il buffer dell'applicazione client si riempie?

Esercizio 4

Considerate un sistema DASH con N versioni video, a N bit rate e qualità diversi, e N versioni audio, a N bit rate e qualità diversi. Supponete di voler dare la possibilità all'utente di scegliere in ogni istante quale delle N versioni video e audio voglia.

(a) Se i file che creiamo mescolano audio e video, in modo che il server invii solo uno stream in un dato istante, quanti file deve memorizzare il server (ognuno a un URL diverso)?

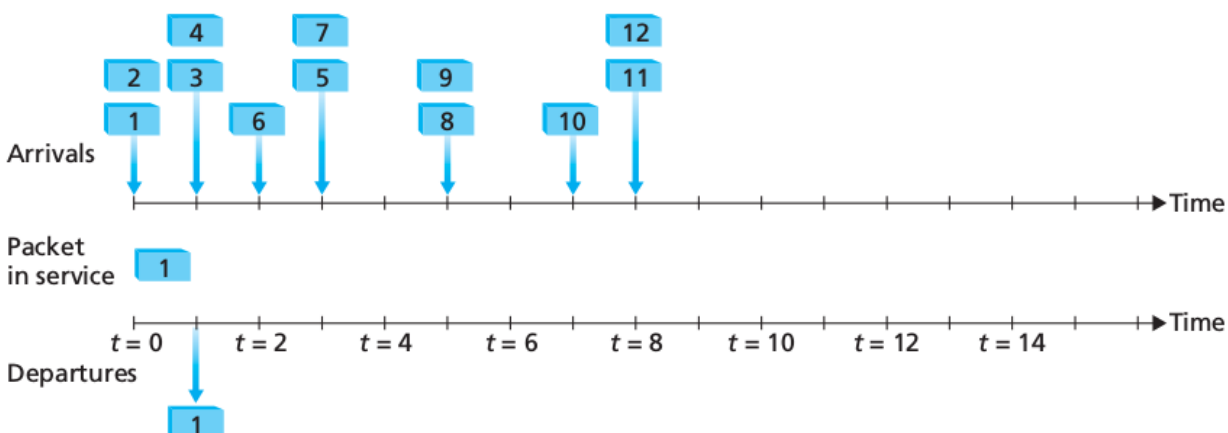
(b) Se invece il server invia separatamente gli stream audio e video e il client li sincronizza, quanti file deve memorizzare il server?

Esercizio 5

Considerate la sottostante figura che descrive l'arrivo di una sequenza di pacchetti in coda. Assumendo che al più un solo pacchetto può lasciare la coda in ogni slot di tempo, rispondete alle seguenti domande:

(a) Assumendo un servizio FIFO, indicate l'istante in cui i pacchetti da 2 a 12 lasciano la coda. Per ciascun pacchetto, qual è il ritardo tra l'arrivo e l'inizio dello slot nel quale viene trasmesso? Qual è la media di questo ritardo su tutti e 12 i pacchetti?

(b) Assumete ora un servizio a priorità: i pacchetti con numero dispari sono ad alta priorità, mentre quelli con numero pari a bassa priorità. Indicate l'istante in cui i pacchetti da 2 a 12 lasciano la coda. Per ciascun pacchetto, qual è il ritardo tra l'arrivo e l'inizio dello slot nel quale viene trasmesso? Qual è la media di questo ritardo su tutti e 12 i pacchetti?



5. Network Security¹

Esercizio 1

Quali sono le differenze fra riservatezza e integrità di un messaggio? Si può avere l'una senza l'altra? Argomentate la risposta.

Esercizio 2

Supponete che N individui vogliano comunicare tra di loro utilizzando la cifratura a chiave simmetrica e che i messaggi fra due persone, i e j , siano visibili a tutti i componenti del gruppo, che non sono però in grado di decodificarli. Quante chiavi sono necessarie nell'intero sistema? Considerate ora la cifratura a chiave pubblica. Quante chiavi sono richieste in questo caso?

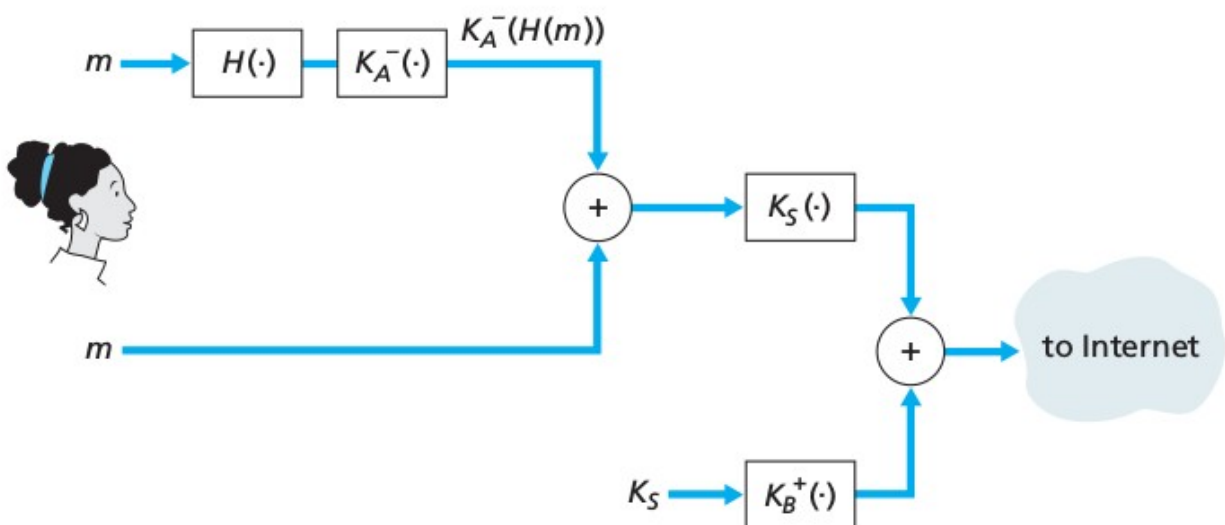
¹ Solo per gli studenti che non hanno nel piano di studi il corso di CYBER SECURITY 1

Esercizio 3

Supponete che Alice e Bob condividano 2 chiavi segrete: una chiave di autenticazione $S1$ e una chiave di cifratura simmetrica $S2$. Descrivete i passaggi necessari per inviare un messaggio affinché sia garantita la sua integrità e la sua riservatezza.

Esercizio 4

La Figura sottostante mostra le operazioni che Alice deve intraprendere con PGP per fornire riservatezza, autenticazione e integrità. Scrivete un diagramma delle operazioni corrispondenti che Bob deve eseguire sul pacchetto ricevuto da Alice.



Esercizio 5

Considerate l' esempio della Figura 8.28 in cui si è stabilita una *Security Association* tra i due router tramite IPsec con protocollo Encapsulation Security Payload (ESP). Supponete che Trudy stia usando la tecnica di man-in-the-middle, in grado di inserire datagrammi nel flusso di datagrammi inviati da R1 e R2. Come parte dell' attacco di replay, Trudy invia copie duplicate di uno dei datagrammi inviati da R1 a R2. R2 decodificherà il datagramma duplicato e lo inoltrerà alla rete della filiale? In caso negativo come fa R2 a rilevare che il datagramma è duplicato.

