CS Exit Ethiopia

Revision Outlines

Computer Science Exit Examination

1 selected course | 18 November 2026

Selected courses

01. Data Communication and Computer Networking

https://csexitethiopia.com

abelasnake2003@gmail.com | Telegram: @Abechu7

Course contents

Each course begins on a new page. PDF bookmarks provide question, study-note section and revision-topic navigation.

Data Communication and Computer Networking 3

Data Communication and Computer Networking

Revision Outlines

Communication components and quality | Exam focus

- Communication components
  - Data: raw representations
  - Information: interpreted data
  - Message; sender; receiver; medium; protocol
  - Source creates data
  - Transmitter: data → signal
  - Receiver reconstructs data
  - Distance: engineering factor, not sixth component
- Communication quality
  - Delivery: intended recipient
  - Accuracy: preserved content
  - Timeliness: deadline
  - Jitter: arrival-delay variation
  - Average delay can conceal disruptive jitter
  - Throughput: achieved transfer rate
  - Reliability: dependable operation
  - Security: unauthorized actions
  - Scalability: growth without unacceptable degradation

Network size, access and architecture

- Network geographic scope
  - PAN: personal Bluetooth devices
  - LAN: building or campus
  - MAN: metropolitan region
  - WAN: distant regions
  - Device count alone insufficient

- Internet: global network of networks
- Internet as largest WAN example

• Access scope and service roles
- Intranet: organizational internal services
- Extranet: approved outsiders
- Access scope ≠ geographic size
- Client requests; server supplies
- Peers perform both roles
- Dedicated servers can also be clients
- DNS; backup; update dependencies
- Ten-user cutoff: guideline only
- Centralization: simpler administration, concentrated dependencies
- Peer networks still require security

Protocols, standards and layers | Exam focus

• Protocols and standards
- Syntax: message structure
- Semantics: field meanings
- Timing: exchange schedule and rate
- Standards enable interoperability
- De facto: established use
- De jure: formal approval
- ISO: international standards
- IEEE: 802.3 Ethernet; 802.11 Wi-Fi
- ITU-T: telecommunications
- ANSI: US standards coordination
- EIA: interface standards
- FCC: regulator

• Layer models
- Reference model: responsibilities and interfaces
- Model ≠ executable software
- OSI: seven reference layers
- TCP/IP: implemented suite, usually four layers

- Five-layer model separates physical and link
- State model before counting

Signals, periods and bandwidth | Exam focus

- Signal characteristics
  - Analog: continuous; digital: discrete symbols
  - Data type ≠ signal type
  - Digital bits modulate analog carriers
  - Sine wave: amplitude, frequency, phase
  - f: cycles/second
  - T=1/f
  - λ=v/f; propagation speed v
  - Phase: within-cycle displacement
  - Composite signals combine frequencies
- Bandwidth and carrier placement
  - Frequency bandwidth=highest−lowest; hertz
  - Low-pass includes zero frequency
  - Band-pass: nonzero frequency range
  - Baseband: no carrier shift
  - Passband: modulated carrier
  - Hz ≠ bit/s
  - 2 kHz → T=0.5 ms

Bit rate, baud and channel capacity | Exam focus

- Bit rate versus baud
  - R: bits/second; bit interval=1/R
  - Baud: symbols/second, not voltage transitions
  - M states → log2(M) bits/symbol
  - R=baud×log2(M), before coding overhead
  - Manchester: extra transitions
  - Binary ≠ universally baud=bit rate
- Channel capacity bounds
  - Nyquist: ideal noiseless channel

- R≤2B log2(M)
- Shannon: Gaussian noise
- C=B log2(1+S/N)
- S/N: linear power ratio
- SNR(dB)=10 log10(S/N)
- Bandwidth; signal levels; noise
- Distance affects attenuation, delay, achievable rate
- Distance absent from simplified formulas

• Worked example Nyquist and Shannon example

- B=3000 Hz; M=4
- 2×3000×log2(4)=12,000 bit/s
- S/N=15 → log2(16)=4
- Shannon limit=12,000 bit/s
- 15 dB ≠ linear ratio 15

Delay, impairments and transmission modes | Exam focus

• Delay components

- Transmission delay=packet bits/link bit rate
- Propagation delay=distance/signal speed
- Processing delay; queueing delay
- 1000 bytes at 10 Mbit/s
- Serialization=0.8 ms
- Higher rate leaves propagation unchanged

• Signal impairments

- Attenuation: reduced strength
- Distortion: changed shape, unequal frequency delays
- Noise: unwanted energy
- Thermal noise: random thermal motion
- Crosstalk: nearby-channel leakage
- Impulse noise: short disturbance
- Amplifiers amplify noise too
- Digital repeaters regenerate decisions
- Corrupted bits not always recoverable

- Transmission modes
  - Simplex: one direction
  - Half duplex: alternating directions, walkie-talkie
  - Full duplex: simultaneous directions, telephone
  - Serial: sequential bits
  - Parallel: multiple conductors, skew risk
  - Asynchronous serial: character start/stop bits
  - Synchronous framing: ongoing clock recovery
  - Serial timing ≠ browser asynchronous requests

Cables, wireless and connectors | Exam focus

- Guided media
  - Twisted pairs reduce coupled interference
  - UTP: unshielded; STP: shielded
  - Coax: axial conductor and outer shield
  - Fiber: guided light; EMI resistance
  - Fiber: high capacity and long reach
  - Suitable optics and installation required
  - Specification determines speed, cost, reach
  - Fiber remains tappable
- Unguided media and Ethernet cables
  - Radio; microwave; infrared
  - Ground waves follow Earth
  - Sky waves: ionized-layer reflection
  - Line-of-sight requires visibility
  - Microwaves belong to radio spectrum
  - Infrared generally blocked by walls
  - Antenna determines directionality
  - Omnidirectional: broad azimuth, not uniform 3-D
  - Straight-through: unlike MDI/MDI-X roles
  - Crossover: like roles, PC-PC, switch-switch
  - Auto-MDI-X removes legacy cable constraint

Topology and failure reasoning | Exam focus

- Topology and link scope
  - Physical: link layout
  - Logical: communication/access relationships
  - Point-to-point: two endpoints
  - Multipoint: shared medium
  - Full mesh uses point-to-point links
  - Contradictory module mesh statement
- Topology failure reasoning
  - Bus: shared backbone; unterminated-break disruption
  - Star: central device
  - Star edge failure: one endpoint
  - Star central failure: whole star
  - Ring: loop; single-break vulnerability
  - Protected dual rings differ
  - Token Ring uses token passing
  - Token access not inherent to rings
  - Tree: hierarchy; hybrid: combined arrangements
- Full undirected mesh calculations
  - Links=$n(n-1)/2$
  - Interfaces/node=$n-1$
  - 50 nodes → 1225 links
  - Redundancy improves fault tolerance
  - Higher cable and interface cost

NICs, repeaters and hubs | Exam focus

- NIC and physical functions
  - NIC: computer network interface
  - NIC commonly implements physical and link
  - Physical interface ≠ exclusively layer 1
  - Connectors; signaling; voltage; timing
  - Physical coding and modulation
  - PHY-MAC interface: hardware signaling

- Repeaters, hubs and device roles
  - Repeater: layer-1 signal regeneration
  - No destination-address inspection
  - Active hub: multiport repeater
  - Signals repeated onto other ports
  - Half-duplex hub: shared collision domain
  - Passive hub: connector
  - No MAC learning or collision elimination
  - Network printer: endpoint consuming services
  - Routers; hubs; access points: intermediaries
- Legacy IEEE 802.3 PHY architecture
  - AUI: attachment unit interface
  - MAU: medium attachment unit
  - MAC interfaces to PLS
  - PLS: Physical Signaling sublayer
  - Physical-layer signaling: PLS
  - Architecture-specific, not universal OSI terminology
  - Other PHY designs: RS; PCS; PMA
  - Reconciliation; coding; medium attachment

Bridges, switches and access points | Exam focus

- Layer-2 bridges and switches
  - Learn source-MAC-to-port mappings
  - Look up destination MAC
  - Known unicast: destination port
  - Same incoming segment: filter
  - Unknown unicast or broadcast: VLAN flood
  - Switch need not select one port
  - Wireless AP: wireless-wired link bridge
- Switch collision and broadcast boundaries
  - Separate collision domain per port
  - Full-duplex point-to-point Ethernet: no collisions
  - Full duplex: no CSMA/CD

- Independent simultaneous conversations
- Broadcasts remain within VLAN
- Additional controls may filter broadcasts
- Layer-3 switch also routes
- Function overrides marketing name

Routers, gateways and traffic controls | Exam focus

- Routers and gateways
  - IP forwarding: destination prefixes, next hops
  - Routers separate broadcast domains
  - Local link broadcasts normally stopped
  - Default gateway: usually router
  - Protocol gateway: application-format translation
  - Gateway ≠ inherently every OSI layer
- Firewall, VPN and modem
  - Firewall: policy-based allow/reject/inspect
  - Firewall need not encrypt
  - VPN: Virtual Private Network
  - Logical private connection over another network
  - Secure VPN: tunnel authentication and encryption
  - Modem: outgoing modulation, incoming demodulation
  - Home router may combine distinct functions

OSI layers and encapsulation | Exam focus

- Encapsulation and routed hops
  - Application data → segment/datagram → packet
  - Packet → frame → bits/symbols
  - Receiving reverses encapsulation
  - Each layer serves layer above
  - Router removes incoming link frame
  - Router inspects IP; creates next-hop frame
  - MAC addresses usually change per hop
  - End-to-end IP ordinarily persists until translation

- 7 Application
  - Network services for applications
  - Message/data
- 6 Presentation
  - Representation; compression; encryption
  - Data
- 5 Session
  - Dialog setup; checkpoints; recovery
  - Data
- 4 Transport
  - Process delivery; segmentation
  - Protocol-dependent reliability
  - TCP segment; UDP datagram; port
- 3 Network
  - Logical addressing; routing
  - Packet; IP
- 2 Data link
  - Hop delivery; framing; MAC access
  - Error detection
  - Frame; MAC
- 1 Physical
  - Signaling; bit/symbol transport
  - Bits/symbols

Link control, framing and error detection | Exam focus

- Link control and framing
  - LLC: upper-protocol identification/multiplexing
  - LLC may provide link control
  - MAC: medium-dependent addressing/access, frame delivery
  - Network addressing: layer 3
  - Ethernet; PPP; HDLC: link protocols
  - Headers: addresses, control/type fields
  - Synchronization and framing depend on protocol

- Error detection versus recovery
  - Redundancy detects, not necessarily corrects
  - Even parity: even total ones
  - 1011 → parity bit 1
  - Odd flips detected; even counts missed
  - CRC: polynomial bits, XOR-division remainder
  - Receiver repeats CRC division
  - Internet checksum: end-around carry, complemented sum
  - Burst: first-last corruption, unchanged interiors included
  - Recovery: retransmission or sufficient FEC redundancy

Access control and reliable-link procedures | Exam focus

- Random access
  - ALOHA: opportunistic sending
  - CSMA: carrier sensing
  - Legacy half-duplex Ethernet: CSMA/CD
  - Collision→jam→stop→random backoff
  - Jam indicates collision, not clearance
  - Wi-Fi 802.11: CSMA/CA
  - Waiting/backoff and acknowledgments
  - Hidden terminals remain despite sensing
- Controlled access and reliable links
  - Polling; reservation; token turns
  - Correct coordination avoids contention collisions
  - Channelization: frequency, time, code
  - Stop-and-wait: one frame, await ACK
  - Timeout retransmission; sequence-bit duplicate detection
  - Sliding window: multiple unacknowledged frames
  - Link reliability/flow control: hop-local
  - Transport reliability/flow control: end-to-end
  - Ethernet detects corruption without delivery guarantee

Line coding, modulation and sampling

- Line coding
  - Digital bits → digital signal patterns
  - NRZ: no forced mid-bit return
  - Manchester: clocking mid-bit transition
  - Manchester bit convention must be specified
  - Differential Manchester: relative-state transitions
  - AMI: alternating successive-one polarities
  - Pseudoternary: alternating zero pulses
  - Block coding adds redundancy
  - Scrambling replaces problematic patterns
  - Scrambling need not increase bit count
  - Multilevel: 2B1Q; 8B6T
  - MLT-3: voltage-transition sequence
- Modulation and digitization
  - ASK: amplitude; FSK: frequency; PSK: phase
  - QAM: amplitude plus phase
  - AM/FM/PM carry analog data
  - PCM: sampling→quantization→encoding
  - Practical sampling: fs>2fmax
  - b bits → 2^b levels
  - Uncompressed rate=fs×b
  - PAM: pulse amplitude; PWM: pulse width
  - PAM/PWM alone ≠ binary PCM code

Network delivery and IPv4 header | Exam focus

- IPv4 service and header
  - IP: connectionless best-effort delivery
  - No end-to-end ordering or retransmission
  - IPv4 address: 32 bits
  - Header: 20-60 bytes, not 32 bits
  - IHL: 32-bit words
  - Total length: header plus payload

- TTL limits router lifetime
- Protocol field: TCP, UDP, upper protocol

• IPv4 checksum and fragmentation
- Header checksum exists
- Module no-error-checking claim incorrect
- Identification; flags; fragment offset
- Sources and routers fragment when allowed
- Destination reassembles
- DF plus insufficient MTU: forwarding fails
- Possible ICMP diagnostic

Transport choice, ports and connections | Exam focus

• TCP versus UDP
- TCP: reliable ordered byte stream
- Sequence numbers; ACKs; retransmission; windows
- Flow control protects receiver
- Congestion control protects network
- UDP: independent datagrams, ports, checksum
- No built-in setup, reliability, retransmission, ordering
- Interactive traffic: late versus lost data
- Application reliability possible over UDP

• Transport endpoints
- Ports identify transport endpoints
- Application chooses transport
- Socket buffer requests subject to OS limits
- TCP connection: source/destination IP and ports
- TCP protocol understood in four-tuple
- IPv4 protocol number ≠ port
- 80: usual HTTP port
- Clients often use ephemeral ports
- SCTP: reliable messages, multiple streams

Trace the TCP handshake | Exam focus

- TCP three-way handshake
  - SYN → SYN+ACK → ACK
  - SYN consumes one sequence position
  - ACK: next expected sequence
  - Client ISN=395; server ISN=260
  - Client SYN: seq395
  - Server SYN+ACK: seq260 ack396
  - Client ACK: seq396 ack261
  - Application byte counts advance sequence numbers
  - FIN consumes one sequence position
- TCP connection interpretation
  - Logical transport state, no reserved circuit
  - Ports multiplex separate applications
  - Separate applications ≠ one TCP stream
  - Layer-4 reliability depends on protocol

Upper layers and the TCP/IP correspondence | Exam focus

- OSI upper-layer roles
  - Session: dialog establishment and management
  - Checkpoints enable interrupted-transfer recovery
  - Presentation: encoding translation, compression, encryption
  - Compression reduces representation size
  - Encryption hides content, need not shrink
  - Application protocols serve applications directly
  - Practical functions distributed differently
  - TLS ≠ separate physical presentation device
- TCP/IP correspondence
  - OSI 5-7 → application
  - Transport retained
  - OSI network → Internet
  - Link plus physical → network access
  - Model does not guarantee reliability

- Application service builds on process transport
- Vague service labels may overlap

DNS, DHCP and address resolution | Exam focus

- DNS and DHCP
  - DNS: names → records
  - A: IPv4; AAAA: IPv6
  - DNS: UDP or TCP port 53
  - DHCP: dynamic IPv4 leases
  - Address; mask; gateway; DNS server
  - Discover → offer → request → acknowledge
  - IP itself does not assign addresses
- Address resolution and companion protocols
  - ARP: on-link IPv4 next-hop → MAC
  - Broadcast request; normally unicast reply
  - Off-subnet ARP resolves gateway MAC
  - Remote target MAC not resolved
  - Network/link boundary; often link-layer classification
  - Network-protocol label: loose textbook convention
  - RARP: hardware → IP
  - BOOTP/DHCP: boot configuration
  - ICMP: errors and diagnostics
  - IGMP: IPv4 multicast membership
  - Companions ≠ constituent pieces of IP

Web, file, mail and remote-login protocols | Exam focus

- Application service protocols
  - HTTP: stateless request/response semantics
  - HTTP message body optional
  - HTTPS: HTTP with TLS
  - FTP: separate control/data connections
  - FTP ≠ SFTP
  - SMTP: mail submission and relay

- POP3: retrieval
- IMAP: server-mailbox access/synchronization
- SMTP ≠ end-user mailbox retrieval

• Usual ports and remote access

- FTP control 21; SSH 22
- Telnet 23; SMTP relay 25
- DNS 53; HTTP 80
- POP3 110; IMAP 143; HTTPS 443
- Telnet: unencrypted terminal
- SSH: protected remote access
- Configured ports may differ
- HTTP exchange ≠ physical duplex mode

IPv4 notation and classful defaults

• IPv4 representation

- Four decimal octets, each 0-255
- 32 binary bits
- Octet weights: 128,64,32,16,8,4,2,1
- 11000001 10000011 00011011 11111111 → 193.131.27.255
- 257 invalid
- Syntax validity ≠ host assignability
- .0/.255 host validity depends on prefix

• Historical classful defaults

- A: leading 0, /8
- B: leading 10, /16
- C: leading 110, /24
- D: 1110 multicast; E: 1111 reserved
- Ordinary A: 1-126; 0/127 special
- B: 128-191; C: 192-223
- Usable: 2^24−2; 2^16−2; 254
- Modern CIDR actual prefix overrides classes

Special ranges, private addresses and IPv6

- Private and special IPv4 ranges
  - RFC1918: 10.0.0.0/8
  - 172.16.0.0/12 through 172.31.255.255
  - 192.168.0.0/16
  - Reusable internally; no global public routing
  - LAN public addressing permitted with allocation
  - 127.0.0.0/8 loopback; commonly 127.0.0.1
  - Loopback works without external link
  - 255.255.255.255: limited broadcast
  - 0.0.0.0: possible unconfigured source
  - Link-local/APIPA: 169.254.0.0/16
  - Automatic selection excludes edge /24 blocks
- IPv6 contrasts
  - 128-bit hexadecimal addresses; flexible prefixes
  - No IPv4-style broadcast
  - Fragmentation: sources only, never routers
  - No automatic traffic encryption
  - Authentication remains necessary
  - Address space, bit length, encryption-support options
  - Specific comparison needed for unique answer

Masks, prefixes and binary AND | Exam focus

- Prefix masks
  - /p: p ones, then 32−p zeros
  - Partial octets: 128,192,224,240,248,252,254
  - /19=255.255.224.0
  - /20=255.255.240.0
  - /21=255.255.248.0
  - 255.248.0.0 ≠ /21
- Network by binary AND
  - Network=address AND mask
  - Host zeros: block start

- Host ones: broadcast
- 172.16.28.252/20: third-octet increment 16
- Network=172.16.16.0; broadcast=172.16.31.255
- Written host/prefix need not be aligned
- 172.105.180.0/21 → 172.105.176.0/21

Find subnet bounds and usable hosts | Exam focus

- Subnet bounds and capacity
  - Ordinary broadcast LAN: h=32−p
  - Total=2^h; usable=2^h−2
  - Reserve network and directed broadcast
  - Changing-octet increment=256−mask octet
  - Round down to increment multiple
  - Last address=next boundary−1
- Subnet boundary examples
  - 192.168.2.64/26: .64-.127
  - Usable .65-.126: 62 hosts
  - 192.168.10.25/28 → .16-.31
  - 172.17.128.0/21 → 172.17.135.255
  - .128.255 and .135.0: valid interior hosts
  - .135.255: broadcast
  - /27: 32 total, 30 usable

Borrow bits and choose a mask | Exam focus

- Equal subnet borrowing
  - Parent /a → child /p
  - Borrowed bits b=p−a
  - Subnets=2^b, no modern subtract-two
  - Class B /16 → /19
  - b=3 → eight subnets
  - 8192 addresses; 8190 conventional hosts
  - /19 alone does not identify parent
- Choose mask from demands

- Smallest h satisfying 2^h−2≥H
- p=32−h
- 24 hosts → /27
- 52 or 57 → /26
- 100 → /25; 500 → /23
- At least six subnets → b=3
- /24 → /27: eight subnets
- Check subnet count and host capacity

Design and implement a VLSM address plan | Exam focus

• VLSM allocation method
- Different masks for LAN sizes
- Sort largest demands first
- Round reservations into power-of-two blocks
- Aligned, nonoverlapping allocations within parent
- Explicit remaining free space

• VLSM worked plan
- /24 demands: 100,60,29
- .0/25: hosts .1-.126
- .128/26: hosts .129-.190
- .192/27: hosts .193-.222
- Remaining .224/27
- Two 100-host LANs: separate /24
- .0/25 plus .128/25
- Count router interfaces unless already included

• Address-plan implementation
- Unique usable IPs and masks
- Default gateway inside local subnet
- Router interfaces and routes
- DHCP exclusions
- Test local→gateway→remote→DNS separately
- Check duplicate addresses and overlap
- Verify return routes before application blame

Point-to-point links and route aggregation

- Point-to-point prefix exceptions
  - Conventional /30: four addresses, two endpoints
  - Often smallest offered WAN choice
  - RFC3021 /31: supported point-to-point links
  - Both /31 addresses usable
  - Subtract-two rule inapplicable to /31
  - /32: single address or host route
  - /30 not universally smallest link prefix
- CIDR aggregation
  - Classless Inter-Domain Routing
  - Replaces rigid class allocation
  - Aggregate contiguous aligned common-prefix blocks
  - Adjacent-looking labels may not aggregate
  - Four consecutive /26 blocks → /24
  - Preserve more-specific routes for correct next-hops

NAT and port translation

- NAT variants
  - Static NAT: fixed address mapping
  - Dynamic NAT: mapping pool
  - PAT/NAPT: address-plus-port mapping
  - Multiple private clients share public address
  - Translation ≠ ARP or encryption
  - Return traffic requires translation state
  - Configured inbound mapping alternative
- Public Internet prerequisites
  - 10.0.0.1 commonly uses gateway NAT
  - Valid routing and public external address
  - NAT supplies neither physical connectivity nor DNS
  - Public address ≠ permission to use
  - LAN: correctly allocated public/private unicast
  - Subnet correctness remains necessary

Routing algorithms and destination sets

- Routing versus forwarding
  - Routing computes paths
  - Forwarding selects packet next hop
  - Longest matching prefix first
  - Then routing-system tie breakers
  - Default /0: no more-specific match
  - Static: configured; dynamic: reachability exchange
  - Distance vector: neighbor estimates
  - Link state: distributed links, shortest paths
  - Interior protocols: within autonomous system
  - BGP: between autonomous systems
- Destination sets and distribution
  - Flooding: eligible-link copies, duplicate/lifetime controls
  - Random walk: probabilistic neighbor
  - Unicast: one; broadcast: all within scope
  - Multicast: subscribed group
  - Anycast: one shared-address member
  - Anycast nearest by routing metric
  - Multi-destination target list ≠ necessarily broadcast
  - Multicast trees: reverse-path checks
  - Ethernet spanning tree: separate layer-2 mechanism

Circuit, message and packet switching

- Circuit versus packet switching
  - Circuit: setup → reserved transfer → release
  - Predictable allocated bandwidth
  - Setup/blocking and idle reservation costs
  - Traditional telephone call
  - Packets statistically share links
  - Queueing: variable delay and loss
  - Voice-over-packet remains possible
  - Buffering; scheduling; capacity planning

- Forwarding and switching variants
  - Datagrams forwarded independently
  - Virtual circuit establishes forwarding state
  - Virtual-circuit reservation optional
  - Message switching stores complete message
  - No dedicated end-to-end message path
  - Store-and-forward waits for full packet/frame
  - Cut-through starts after sufficient header
  - Fragment-free waits collision-sensitive initial portion
  - Routing ≠ guaranteed geometrically shortest path

Multiplexing and channelization

- Multiplexing and demultiplexing
  - Multiple streams share one link
  - Receiver separates streams
  - Multiplexing ≠ broadcasting
  - FDM: frequency bands, guard spacing
  - WDM: optical wavelengths
  - TDM: time slots
  - Synchronous TDM: recurrent slots, including idle
  - Statistical TDM: demand allocation, identification
- Channelization versus port multiplexing
  - FDMA: user frequency allocation
  - TDMA: user time allocation
  - CDMA: coded-signal separation
  - Physical multiplexing ≠ transport port multiplexing
  - Combining-signals question: multiplexing
  - Missing correct option remains missing

Identify networking layers and addressing assumptions

- Ambiguous networking stems
  - Identify exact layer, protocol, scope
  - Link and transport: flow/error control

- Locally administered MAC addresses
- Bridges and switches: both layer 2
- LAN: public or private unicast
- UDP and IP: both connectionless
- Session dialog ≠ TCP connection
- Overlaps need narrower stem/multiple selections

• Damaged addressing and option questions

- Host without prefix: capacity indeterminate
- Explicit classful assumption permits default
- Subnet count requires parent block
- Obsolete zero/all-ones subnet exclusions: explicit only
- Missing concept ≠ duplicated distractor answer
- Restore OCR-damaged original options