Parte 1 - Multiple:

1. C) Session Layer
2. B) Network Layer
3. C) Broadcast
4. C) Controllo di flusso
5. C) È usato principalmente come modello di riferimento
6. C) Un'unità di dati del livello Data Link
7. B) Identificatori del protocollo di livello superiore
8. B) Session layer
9. A) IEEE
10. B) Incapsulamento

Parte 2 - Vero/Falso:

1. F (TCP/IP ha 4 livelli, OSI ne ha 7)
2. F
3. V
4. V
5. F (Si occupa dell'indirizzamento fisico)
6. V
7. V
8. F (Protocol Data Unit)
9. F (A livello data link)
10. F (È decentralizzato)

Risposte aperte da 5 punti:

1. Confronto OSI vs TCP/IP: "Il modello OSI è composto da 7 livelli (Applicazione, Presentazione, Sessione, Trasporto, Rete, Data Link, Fisico), mentre TCP/IP ne ha 4 (Applicazione, Trasporto, Internet, Network Access). Il modello OSI è teorico e fornisce linee guida precise per ogni livello, mentre TCP/IP è più pratico e implementato. OSI separa chiaramente le funzioni: presentazione gestisce la sintassi dei dati, sessione coordina il dialogo, trasporto garantisce l'affidabilità. TCP/IP combina alcune di queste funzioni nel livello applicazione. Nonostante le differenze, OSI rimane fondamentale come riferimento per comprendere i principi di networking e per progettare nuovi protocolli, offrendo una struttura modulare che facilita l'evoluzione tecnologica."
2. LLC e MAC: "Il Data Link Layer è diviso in due sottolivelli: LLC (Logical Link Control) e MAC (Media Access Control). LLC fornisce un'interfaccia uniforme al livello Network, gestendo il controllo di flusso, la sequenzializzazione dei frame e il recupero degli errori. Utilizza i campi DSAP e SSAP per identificare i protocolli di livello superiore. Il MAC gestisce l'accesso al mezzo fisico, definisce gli indirizzi hardware (MAC address) e implementa meccanismi di controllo delle collisioni. I due sottolivelli collaborano: MAC gestisce la trasmissione fisica dei frame creati da LLC, che a sua volta maschera al Network Layer le specificità del mezzo trasmissivo sottostante."
3. Architetture di rete: "Le principali architetture sono: Client-Server e Peer-to-Peer (P2P). Client-Server: centralizza servizi su server dedicati, offre gestione semplificata e sicurezza migliore, ma rischia colli di bottiglia e single point of failure. Vantaggi: controllo centralizzato, backup facilitato, sicurezza gestibile. Svantaggi: costi hardware/software, vulnerabilità server. P2P: ogni nodo è sia client che server, offre scalabilità e resilienza. Vantaggi: robustezza, costi ridotti, utilizzo efficiente risorse. Svantaggi: sicurezza complessa, prestazioni variabili, difficile gestione. Esistono anche architetture ibride che combinano vantaggi di entrambe per applicazioni specifiche."
4. Enti standardizzazione: "Gli enti di standardizzazione sono fondamentali per l'interoperabilità delle reti. IEEE (Institute of Electrical and Electronics Engineers) ha definito gli standard 802: 802.3 (Ethernet), 802.11 (Wi-Fi), rivoluzionando le LAN. ISO (International Organization for Standardization) ha creato il modello OSI, framework teorico essenziale. IETF (Internet Engineering Task Force) gestisce gli standard Internet attraverso gli RFC, definendo protocolli come TCP/IP, HTTP, SMTP. La loro collaborazione garantisce l'evoluzione coerente delle tecnologie di rete: IEEE per il livello fisico/data link, IETF per i protocolli di rete, ISO per i modelli teorici. Questo sistema ha permesso lo sviluppo di Internet come la conosciamo oggi."