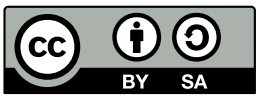
How to Esame

Esercizi e Soluzioni dalle Correzioni d'Esame

Basato sulle trascrizioni del Prof. Luciano Bononi

19 giugno 2025



Indice

Parte I
Progettazione e Concetti di Rete

1 Progettazione di Sistemi Wireless

Questa sezione copre i concetti fondamentali per progettare e verificare un sistema di comunicazione wireless funzionante.

1.1 Path Loss (Free Space Loss)

Formula del Free Space Loss (FSL)

L'attenuazione del segnale nello spazio libero si calcola con:

$$\text{FSL (dB)} = \text{Costante} + 20 \cdot \log_{10}(\text{Frequenza}) + 20 \cdot \log_{10}(\text{Distanza})$$

Parametri:

- **Costante:** Varia con le condizioni atmosferiche.
  - **36,6:** Per condizioni **peggiori** (umidità, nebbia).
  - **32,4:** Per condizioni **ideali** (secco, soleggiato).
- **Frequenza:** Inserire il valore in **MHz**.
- **Distanza:** Inserire il valore in **miglia**.

1.2 La Regola dei 6 dB

La Regola dei 6 dB

Regola pratica essenziale per calcoli rapidi:

- **Raddoppiando la distanza, si perdono 6 dB** di potenza.
- **Dimezzando la distanza, si guadagnano 6 dB** di potenza.

Spiegazione: La potenza decade con il quadrato della distanza ($1/d^2$). Raddoppiare d significa ricevere $1/4$ della potenza. In dB, dividere per 4 equivale a una perdita di $-3\,\text{dB} + -3\,\text{dB} = -6\,\text{dB}$.

Esempio Pratico con la Regola dei 6 dB

Testo: Un sistema ha un link funzionante fino a $14\,\text{miglia}$. Si vuole garantire un Fade Margin di $18\,\text{dB}$. Quale sarà la nuova distanza massima?

Soluzione:

1. **Obiettivo:** Dobbiamo "guadagnare" $18\,\text{dB}$.
2. **Ragionamento:** Ogni $6\,\text{dB}$ di guadagno richiede di dimezzare la distanza. Dobbiamo dimezzarla 3 volte ($18 = 3 \times 6$).
3. **Calcolo:** 14 miglia $\xrightarrow{/2}$ 7 miglia $\xrightarrow{/2}$ 3.5 miglia $\xrightarrow{/2}$ 1.75 miglia.
4. **Risposta:** La nuova distanza massima è $1.75\,\text{miglia}$.

1.3 Link Budget, Receiver Sensitivity (RS) e Fade Margin (FOM)

- **Receiver Sensitivity (RS):** Potenza minima (in dBm) di cui un ricevitore ha bisogno per funzionare. Un valore più basso (es. $-95\,\text{dBm}$) indica un ricevitore migliore.
- **Link Budget:** Potenza in **eccesso** che arriva al ricevitore rispetto alla sua soglia RS.
- **Fade Operative Margin (FOM):** Margine di sicurezza (tipicamente $10\,\text{dB}$ a $20\,\text{dB}$) per tollerare disturbi.

Formule Chiave

$$\text{Link Budget (dB)} = \text{Potenza Ricevuta (dBm)} - \text{RS (dBm)}$$

Per un sistema robusto:

$$\text{Link Budget (dB)} \geq \text{FOM desiderato (dB)}$$

Accorgimenti del Professore

La RS non è un valore unico. Un dispositivo può avere diverse soglie di RS, ciascuna associata a un bitrate differente. Per garantire un certo bitrate, la potenza ricevuta deve superare la RS corrispondente.

1.4 Esercizio Completo: Progettazione di un Link Wireless

Esercizio: Calcolo Link Budget e Velocità

Testo: Un trasmettitore T fornisce $25\,\text{mW}$ a un'antenna con guadagno di $8\,\text{dBi}$. Il ricevitore R ha un'antenna con guadagno di $3\,\text{dBi}$. Il path loss a 1 miglio è $-80\,\text{dB}$. La RS di R è $-75\,\text{dBm}$. A quale velocità avviene la comunicazione? La tabella delle prestazioni è:

Link Budget minimo	Bitrate nominale
$5\,\text{dB}$	$1\,\text{Mbps}$
$8\,\text{dB}$	$2\,\text{Mbps}$
$14\,\text{dB}$	$4\,\text{Mbps}$
$20\,\text{dB}$	$8\,\text{Mbps}$
$26\,\text{dB}$	$16\,\text{Mbps}$

Soluzione:

1. **Convertire la potenza di trasmissione in dBm:** La regola è: $0\,\text{dBm} = 1\,\text{mW}$. Per ottenere $25\,\text{mW}$: $1\,\text{mW} \times 10 \times 10/2/2$. In dBm: $0\,\text{dBm} + 10\,\text{dB} + 10\,\text{dB} - 3\,\text{dB} - 3\,\text{dB} = 14\,\text{dBm}$. Quindi, Ptx = $14\,\text{dBm}$.
2. **Calcolare la potenza ricevuta:** Sommiamo tutti i guadagni e le perdite.

$$\text{Potenza Ricevuta} = \text{Ptx} + \text{Gain}_{\text{TX}} + \text{Gain}_{\text{RX}} + \text{Path Loss}$$

$$\text{Potenza Ricevuta} = 14 + 8 + 3 - 80 = -55\,\text{dBm}$$

3. **Calcolare il Link Budget:**

$$\text{Link Budget} = \text{Potenza Ricevuta} - \text{RS}$$

$$\text{Link Budget} = (-55\,\text{dBm}) - (-75\,\text{dBm}) = -55 + 75 = 20\,\text{dB}$$

4. **Determinare la velocità:** Con un Link Budget di $20\,\text{dB}$, il sistema può raggiungere il livello di prestazioni corrispondente. Dalla tabella, un Link Budget di $20\,\text{dB}$ garantisce una velocità di $8\,\text{Mbps}$.

2 Indirizzamento IPv4: Subnetting e Supernetting

2.1 Teoria in Breve

- **Subnetting:** Suddivisione di una rete più grande in sottoreti più piccole. Si "rubano" bit dalla parte host della maschera per creare un identificatore di sottorete.
- **Supernetting (CIDR):** Aggregazione di più reti contigue in un unico blocco più grande. Si "restituiscono" bit dalla parte di rete alla parte host, riducendo la lunghezza della maschera (es. da /24 a /23).

- **VLSM (Variable Length Subnet Mask):** Tecnica che permette di usare maschere di sottorete di lunghezza diversa all'interno della stessa rete, ottimizzando l'uso degli indirizzi.
- **Regola d'oro per la progettazione:** Iniziare sempre l'allocazione dalla sottorete che richiede il maggior numero di host per minimizzare la frammentazione dello spazio di indirizzamento.

2.2 Esercizio Guidato: Progettazione di Rete Complessa

Esercizio: Progettazione Rete con VLSM

Testo: Progettare l'allocazione degli indirizzi per la rete `177.34.146.0/23`. Le sottoreti richieste sono: Subnet A (118 host), Subnet B (157 host), Subnet A1 (dentro A, 42 host), Subnet A2 (dentro A, 56 host).

Soluzione Guidata:

1. **Analisi Rete Iniziale:** `177.34.146.0/23` è un supernetting. Range: da `177.34.146.0` a `177.34.147.255` (512 indirizzi). Router di N: `177.34.147.254`. Broadcast: `177.34.147.255`.
2. **Strategia:** La sottorete più grande a livello gerarchico è B (157 host). Richiede 256 indirizzi (2^8), quindi una maschera /**24**. Iniziamo da B.
3. **Allocazione Subnet B (157 host):**
   - Si alloca il blocco `177.34.147.0/24`. (Si potrebbe partire anche da `146.0`, ma partendo dalla fine si lascia spazio contiguo per A).
   - **Rete B:** `177.34.147.0/24`.
   - Router di B: `177.34.147.254` (coincide con quello di N, scelta di design).
4. **Allocazione Subnet A (118 host + A1 + A2):**
   - A deve contenere sé stessa e le sue sottoreti. Host totali A: $118 + 42 + 56 \approx 216$. Servono 256 indirizzi. Anche A avrà una maschera /**24**.
   - **Rete A:** `177.34.146.0/24`.
   - Router di A: `177.34.146.254`.
   - Default Gateway di A: il router di N, `177.34.147.254`.
5. **Allocazione Subnet A1 e A2 (dentro A):**
   - Si applica di nuovo la regola: A2 (56 host) è più grande di A1 (42 host). Entrambe richiedono 64 indirizzi (2^6), quindi maschera /**26**.
   - **Allocazione A2:** Si prende il primo blocco da 64 di A.
     - **Rete A2:** `177.34.146.0/26`.
     - Router di A2: `177.34.146.62`. Default Gateway: il router di A (`177.34.146.254`).
   - **Allocazione A1:** Si prende il blocco successivo.
     - **Rete A1:** `177.34.146.64/26`.
     - Router di A1: `177.34.146.126`. Default Gateway: il router di A.

Parte II
Protocolli, Sicurezza e Trasmissione

3 Protocolli di Rete

3.1 Fragmentation and Reassembly (IPv4)

Frammentazione e Riassemblaggio

A cosa serve? La frammentazione è necessaria quando un datagramma IP, per raggiungere la sua destinazione, deve attraversare una rete il cui **Maximum Transmission Unit (MTU)** è più piccolo della dimensione del datagramma stesso.

- **Funzionamento:** Un router, trovando l'MTU del link di uscita troppo piccolo, suddivide il datagramma originale in più datagrammi più piccoli, chiamati **frammenti**.
- Ogni frammento è un datagramma IP valido, ma condivide con gli altri frammenti dello stesso pacchetto originale parte dell'header.
- **Campi dell'Header IP utilizzati:**
  - **Identification:** Un numero identico per tutti i frammenti dello stesso datagramma originale. Permette all'host di destinazione di raggruppare i frammenti corretti.
  - **Flags:** Un campo di 3 bit. Il bit **More Fragments (MF)** è a 1 per tutti i frammenti tranne l'ultimo, segnalando che altri frammenti seguiranno. Il bit **Don't Fragment (DF)** può essere impostato per impedire la frammentazione (causando un errore ICMP se necessario).
  - **Fragment Offset:** Indica la posizione del frammento all'interno del datagramma originale, misurata in unità di 8 byte.
- **Riassemblaggio:** Avviene **solo sull'host di destinazione finale**. I router intermedi non riassemblano i frammenti, ma li instradano indipendentemente.

3.2 Broadcast a livello MAC e di Rete

Accorgimenti del Professore

Broadcast MAC vs. Broadcast di Rete **Perché servono entrambi?** Non basta averne solo uno perché operano a livelli e con scopi diversi.

- **Broadcast MAC (es.** `FF:FF:FF:FF:FF:FF`**):**
  - **Scopo:** Raggiungere **tutti i dispositivi sullo stesso segmento di rete locale (LAN) o dominio di broadcast**.
  - **Funzionamento:** Un frame con indirizzo MAC di destinazione broadcast viene processato da ogni scheda di rete su quel segmento. Non viene inoltrato dai router.
  - **Esempio d'uso tipico:** Il protocollo **ARP (Address Resolution Protocol)**. Un host che conosce l'IP di un altro host sulla stessa LAN, ma non il suo MAC address, invia una richiesta ARP in broadcast MAC chiedendo "Chi ha questo IP?". Solo l'host con quell'IP risponderà.
- **Broadcast di Rete (es.** `255.255.255.255` **o indirizzo di broadcast di una subnet):**
  - **Scopo:** Raggiungere **tutti gli host all'interno di una specifica sottorete IP**.
  - **Funzionamento:** Un pacchetto con indirizzo IP di destinazione broadcast viene, a livello MAC, incapsulato in un frame con MAC broadcast per essere consegnato a tutti sulla LAN. I router, per default, **non inoltrano** i pacchetti di broadcast per limitarne la propagazione e prevenire i "broadcast storm".
  - **Esempio d'uso tipico:** Il protocollo **DHCP (Dynamic Host Configuration Protocol)**. Un client appena connesso alla rete non ha un indirizzo IP. Invia una richiesta DHCP in broadcast di rete per trovare un server DHCP che possa assegnargli un indirizzo.

3.3 Slow Start e Congestion Avoidance (TCP)

Controllo di Congestione in TCP

Queste sono due fasi del meccanismo di controllo della congestione di TCP, che serve a evitare di sovraccaricare la rete.

- **Congestion Window (cwnd):** È una variabile mantenuta dal mittente che limita il numero di dati non ancora riscontrati (acknowledged) che possono essere in transito.
- **Slow Start:**
  - **Scopo:** Trovare rapidamente la capacità disponibile della rete all'inizio di una connessione o dopo un timeout per congestione.
  - **Funzionamento:** La `cwnd` inizia a 1 MSS (Maximum Segment Size) e **raddoppia ad ogni RTT** (Round Trip Time) in cui riceve ACK. Questa è una crescita **esponenziale**.
  - **Fine della fase:** La fase di Slow Start termina quando la `cwnd` raggiunge un valore di soglia chiamato `ssthresh` (slow start threshold).
- **Congestion Avoidance:**
  - **Scopo:** Sondare più cautamente la banda disponibile una volta che la rete si sta avvicinando alla saturazione.
  - **Funzionamento:** Una volta superata la soglia `ssthresh`, la `cwnd` aumenta in modo **additivo** (tipicamente di 1 MSS per ogni RTT). La crescita è **lineare** e molto più lenta.
  - **Gestione della perdita:** Se viene rilevata una perdita di pacchetti (es. tramite 3 ACK duplicati), TCP dimezza la `ssthresh` e riporta la `cwnd` a 1, ripartendo da Slow Start.

4 Sicurezza delle Reti

4.1 Teoria in Breve

- **Crittografia Simmetrica (es. AES):** Usa la **stessa chiave** per cifrare e decifrare. È molto veloce ma richiede un modo sicuro per scambiare la chiave.
- **Crittografia Asimmetrica (es. RSA):** Usa una coppia di chiavi: una **pubblica** (per cifrare) e una **privata** (per decifrare). La chiave pubblica può essere distribuita liberamente. È più lenta di quella simmetrica.
- **Firma Digitale:** Si ottiene cifrando l'hash di un messaggio con la propria **chiave privata**. Chiunque può verificarla usando la chiave pubblica del mittente. Garantisce **autenticità** (il mittente è chi dice di essere) e **integrità** (il messaggio non è stato modificato).
- **Approccio Ibrido:** Per messaggi grandi, si usa un approccio efficiente: si genera una chiave simmetrica casuale (*session key*) per cifrare il messaggio, e poi si usa la crittografia asimmetrica per cifrare e inviare solo la *session key*.

4.2 Esercizio Guidato: Scenario di Sicurezza Complesso

Esercizio: Scambio Sicuro tra Alice, Bob e Charlie

Testo: Alice deve spedire m_1 (breve) a Bob e m_2 (breve) a Charlie. Bob e Charlie devono potersi scambiare i messaggi ricevuti. Garanzie richieste:

- **Confidenzialità:** Trudy non deve leggere i messaggi.
- **Garanzia del Mittente:** Bob e Charlie devono essere certi che i messaggi provengano da Alice.
- **Integrità:** I messaggi non devono essere stati modificati.
- **Attacchi Possibili:** Come può Trudy attaccare la comunicazione e come si risolve?

Soluzione Guidata: Dato che i messaggi sono brevi, si può usare la crittografia asimmetrica direttamente.

1. **Preparazione:** Alice ottiene le chiavi pubbliche di Bob (K_{B+}) e Charlie (K_{C+}) da una Certification Authority (CA) per evitare attacchi Man-in-the-Middle.
2. **Alice $\rightarrow$ Bob:** Alice invia a Bob:

$$K_{B+}(m_1, K_{A-}(H(m_1)))$$

   - $K_{B+}(\dots)$: La cifratura con la chiave pubblica di Bob garantisce la **confidenzialità**. Solo Bob può decifrare con la sua chiave privata K_{B-}.
   - $K_{A-}(H(m_1))$: La firma digitale di Alice sull'hash del messaggio garantisce **autenticità** e **integrità**.

3. **Alice $\rightarrow$ Charlie:** Alice invia a Charlie in modo analogo:

$$K_{C+}(m_2, K_{A-}(H(m_2)))$$

4. **Scambio Bob $\leftrightarrow$ Charlie:**
   - **Bob $\rightarrow$ Charlie:** Bob, dopo aver decifrato e verificato m_1, vuole inoltrarlo a Charlie. Invia l'intero blocco ricevuto da Alice, ma cifrato per Charlie:

$$K_{C+}(m_1, K_{A-}(H(m_1)))$$

     Charlie decifra e verifica la firma originale di Alice, confermando che il messaggio è autentico e integro.
   - **Charlie $\rightarrow$ Bob:** Stesso procedimento per m_2.
5. **Attacchi di Trudy e Contromisure:**
   - **Attacco di Replay:** Trudy potrebbe intercettare un messaggio (es. quello di Alice a Bob) e reinviarlo in un secondo momento. Bob lo accetterebbe come valido.
   - **Soluzione:** Bisogna includere un **Nonce** (un numero casuale usato una sola volta, o un timestamp) all'interno della parte firmata del messaggio. Esempio:

$$K_{B+}(m_1, K_{A-}(H(m_1) + R))$$

     Bob, ricevendo il messaggio, controlla se ha già visto il nonce R. Se sì, scarta il messaggio come un duplicato.
   - **Attacco DoS (Denial of Service):** Trudy potrebbe bombardare Bob con messaggi spazzatura, costringendolo a eseguire onerose operazioni di decifratura RSA. Non c'è una soluzione crittografica semplice; la soluzione è a livello di infrastruttura (es. firewall).

5 Teoria della Trasmissione

5.1 Canale Radio OFDM e Codifica PSK

Esercizio: Calcolo Prestazioni Canale OFDM

Testo: Un canale radio OFDM ha 18 sub-carrier e un symbol rate di $500\,000\,\text{simboli/sec}$ per sub-carrier. Quale codifica PSK si deve usare per trasferire un file di $54\,\text{Mbit}$ in non più di $4\,\text{secondi}$, massimizzando la resistenza all'errore? Calcolare il tempo esatto di trasferimento.

Soluzione Guidata:

1. **Calcolare la capacità totale del canale in simboli/sec:**

$$\text{Capacità simboli} = \text{N. sub-carrier} \times \text{Symbol rate}$$

$$\text{Capacità simboli} = 18 \times 500.000 = 9\,000\,000\,\text{simboli/sec}$$

2. **Calcolare il bitrate minimo richiesto:**

$$\text{Bitrate richiesto} = \frac{\text{Dimensione file}}{\text{Tempo massimo}} = \frac{54\,\text{Mbit}}{4\,\text{s}} = 13.5\,\text{Mbit/s}$$

3. **Determinare i bit/simbolo necessari e scegliere la codifica:** Per raggiungere il bitrate richiesto, ogni simbolo deve trasportare un certo numero di bit.

$$\text{Bit/simbolo necessari} = \frac{\text{Bitrate richiesto}}{\text{Capacità simboli}} = \frac{13.500.000}{9.000.000} = 1.5\,\text{bit/simbolo}$$

   - La codifica deve fornire **almeno** 1.5 bit/simbolo.
   - **BPSK** (o 2-PSK) fornisce 1 bit/simbolo. Non è sufficiente.
   - **QPSK** (o 4-PSK) fornisce 2 bit/simbolo. È la scelta giusta.
   - Si sceglie la codifica con il minor numero di bit che soddisfa il requisito per **massimizzare la resistenza all'errore** (meno punti nella costellazione sono più distanti e quindi più robusti).

4. **Calcolare il bitrate effettivo con la codifica scelta (QPSK):**

$$\text{Bitrate effettivo} = \text{Capacità simboli} \times \text{Bit/simbolo (QPSK)}$$

$$\text{Bitrate effettivo} = 9.000.000 \times 2 = 18\,\text{Mbit/s}$$

5. **Calcolare il tempo esatto di trasferimento:**

$$\text{Tempo trasferimento} = \frac{\text{Dimensione file}}{\text{Bitrate effettivo}} = \frac{54\,000\,000\,\text{bit}}{18\,000\,000\,\text{bit/s}} = 3\,\text{secondi}$$

5.2 Interferenza Multipath

Esercizio: Interferenza tra Segnale Diretto e Riflesso

Testo: Un segnale radio a $37.5\,\mathrm{MHz}$ viene ricevuto tramite due percorsi:

- **Line-of-Sight (diretto):** percorso di $29\,\mathrm{metri}$.
- **Riflesso:** il segnale percorre $21\,\mathrm{metri}$, rimbalza su un muro a 90°, e poi raggiunge il ricevitore.

I due segnali ricevuti consentono una buona comunicazione?

Soluzione Guidata: L'obiettivo è capire se i due segnali arrivano in fase (interferenza costruttiva) o in controfase (interferenza distruttiva).

1. **Calcolare la lunghezza del percorso riflesso:** Il percorso forma un triangolo rettangolo, con l'ipotenusa pari alla distanza Line-of-Sight ($29\,\mathrm{m}$) e un cateto pari a $21\,\mathrm{m}$.

   $$\text{Cateto minore} = \sqrt{29^2 - 21^2} = \sqrt{841 - 441} = \sqrt{400} = 20\,\mathrm{metri}$$

   La lunghezza totale del percorso riflesso è la somma dei due cateti:

   $$\text{Lunghezza riflessa} = 21 + 20 = 41\,\mathrm{metri}$$

2. **Calcolare la differenza di percorso:**

   $$\Delta d = \text{Lunghezza riflessa} - \text{Lunghezza diretta} = 41 - 29 = 12\,\mathrm{metri}$$

3. **Calcolare la lunghezza d'onda (λ) del segnale:** La velocità della luce $c \approx 3 \times 10^8\,\mathrm{m/s}$. La frequenza $f = 37.5\,\mathrm{MHz} = 37.5 \times 10^6\,\mathrm{Hz}$.

   $$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{37.5 \times 10^6} = 8\,\mathrm{metri}$$

4. **Verificare la relazione di fase:** Controlliamo quante lunghezze d'onda sono contenute nella differenza di percorso.

   $$\frac{\Delta d}{\lambda} = \frac{12}{8} = 1.5$$

   Risposta: Poiché la differenza di percorso è un multiplo di mezza lunghezza d'onda (in questo caso 1.5λ), i due segnali arrivano in **opposizione di fase** (interferenza distruttiva). Avendo quasi la stessa energia, si annullano a vicenda. **La comunicazione non sarà buona**.