CS Exit Ethiopia

Complete Study Notes

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 6

How to use these study notes

START01 A practical study cycle

Start with a small set of questions before reading.

Mark the exact thing that stopped you: an unknown term, a rule, a calculation, a trace or a choice between alternatives.

Use the question lookup to open the relevant section.

Read one section, close it, and explain the rule in your own words.

Solve the question again and say why each other choice fails.

Then change one assumption or input and solve the variation.

This checks understanding beyond recognition.

A useful 60-minute session: 10 minutes of cold questions, 20 minutes of focused reading, 20 minutes of closed-book solving and 10 minutes updating an error log.

Adjust the timing to your needs.

Revisit mistakes after a gap, for example the next day, several days later and the following week.

These intervals are a practical starting plan, not a fixed learning law.

Record the section ID, your mistaken rule, the corrected rule and one boundary case.

Keep the log short enough to review.

Mix related courses during revision: programming with data structures; databases with security; networking with administration.

Explain how the same word changes meaning across contexts.

START02 What to emphasize

Emphasize definitions, key differences, algorithm costs, SDLC models, databases, networking and security.

Use short oral questions to check understanding and correct common misconceptions.

Combine those habits with the tracing, calculation, design and diagnosis demanded by the Ministry learning outcomes.

Allocate revision by both exam share and your error log.

A course with fewer items can still deserve more time if your foundations are weak.

The blueprint is a planning baseline, not a prediction of exact questions.

Definitions: distinguish nearby concepts, not just their names.

Calculations: write units, formulas, assumptions and intermediate steps.

Code and SQL: check validity before tracing the text; state any changes before analyzing a corrected version.

Algorithms and protocols: know the input, decision rule, state change, termination and failure cases.

Design choices: state the criterion.

A choice can change when cost, reliability, consistency or latency matters more.

Course group	Items in the 100-item blueprint	Revision implication
Web Programming	9	Reserve extra practice for HTML, CSS, JavaScript, PHP, client/server behavior and safe data handling.
Data Structures and Algorithms	7	Trace operations and compare their assumptions and costs.
Each of the other fourteen courses	6 each	Study all sixteen; do not abandon a whole course based on a short note or an alleged repeated-question list.

START03 How to handle exam traps

Underline NOT, FALSE, BEST and EXCEPT before comparing choices.

Check whether the stem supplies enough facts to select one answer.

A long scenario is not automatically an analysis question, and a familiar answer letter is not evidence.

When code is invalid, a diagram is absent, or two choices express the same rule, identify the clarification needed before answering.

Learn the correct rule and the smallest clarification needed.

Do not memorize an arbitrary key as a universal fact.

Distinguish worst case from average case, and an upper bound from a tight bound.

Check language version, SQL dialect, addressing assumptions, graph weights and tie-breaking rules.

For subnetting and scheduling, calculate rather than guess from a familiar number.

Use timed mixed papers only after you can explain your errors.

Revisit the reading sections behind recurring mistakes.

Data Communication and Computer Networking

Complete Study Notes

NET01 | Communication components and quality

Data are raw representations; information is data interpreted for a purpose.

Communication requires a message, sender, receiver, medium and agreed protocol.

A source creates data; a transmitter converts it to a signal; a receiver reconstructs data.

Distance affects engineering but is not a sixth component.

Delivery means reaching the intended recipient; accuracy means preserving content; timeliness means meeting a deadline; jitter means variation in arrival delay.

A call can have acceptable average delay yet sound broken because of jitter.

Throughput measures achieved transfer rate, reliability measures dependable operation, and security concerns unauthorized actions.

Scalability means accommodating growth without unacceptable service degradation.

Data Communication and Computer Networking module

NET02 | Network size, access and architecture

PAN connects personal devices, such as Bluetooth accessories.

LAN covers a local building or campus; MAN spans a metropolitan region; WAN connects distant regions.

Device count alone does not determine the category.

The Internet is a global network of networks, commonly the largest example of a WAN.

An intranet serves an organization internally; an extranet exposes selected services to approved outsiders.

Neither term alone specifies geographic size.

A client requests a service; a server supplies it.

Peer systems may perform both roles.

Dedicated servers concentrate on service workloads but can still be clients of DNS, backup or update services.

A ten-user cutoff is a teaching guideline, not a technical law.

Centralization simplifies administration but creates dependencies; peer networks still need security.

Data Communication and Computer Networking module

NET03 | Protocols, standards and layers

Protocol syntax defines message structure, semantics defines field meanings, and timing defines when/how fast exchanges occur.

A standard supports interoperability.

De facto means established through use; de jure means formally approved.

ISO develops international standards; IEEE develops LAN standards such as 802.3 and 802.11; ITU-T develops telecommunications standards.

ANSI coordinates US standards, EIA is associated with interface standards, and FCC is a regulator.

A reference model divides responsibilities and interfaces; it is not itself executable networking software.

OSI is a seven-layer reference model; TCP/IP describes an implemented protocol suite, usually taught with four layers.

A five-layer teaching model separates physical and link functions.

State the model before counting layers.

Data Communication and Computer Networking module

NET04 | Signals, periods and bandwidth

Analog signals vary continuously; digital signals use discrete symbol states.

Data and signal types are separate: digital bits can modulate an analog carrier.

A sine wave has amplitude, frequency and phase.

Frequency f counts cycles/second, period $T=1/f$, and wavelength $\lambda=v/f$ depends on propagation speed v. Phase specifies displacement within a cycle.

Composite signals combine frequencies.

Frequency bandwidth is highest minus lowest frequency, measured in hertz.

A low-pass channel includes zero frequency; a band-pass channel occupies a nonzero frequency range.

Baseband sends the signal without shifting it to a carrier; passband transmission modulates a carrier.

Do not confuse hertz with bit/s, even though both are informally called bandwidth.

At 2 kHz, one period is 0.5 ms.

Data Communication and Computer Networking module

NET05 | Bit rate, baud and channel capacity

Bit rate R is bits/second; a bit interval is 1/R. Baud is symbols/second, not necessarily the number of voltage transitions.

With M equally encoded symbol states, each symbol can carry log2(M) bits; R=baud×log2(M), before coding overhead.

Binary Manchester uses extra transitions, so binary does not universally mean baud equals bit rate.

For an ideal noiseless channel, Nyquist gives R≤2B log2(M).

For Gaussian noise, Shannon gives C=B log2(1+S/N), with a linear power ratio; SNR(dB)=10 log10(S/N).

Bandwidth, signal levels and noise appear explicitly.

Distance affects attenuation, delay and often achievable rate, but is not a separate variable in these simplified capacity formulas.

Example

Worked example

- B=3000 Hz and M=4 give a 12,000 bit/s noiseless limit. If S/N=15, Shannon also gives 3000×log2(16)=12,000 bit/s. Do not insert 15 dB as a linear ratio.

University of Florida, R. Newman-Wolfe: Transmission

NET06 | Delay, impairments and transmission modes

Transmission delay is packet bits divided by link bit rate; propagation delay is distance divided by signal speed.

Processing and queueing add delay.

A 1000-byte packet takes 0.8 ms to serialize at 10 Mbit/s; increasing line rate does not reduce propagation time.

Attenuation reduces signal strength.

Distortion changes shape, often because frequencies have different delays.

Noise adds unwanted energy: thermal noise comes from random thermal motion, crosstalk leaks from nearby channels, and impulse noise is a short disturbance.

Amplifiers amplify noise too; digital repeaters regenerate decisions but cannot reconstruct every corrupted bit.

Simplex is one way, half duplex alternates directions, and full duplex permits simultaneous sending/receiving.

A walkie-talkie is half duplex; a telephone conversation uses full duplex.

Serial sends sequential bits; parallel uses multiple conductors and may suffer skew.

Character-oriented asynchronous serial adds start/stop bits; synchronous framing uses ongoing clock recovery.

Neither is synonymous with browser asynchronous requests.

Data Communication and Computer Networking module

NET07 | Cables, wireless and connectors

Twisted pairs reduce coupled interference; UTP has no added shield and STP adds shielding.

Coax has an inner conductor and outer shield sharing an axis.

Fiber guides light and resists electromagnetic interference; it supports high capacity and long reach, but requires suitable optics and installation.

Exact speed, cost and reach depend on the specification, not the material alone.

Fiber can still be tapped.

Radio, microwave and infrared are unguided media.

Ground waves follow Earth, sky waves can reflect from ionized layers, and line-of-sight paths require suitable visibility.

Microwaves are radio waves in the broader physical classification.

Infrared generally does not penetrate walls.

Directionality depends on antennas: omnidirectional means broad azimuth coverage, not equal radiation in every 3-D direction.

Legacy Ethernet straight-through cables join unlike MDI/MDI-X roles; crossover joins like roles, such as PC-PC or switch-switch.

Auto-MDI-X can remove that requirement.

Data Communication and Computer Networking module

NET08 | Topology and failure reasoning

Physical topology describes link layout; logical topology describes communication/access relationships.

Point-to-point links join two endpoints; multipoint links share a medium.

A full mesh consists of point-to-point links.

Bus uses a shared backbone; an unterminated break can disrupt the segment.

Star connects endpoints through a central device: one edge failure isolates that endpoint, whereas central failure affects the star.

Ring forms a loop; basic single rings are vulnerable to a break, while protected dual rings differ.

Token passing is associated with Token Ring but is an access method, not a necessary property of every ring.

Tree is hierarchical; hybrid combines arrangements.

A full undirected mesh of n nodes needs n(n-1)/2 links and n-1 interfaces per node.

For 50 nodes: 50×49/2=1225 links.

Redundant paths improve fault tolerance at greater cable and interface cost.

Data Communication and Computer Networking module

NET09 | NICs, repeaters and hubs

A NIC supplies a computer's network interface and commonly implements both physical and link functions.

Calling a NIC a physical interface does not mean all its functions are layer 1.

Physical specifications include connectors, signaling, voltage, timing and physical coding/modulation; the PHY interface to MAC handles hardware signaling.

A repeater regenerates layer-1 signals without inspecting destination addresses.

An active hub is a multiport repeater: it repeats incoming signals onto other ports, placing half-duplex endpoints in one collision domain.

A passive hub is a connector.

A hub neither learns MAC addresses nor eliminates collisions.

An endpoint such as a network printer consumes services; routers, hubs and access points are intermediary devices.

In the legacy IEEE 802.3 architecture with an attachment unit interface (AUI) and medium attachment unit (MAU), the MAC interfaces to the Physical Signaling (PLS) sublayer.

For this legacy MAC interface, the relevant sublayer is PLS.

This name is architecture-specific: other PHY designs use reconciliation (RS), physical coding (PCS), physical medium attachment (PMA) and related sublayers.

Do not present PLS as a universal OSI sublayer name.

IEEE 802.3 10GBASE-ER architectures, David Law

NET10 | Bridges, switches and access points

A bridge or ordinary Ethernet switch operates at layer 2.

It learns source-MAC-to-port mappings, looks up the destination, forwards a known unicast to its port, filters it if the destination is on the incoming segment, and floods an unknown unicast or broadcast within its VLAN.

A switch does not always send only to one destination port.

Wireless access points normally bridge wireless and wired link-layer traffic.

Each switch port separates collision domains; full-duplex point-to-point Ethernet has no collisions and does not use CSMA/CD.

Switching permits independent conversations simultaneously.

Broadcasts still reach the VLAN unless another control filters them.

A layer-3 switch also routes, so device marketing names do not override the function being examined.

Data Communication and Computer Networking module

NET11 | Routers, gateways and traffic controls

Routers forward IP packets between networks using destination prefixes and next hops.

They separate broadcast domains and normally do not forward local link broadcasts.

A default gateway is usually a router, while a protocol gateway can translate application formats; therefore a gateway is not inherently a device that implements every OSI layer.

A firewall allows, rejects or inspects traffic under a security policy; it does not necessarily encrypt.

A VPN, Virtual Private Network, provides a logical private connection over another network; a secure VPN authenticates/encrypts its tunnel.

A modem modulates outgoing and demodulates incoming carrier signals.

These functions may coexist in one home router but remain conceptually distinct.

Data Communication and Computer Networking module

NET12 | OSI layers and encapsulation

Sending proceeds from application data to transport segment/datagram, network packet, link frame and physical bits/symbols; receiving reverses the order.

Each layer serves the layer above.

A router removes a received link frame, inspects IP, and creates a new link frame for the next hop.

MAC addresses usually change across routed hops; end-to-end IP addresses ordinarily remain until translation.

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

Data Communication and Computer Networking module

NET13 | Link control, framing and error detection

Link-layer LLC identifies or multiplexes upper-layer protocols and may supply link control; MAC handles medium-dependent addressing/access and frame delivery.

Network addressing belongs to layer 3.

Ethernet, PPP and HDLC are link protocols.

Frame headers may carry addresses and control/type fields; synchronization and exact framing depend on the protocol.

Detection adds redundancy but does not guarantee correction.

Even parity adds a bit so the total number of ones is even: 1011 needs parity 1.

It detects every odd number of bit flips but misses even counts.

CRC treats bits as a polynomial and appends the XOR-division remainder; the receiver repeats the division.

Internet checksums add words with end-around carry and complement the sum.

A burst spans from the first corrupted bit through the last, including unchanged interior bits.

Retransmission or sufficient forward-error-correcting redundancy is needed for recovery.

Data Communication and Computer Networking module

NET14 | Access control and reliable-link procedures

Random access allows contention: ALOHA sends opportunistically; CSMA senses before sending.

In legacy half-duplex Ethernet, CSMA/CD detects collision, sends a jam indication, stops, and retries after random backoff.

The jam signals a collision, not its clearance.

Wi-Fi 802.11 uses CSMA/CA with waiting/backoff and acknowledgments; sensing does not eliminate hidden-terminal collisions.

Controlled access uses polling, reservations or a token to grant turns; correctly coordinated access avoids contention collisions.

Channelization divides frequency, time or code resources.

Stop-and-wait sends one frame and waits for ACK, retransmitting on timeout; sequence bits distinguish duplicates.

Sliding windows permit multiple unacknowledged frames.

Link reliability/flow control is hop-local; transport reliability/flow control is end-to-end.

Ethernet detects corruption but does not itself guarantee reliable delivery.

Data Communication and Computer Networking module

NET15 | Line coding, modulation and sampling

Line coding maps digital bits to digital signal patterns.

NRZ uses levels without a forced mid-bit return; Manchester supplies a mid-bit transition for clocking, with bit convention specified.

Differential Manchester encodes using transitions relative to previous state.

AMI alternates the polarity of successive ones; pseudoternary alternates zero pulses.

Block coding adds code redundancy; scrambling replaces problematic patterns without necessarily increasing bit count.

Multilevel schemes include 2B1Q and 8B6T; MLT-3 uses a sequence of voltage transitions.

ASK varies carrier amplitude, FSK frequency, PSK phase; QAM combines amplitude and phase.

AM/FM/PM can carry analog data.

PCM digitizes analog input by sampling, quantizing and encoding.

Sampling must exceed twice the highest retained baseband frequency in practical designs; b-bit samples have 2^b quantization levels and uncompressed rate fs×b. PAM/PWM are pulse modulation methods; pulse amplitude or width alone is not a binary PCM code.

Data Communication and Computer Networking module

NET16 | Network delivery and IPv4 header

IP supplies connectionless best-effort packet delivery, not end-to-end ordering or retransmission.

IPv4 addresses are 32 bits.

Its minimum header is 20 bytes and can grow to 60 bytes; it is not a 32-bit header.

IHL counts 32-bit words; total length includes header and payload.

TTL limits lifetime across routers; the protocol field identifies TCP, UDP or another upper-layer protocol.

The IPv4 checksum protects its header; IP does not lack error checking altogether.

Identification, flags and offset support fragmentation.

IPv4 sources and routers may fragment when allowed; reassembly occurs at the destination.

If DF is set and the next MTU is too small, forwarding fails and an ICMP diagnostic may be returned.

IETF RFC 791

NET17 | Transport choice, ports and connections

TCP offers a reliable ordered byte stream using sequence numbers, acknowledgments, retransmission and windows.

Flow control protects the receiver; congestion control protects network capacity.

UDP sends independent datagrams with ports and a checksum but no built-in setup, delivery guarantee, retransmission or ordering.

Live interactive traffic may choose UDP when late data is less useful than lost data.

Application protocols can add reliability over UDP.

Ports identify transport endpoints; the application can choose a transport and request socket buffer sizes, subject to OS limits.

A TCP connection is identified by source/destination IP and source/destination port, with TCP understood.

IPv4 protocol numbers identify upper protocols; 80 is a usual HTTP port, not an IP protocol number.

Clients often use ephemeral ports.

SCTP is a reliable message-oriented transport with multiple streams.

IETF RFC 9293

NET18 | Trace the TCP handshake

TCP establishes state with SYN, SYN+ACK, then ACK.

SYN consumes one sequence position even with no application bytes.

An acknowledgment states the next expected sequence number.

For client ISN=395 and server ISN=260: client sends SYN seq395; server sends SYN+ACK seq260 ack396; client sends ACK seq396 ack261.

Later byte counts advance sequence numbers.

FIN also consumes one sequence position.

TCP setup creates a logical transport connection, not a reserved physical circuit.

Ports allow multiplexing separate applications over IP; they do not combine all applications into one TCP byte stream.

Do not assign TCP reliability to all layer-4 protocols merely because the reference layer lists reliability as a possible service.

IETF RFC 9293

NET19 | Upper layers and the TCP/IP correspondence

OSI session roles establish/manage dialogs and can coordinate checkpoints so transfer resumes after interruption.

Presentation roles translate encodings and handle compression/encryption.

Compression reduces representation size; encryption hides content and need not shrink it.

Application protocols provide services directly to applications.

Practical implementations distribute these functions differently; TLS is not proof of a separate physical presentation-layer device.

The four-layer TCP/IP model folds OSI layers 5-7 into application, retains transport, calls layer 3 Internet, and combines link/physical as network access.

A model is a guide to functions, not a guarantee that every application gets a reliable network.

Distinguish end-to-end application service from its underlying process-to-process transport.

Data Communication and Computer Networking module

NET20 | DNS, DHCP and address resolution

DNS resolves names to records, including IPv4 A and IPv6 AAAA addresses; it can use UDP or TCP port 53.

DHCP dynamically leases IPv4 settings, commonly address, mask, gateway and DNS server.

Its basic exchange is discover, offer, request, acknowledge.

IP itself does not assign addresses.

ARP resolves an on-link IPv4 next hop to a link address, using a broadcast request and normally unicast reply.

For an off-subnet target, ARP resolves the gateway, not the remote target's MAC.

It bridges the network/link addressing boundary and is often classified at the link layer; calling ARP simply a network protocol uses a loose textbook convention.

RARP reverses hardware-to-IP lookup; BOOTP/DHCP support boot configuration.

ICMP reports errors and diagnostics; IGMP manages IPv4 multicast membership.

These are separate companion protocols, not four pieces whose combination is IP.

IETF RFC 826

NET21 | Web, file, mail and remote-login protocols

HTTP defines web request/response semantics; it is stateless, and a message body may be absent.

HTTPS adds TLS protection.

FTP transfers files using control and separate data connections; it is not the same protocol as SFTP.

SMTP submits and relays mail; POP3 retrieves messages and IMAP accesses/synchronizes server mailboxes.

Saying SMTP handles both sending and end-user mailbox retrieval is inaccurate.

Usual service ports: FTP control 21, SSH 22, Telnet 23, SMTP relay 25, DNS 53, HTTP 80, POP3 110, IMAP 143, HTTPS 443.

Telnet provides unencrypted remote terminals; SSH protects remote access.

Servers can be configured on other ports.

A browser's HTTP exchange does not determine the physical duplex mode of its network interface.

Data Communication and Computer Networking module

NET22 | IPv4 notation and classful defaults

Write IPv4 as four decimal octets 0-255, or as 32 binary bits.

Use weights 128,64,32,16,8,4,2,1 within each octet.

Thus 11000001 10000011 00011011 11111111 is 193.131.27.255.

A value such as 257 is impossible.

Syntactic validity differs from assignability: an address ending .0 or .255 can be a host under some prefixes.

Historical classes use leading patterns: A 0 with /8, B 10 with /16, C 110 with /24; D 1110 is multicast and E 1111 reserved.

Ordinary class-A first octets are 1-126 because 0 and 127 have special uses.

B spans 128-191 and C 192-223.

Default usable counts are 2^24-2, 2^16-2 and 254.

Modern CIDR requires the actual prefix and overrides class defaults.

Data Communication and Computer Networking module

NET23 | Special ranges, private addresses and IPv6

RFC1918 private blocks are 10.0.0.0/8, 172.16.0.0/12 (through 172.31.255.255), and 192.168.0.0/16.

They can be reused internally but are not globally routed as public destinations.

A LAN may also use legitimately assigned public addresses; private is common, not mandatory. 127.0.0.0/8 is IPv4 loopback, commonly 127.0.0.1, for local protocol access without an external link. 255.255.255.255 is limited broadcast; 0.0.0.0 can identify an unconfigured source.

Link-local/APIPA uses 169.254.0.0/16, with edge /24 blocks excluded from normal automatic selection.

IPv6 has 128-bit hexadecimal addresses, flexible prefixes and no IPv4-style broadcast.

Sources, not routers, fragment IPv6 packets.

IPv6 does not automatically encrypt traffic or make authentication unnecessary.

Compare IPv6’s larger 128-bit address space and encryption support separately; specify the property being evaluated.

IETF RFC 1918

IETF RFC 8200

NET24 | Masks, prefixes and binary AND

A /p IPv4 prefix has p leading one bits followed by 32-p zeros.

Partial octet masks are 128,192,224,240,248,252,254. /19 is 255.255.224.0; /20 is 255.255.240.0; /21 is 255.255.248.0, correcting the study guide’s 255.248.0.0 mistake.

Compute network=address AND mask.

Host bits zero identify the block start; host bits one give broadcast.

With 172.16.28.252/20, the third octet is grouped in blocks of 16, so the network is 172.16.16.0 and broadcast 172.16.31.255.

A written host/prefix such as 172.105.180.0/21 need not be an aligned block label: masking yields 172.105.176.0/21.

Data Communication and Computer Networking module

NET25 | Find subnet bounds and usable hosts

For ordinary broadcast LANs let h=32-p. Total addresses=2^h; usable hosts=2^h-2, reserving network and directed broadcast.

Find the changing octet's increment as 256-mask octet, round the address down to a multiple, and extend through the next boundary minus one.

192.168.2.64/26 spans .64-.127; usable .65-.126 gives 62 hosts. 192.168.10.25/28 spans .16-.31, so its network is .16. 172.17.128.0/21 spans 172.17.128.0-172.17.135.255; .128.255 and .135.0 are valid interior hosts, but .135.255 is broadcast. /27 gives 32 total and 30 usable, not 32 usable.

Data Communication and Computer Networking module

NET26 | Borrow bits and choose a mask

To split parent /a into equal /p blocks, borrow b=p-a bits and obtain 2^b subnets.

Do not subtract two subnets under modern practice.

For a Class B /16 parent split to /19, b=3 gives eight subnets, each with 8192 addresses and 8190 conventional hosts.

A /19 alone does not state its parent.

For H hosts, choose the smallest h satisfying 2^h-2≥H, then p=32-h. For 24 hosts use /27; 52 or 57 use /26; 100 use /25; 500 use /23.

For at least six equal subnets choose b=3.

A Class C /24 split to /27 yields eight subnets.

Always check both the number of subnets and the host capacity.

Data Communication and Computer Networking module

NET27 | Design and implement a VLSM address plan

VLSM assigns different masks to different LAN sizes.

Sort demands largest first, round each to a power-of-two address block including reservations, allocate aligned nonoverlapping blocks within the parent, and leave the remaining space explicit.

For a /24 with LAN demands 100,60,29: allocate .0/25 (hosts .1-.126), .128/26 (.129-.190), and .192/27 (.193-.222); .224/27 remains.

Two remote LANs of 100 each fit .0/25 and .128/25 within a separate /24.

Count router interfaces as hosts if not already included in the demand.

Implementation assigns unique usable IPs/masks, puts each default gateway in its local subnet, configures router interfaces/routes and DHCP exclusions, then tests local reachability, gateway reachability, remote routing and DNS separately.

Check duplicate addresses, overlap and return routes before blaming an application.

Data Communication and Computer Networking module

NET28 | Point-to-point links and route aggregation

A conventional /30 has four addresses and two usable endpoints; check the link and addressing assumptions when selecting a WAN prefix.

RFC3021 permits /31 on supported point-to-point links: both addresses are endpoints, so the subtract-two rule does not apply. /32 identifies one address/host route.

Do not claim /30 is universally the smallest valid link prefix.

CIDR, Classless Inter-Domain Routing, replaces rigid class allocation and supports aggregation.

Combine contiguous aligned blocks sharing leading bits; unrelated adjacent-looking labels may not aggregate cleanly.

Four consecutive /26 blocks covering a /24 summarize to /24.

More-specific routes must remain available where the aggregate would otherwise send traffic to the wrong next hop.

IETF RFC 3021

IETF RFC 4632

NET29 | NAT and port translation

Static NAT gives a fixed address mapping; dynamic NAT allocates mappings from a pool.

PAT/NAPT maps address-plus-port combinations so multiple private clients share a public address.

It is translation, not ARP resolution and not encryption.

Return traffic must match the translation state or a configured inbound mapping.

A private host such as 10.0.0.1 commonly reaches the public Internet through NAT at a gateway, together with valid routing and a public external address.

NAT alone does not supply a physical connection or DNS.

A public address does not automatically grant permission to use it; both public and private unicast addresses can be used on a LAN under the correct allocation and subnet.

Data Communication and Computer Networking module

NET30 | Routing algorithms and destination sets

Routing computes paths; forwarding chooses a next hop for an individual packet.

Select the matching route with the longest prefix, then apply the routing system's tie-breaking criteria.

A default /0 matches when nothing more specific does.

Static routes are configured; dynamic protocols exchange reachability.

Distance vector uses neighbor estimates, while link state distributes link information and computes shortest paths.

Interior protocols operate within an autonomous system; BGP exchanges routes between systems.

Flooding sends copies on eligible outgoing links with duplicate/lifetime controls; random walk picks a neighbor probabilistically.

Unicast targets one destination, broadcast all in a scope, multicast a subscribed group and anycast one member sharing an address, normally nearest under routing metrics.

Multi-destination packets can list multiple targets; this is not necessarily identical to broadcast.

Group multicast trees use mechanisms such as reverse-path checks; Ethernet spanning tree is a different layer-2 mechanism.

Data Communication and Computer Networking module

NET31 | Circuit, message and packet switching

Circuit switching sets up a path with reserved resources, transfers data, then releases it.

Predictable allocated bandwidth trades against setup/blocking and wasted reservation during silence.

A traditional telephone call is the standard example.

Packet switching divides data into packets that share links statistically; queueing can add variable delay and loss.

This does not make modern voice-over-packet impossible: buffering, scheduling and capacity planning manage it.

Datagram packets are forwarded independently.

Virtual circuits establish forwarding state, but resource reservation is optional, not a necessary property of every virtual circuit.

Message switching stores a complete message before forwarding, without a dedicated end-to-end path.

Packet store-and-forward waits for the full packet/frame; cut-through starts after enough header arrives; fragment-free historically waits through the initial collision-sensitive portion.

No routing algorithm guarantees that every packet always takes the geometrically shortest route.

Data Communication and Computer Networking module

NET32 | Multiplexing and channelization

Multiplexing combines multiple input streams onto a shared link; demultiplexing separates them at the receiver.

It differs from broadcasting one message to many destinations.

FDM assigns distinct frequency bands with suitable guard spacing; WDM assigns different optical wavelengths.

TDM allocates time slots: synchronous TDM reserves recurrent slots even if an input is idle, while statistical TDM allocates according to demand and needs identification.

FDMA and TDMA allocate frequencies or time among users; CDMA separates coded signals.

Physical multiplexing is different from transport port multiplexing.

Combining signals onto a shared link is multiplexing; distinguish it from point-to-point connectivity, broadcast, synchronization and multicast.

Data Communication and Computer Networking module

NET33 | Identify networking layers and addressing assumptions

First identify the exact layer, protocol and scope.

Flow/error control can exist at both link and transport layers; MAC addresses can be locally administered; bridges and switches both operate at layer 2.

A LAN can use public or private unicast space.

UDP and IP are both connectionless.

Session dialogs and TCP connections are distinct senses of connection.

Distinguish the protocol, layer and scope before treating these descriptions as exclusive.

A host address without a prefix does not determine capacity unless the question explicitly assumes historical classful addressing.

A subnet count needs a parent block.

Excluding subnet zero and the all-ones subnet is an obsolete convention; apply it only when explicitly stated.

Choose a networking concept by its definition rather than by repeated distractors.

Read complete, unambiguous option labels before matching them to networking concepts.

Data Communication and Computer Networking module

NET-S01 | Independent routing classifications

Adaptive or dynamic routing changes routes in response to updated network information; nonadaptive or static routing uses configured choices. Distributed routing means routers perform computations using exchanged information instead of requiring one central route computation. These properties do not imply random next-hop selection: the path-selection rule is a separate classification.

Data Communication and Computer Networking module · page 19

RFC 1058 - Distance-vector computation and topology changes

NET-S02 | Management, traffic service and application transport bindings

SNMP means Simple Network Management Protocol. Its management applications monitor and control managed devices, such as hosts and routers, by exchanging management information with their agents. This device-management role differs from transferring email, resolving names or mapping an IP address to a MAC address.

In the conventional service bindings, FTP control, SMTP mail transfer and Telnet remote terminals use TCP. DNS supports both UDP and TCP on port 53; it is not exclusively a UDP service. The application protocol's service role is distinct from the transport carrying its messages.

Quality of service (QoS) controls traffic treatment to meet objectives such as throughput, delay, jitter or loss. Classification, queue scheduling and allocation of buffer or bandwidth resources implement such treatment. QoS concerns delivered service behavior; scalability concerns accommodating growth, and security concerns unauthorized actions.

RFC 3411 - SNMP architecture, section 1.2

Data Communication and Computer Networking module · page 28

RFC 2475 - Differentiated-services architecture

NET-S03 | Why IPv4 conservation and IPv6 matter

The finite IPv4 address space has faced allocation scarcity. Private addressing with NAT conserves public IPv4 addresses, while IPv6 provides a much larger address space.

Data Communication and Computer Networking module · page 19

NET-S04 | Computer networks and network interfaces

A computer network connects computers or other devices so they can exchange information and share resources such as files, storage and printers. The interconnection uses both hardware and software; neither hardware alone nor software alone is the definition of the whole network.

NIC expands to Network Interface Card. It is the host's network interface, providing the connection through which the host sends and receives network signals. A cable connector attaches the medium to that interface; it is distinct from an intermediary switch or router.

CRC expands to Cyclic Redundancy Check.

Data Communication and Computer Networking module · page 22

Data Communication and Computer Networking module · page 23

Data Communication and Computer Networking module · page 13

NET-S05 | Network-access technologies and geographic use

Ethernet and Token Ring are traditional LAN technologies. X.25 and Frame Relay are traditional WAN technologies. TCP/IP can run over different network-access technologies; its Internet-layer packet service does not require one particular link medium or frame format.

Data Communication and Computer Networking module · page 26

NET-S06 | Interface addresses and transport-number namespaces

An IP address identifies a network interface rather than limiting a whole computer to one address. A computer or router can have several interfaces and addresses. Under a supplied IPv4 prefix, leading bits identify the network and the remaining bits identify an address within that network; a MAC address is a separate link-layer identifier.

TCP and UDP port fields are 16 bits, allowing numbers from 0 through 65535. Well-known ports are 0-1023, registered ports are 1024-49151, and dynamic/private ports are 49152-65535. Client endpoints can use dynamically selected ports instead of every application requiring a well-known assignment. These port numbers are distinct from the IP version and upper-protocol fields.

A bridge or switch's MAC address table is its learned forwarding database: it associates MAC addresses with ports for frame forwarding. It differs from an ARP cache, which associates an IPv4 next hop with a link address, and from a routing table, which selects next hops for IP prefixes.

A common IPv6 unicast subnet uses a 64-bit subnet prefix and a 64-bit interface identifier. This split does not make the complete address 64 bits: it remains 128 bits. Special uses and explicitly different prefix lengths must be considered separately.

Data Communication and Computer Networking module · page 18

Data Communication and Computer Networking module · page 28

Cisco - Configure MAC address learning and forwarding tables

RFC 7421 - Analysis of the 64-bit boundary in IPv6 addressing

NET-S07 | Physical signaling and legacy Ethernet cable roles

Fiber-optic links can use near-infrared light. The selected optical wavelength is part of the link's physical signaling specification, just as connectors and electrical signal levels are physical-interface specifications. This does not require every fiber link to use the same wavelength.

For legacy fixed Ethernet port roles, PCs and router Ethernet endpoints use the same endpoint role, while ordinary switch ports use the opposite role. Thus a direct router-to-PC link uses crossover wiring; PC-to-switch or router-to-switch uses straight-through wiring. Automatic MDI-X can remove the need to choose the crossover manually.

Ethernet switches can have fiber-optic interfaces with suitable optical transceivers. A forwarding role therefore does not impose a copper-only restriction: distinguish what the device does with frames from the physical medium used by its ports.

Intermodulation distortion occurs when multiple signals interact through a nonlinear component and generate unwanted combination-frequency products. Its mechanism differs from random thermal motion, adjacent-channel leakage and an isolated impulse disturbance.

Cisco - Introduction to Optical Fibers, dB, Attenuation and Measurements

Data Communication and Computer Networking module · page 14

Cisco Press - Switch Speeds and Forwarding Methods

Cisco - Configuring interface characteristics and auto-MDI-X

Cisco - Troubleshoot fiber links on Catalyst 9000 series switches

National Instruments - Nonlinearity testing using multitone generation