

1									
2									
3									
4									
5									
6									
7									
8									
9									
0	X								

Registration number

--

Signature

Note:

- Cross your immatriculation number in the crossboxes. It will be evaluated automatically.
- Sign in the signature field.
- Allowed tools are only a pocket calculator and an analog dictionary English ↔ native language without notes.
- Potentially helpful information from the cheat sheet is printed at the page ends.
- Do not write with red or green colors nor use pencils.

This quiz contains multiple choice/multiple answer sub-tasks, i.e. at least one answer option is correct in each case. These sub-tasks are scored with 1 point per correct answer and –1 point per incorrect answer. Missing answers have no effect. The minimum score per sub-task is 0 points.

Do not open the quiz until the start of the working time was announced!

Routing

In the following subtasks we consider a router that should forward a packet with Longest Prefix Matching (LPM).

Entry	Destination	Next-Hop	Iface
①	10.0.0.0/24	192.168.2.254	eth2
②	192.168.1.0/24	0.0.0.0	eth1
③	192.168.2.0/24	0.0.0.0	eth2
④	10.0.0.0/8	192.168.2.254	eth2

Table 1.1: Routing Table A

a)* Using **Routing Table A**, which entry will be selected to forward a packet with destination address 10.0.20.5?

☐ ① ☐ ② ☐ ③ ☒ ④ ☐ none

b)* Using **Routing Table A**, which entry will be selected to forward a packet with destination address 172.18.3.55?

☐ ① ☐ ② ☐ ③ ☐ ④ ☒ none

c)* Is there an entry that can be omitted from **Routing Table A** without affecting the result of forwarding decisions, and if so, which one?

☒ ① ☐ ② ☐ ③ ☐ ④ ☐ not possible

Entry	Destination	Next-Hop	Iface
⑤	172.17.0.0/28	0.0.0.0	eth1
⑥	192.168.0.0/25	172.17.0.2	eth1
⑦	192.168.128.0/25	0.0.0.0	eth2
⑧	192.168.0.0/17	0.0.0.0	eth3

Table 1.2: Routing Table B

d)* Using **Routing Table B**, which entry will be selected to forward a packet with destination address 172.17.0.1?

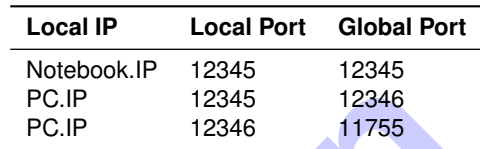
☒ ⑤ ☐ ⑥ ☐ ⑦ ☐ ⑧ ☐ none

e)* Using **Routing Table B**, which entry will be selected to forward a packet with destination address 192.168.0.254?

☐ ⑤ ☐ ⑥ ☐ ⑦ ☒ ⑧ ☐ none

dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary	dec	hex	binary
0	00	00000000	16	10	00010000	32	20	00100000	48	30	00110000	64	40	01000000	80	50	01010000	96	60	01100000	112	70	01110000	128	80	10000000	144	90	10010000
1	01	00000001	17	11	00010001	33	21	00100001	49	31	00110001	65	41	01000001	81	51	01010001	97	61	01100001	113	71	01110001	129	81	10000001	145	91	10010001
2	02	00000010	18	12	00010010	34	22	00100010	50	32	00110010	66	42	01000010	82	52	01010010	98	62	01100010	114	72	01110010	130	82	10000010	146	92	10010010
3	03	00000011	19	13	00010011	35	23	00100011	51	33	00110011	67	43	01000011	83	53	01010011	99	63	01100011	115	73	01110011	131	83	10000011	147	93	10010011
4	04	00000100	20	14	00010100	36	24	00100100	52	34	00110100	68	44	01000100	84	54	01010100	100	64	01100100	116	74	01110100	132	84	10000100	148	94	10010100
5	05	00000101	21	15	00010101	37	25	00100101	53	35	00110101	69	45	01000101	85	55	01010101	101	65	01100101	117	75	01110101	133	85	10000101	149	95	10010101
6	06	00000110	22	16	00010110	38	26	00100110	54	36	00110110	70	46	01000110	86	56	01010110	102	66	01100110	118	76	01110110	134	86	10000110	150	96	10010110
7	07	00000111	23	17	00010111	39	27	00100111	55	37	00110111	71	47	01000111	87	57	01010111	103	67	01100111	119	77	01110111	135	87	10000111	151	97	10010111
8	08	00001000	24	18	00011000	40	28	00101000	56	38	00111000	72	48	01001000	88	58	01011000	104	68	01101000	120	78	01111000	136	88	10001000	152	98	10011000
9	09	00001001	25	19	00011001	41	29	00101001	57	39	00111001	73	49	01001001	89	59	01011001	105	69	01101001	121	79	01111001	137	89	10001001	153	99	10011001
10	0a	00001010	26	1a	00011010	42	2a	00101010	58	3a	00111010	74	4a	01001010	90	5a	01011010	106	6a	01101010	122	7a	01111010	138	8a	10001010	154	9a	10011010
11	0b	00001011	27	1b	00011011	43	2b	00101011	59	3b	00111011	75	4b	01001011	91	5b	01011011	107	6b	01101011	123	7b	01111011	139	8b	10001011	155	9b	10011011
12	0c	00001100	28	1c	00011100	44	2c	00101100	60	3c	00111100	76	4c	01001100	92	5c	01011100	108	6c	01101100	124	7c	01111100	140	8c	10001100	156	9c	10011100
13	0d	00001101	29	1d	00011101	45	2d	00101101	61	3d	00111101	77	4d	01001101	93	5d	01011101	109	6d	01101101	125	7d	01111101	141	8d	10001101	157	9d	10011101
14	0e	00001110	30	1e	00011110	46	2e	00101110	62	3e	00111110	78	4e	01001110	94	5e	01011110	110	6e	01101110	126	7e	01111110	142	8e	10001110	158	9e	10011110
15	0f	00001111	31	1f	00011111	47	2f	00101111	63	3f	00111111	79	4f	01001111	95	5f	01011111	111	6f	01101111	127	7f	01111111	143	8f	10001111	159	9f	10011111

In the following subtasks, we inspect an *HTTPS 1.1 GET Response* **sent from the server SRV to the PC**. It is sent in response to a request made to the URL `https://cns.net.in.tum.de`. The router **R** performs NAT with the NAT-Table given next to the topology. The first entry in the NAT-Table was caused by a no longer connected notebook. We use the notation *device[.interface].address_type* to refer to the IP/MAC address of an interface of a specific device (e.g. *R7.wan5.IP* or *SRV.MAC*).



- Now we inspect the effect of the **router R** on the packet from point **P2** to point **P3**.

- 1)* Which protocol is used **above** the Transport Layer in a typical *HTTPS 1.1 GET Response*?

- | dec | hex | binary | dec | hex | binary | dec | hex | binary | dec | hex | binary | dec | hex | binary | dec | hex | binary | dec | hex | binary | | | |
|-----|-----|----------|-----|-----|----------|-----|-----|----------|-----|-----|----------|-----|-----|----------|-----|-----|----------|-----|-----|----------|-----|----|----------|
| 128 | 80 | 10000000 | 144 | 90 | 10010000 | 160 | a0 | 10100000 | 176 | b0 | 10110000 | 192 | c0 | 11000000 | 208 | d0 | 11010000 | 224 | e0 | 11100000 | 240 | f0 | 11110000 |
| 129 | 81 | 10000001 | 145 | 91 | 10010001 | 161 | a1 | 10100001 | 177 | b1 | 10110001 | 193 | c1 | 11000001 | 209 | d1 | 11010001 | 225 | e1 | 11100001 | 241 | f1 | 11110001 |
| 130 | 82 | 10000010 | 146 | 92 | 10010010 | 162 | a2 | 10100010 | 178 | b2 | 10110010 | 194 | c2 | 11000010 | 210 | d2 | 11010010 | 226 | e2 | 11100010 | 242 | f2 | 11110010 |
| 131 | 83 | 10000011 | 147 | 93 | 10010011 | 163 | a3 | 10100011 | 179 | b3 | 10110011 | 195 | c3 | 11000011 | 211 | d3 | 11010011 | 227 | e3 | 11100011 | 243 | f3 | 11110011 |
| 132 | 84 | 10000100 | 148 | 94 | 10010100 | 164 | a4 | 10100100 | 180 | b4 | 10110100 | 196 | c4 | 11000100 | 212 | d4 | 11010100 | 228 | e4 | 11100100 | 244 | f4 | 11110100 |
| 133 | 85 | 10000101 | 149 | 95 | 10010101 | 165 | a5 | 10100101 | 181 | b5 | 10110101 | 197 | c5 | 11000101 | 213 | d5 | 11010101 | 229 | e5 | 11100101 | 245 | f5 | 11110101 |
| 134 | 86 | 10000110 | 150 | 96 | 10010110 | 166 | a6 | 10100110 | 182 | b6 | 10110110 | 198 | c6 | 11000110 | 214 | d6 | 11010110 | 230 | e6 | 11100110 | 246 | f6 | 11110110 |
| 135 | 87 | 10000111 | 151 | 97 | 10010111 | 167 | a7 | 10100111 | 183 | b7 | 10110111 | 199 | c7 | 11000111 | 215 | d7 | 11010111 | 231 | e7 | 11100111 | 247 | f7 | 11110111 |
| 136 | 88 | 10001000 | 152 | 98 | 10011000 | 168 | a8 | 10101000 | 184 | b8 | 10111000 | 200 | c8 | 11001000 | 216 | d8 | 11011000 | 232 | e8 | 11101000 | 248 | f8 | 11111000 |
| 137 | 89 | 10001001 | 153 | 99 | 10011001 | 169 | a9 | 10101001 | 185 | b9 | 10111001 | 201 | c9 | 11001001 | 217 | d9 | 11011001 | 233 | e9 | 11101001 | 249 | f9 | 11111001 |
| 138 | 8a | 10001010 | 154 | 9a | 10011010 | 170 | aa | 10101010 | 186 | ba | 10111010 | 202 | ca | 11001010 | 218 | da | 11011010 | 234 | ea | 11101010 | 250 | fa | 11111010 |
| 139 | 8b | 10001011 | 155 | 9b | 10011011 | 171 | ab | 10101011 | 187 | bb | 10111011 | 203 | cb | 11001011 | 219 | db | 11011011 | 235 | eb | 11101011 | 251 | fb | 11111011 |
| 140 | 8c | 10001100 | 156 | 9c | 10011100 | 172 | ac | 10101100 | 188 | bc | 10111100 | 204 | cc | 11001100 | 220 | dc | 11011100 | 236 | ec | 11101100 | 252 | fc | 11111100 |
| 141 | 8d | 10001101 | 157 | 9d | 10011101 | 173 | ad | 10101101 | 189 | bd | 10111101 | 205 | cd | 11001101 | 221 | dd | 11011101 | 237 | ed | 11101101 | 253 | fd | 11111101 |
| 142 | 8e | 10001110 | 158 | 9e | 10011110 | 174 | ae | 10101110 | 190 | be | 10111110 | 206 | ce | 11001110 | 222 | de | 11011110 | 238 | ee | 11101110 | 254 | fe | 11111110 |
| 143 | 8f | 10001111 | 159 | 9f | 10011111 | 175 | af | 10101111 | 191 | bf | 10111111 | 207 | cf | 11001111 | 223 | df | 11011111 | 239 | ef | 11101111 | 255 | ff | 11111111 |

TCP, DNS and Security

m)* What is correct regarding **congestion control**?

- | | |
|---|---|
| <input type="checkbox"/> Attempts to increase load at the sender | <input type="checkbox"/> Attempts to prevent overload at the receiver |
| <input type="checkbox"/> Adjusts the receive window | <input checked="" type="checkbox"/> Adjusts the send window |
| <input type="checkbox"/> Attempts to prevent overload at the sender | <input checked="" type="checkbox"/> Attempts to prevent overload in the network |

n)* What is the correct PTR record for the IPv4 address 188.95.232.13 that is reachable under the domain name `cns.net.in.tum.de`. (TTL and Class are omitted)?

- | | | |
|---|-----|-----------------------------|
| <input type="checkbox"/> 188.95.232.13.in-addr.arpa. | PTR | cns.net.in.tum.de. |
| <input checked="" type="checkbox"/> 13.232.95.188.in-addr.arpa. | PTR | cns.net.in.tum.de. |
| <input type="checkbox"/> cns.net.in.tum.de. | PTR | 188.95.232.13.in-addr.arpa. |
| <input type="checkbox"/> de.tum.in.net.cns. | PTR | 188.95.232.13 |

o)* What is correct regarding **symmetric** encryption?

- | | |
|---|--|
| <input type="checkbox"/> Does not require a secure key exchange | <input type="checkbox"/> Usually quite slow |
| <input type="checkbox"/> Uses a pair of keys | <input type="checkbox"/> The key is publicly available |
| <input checked="" type="checkbox"/> Usually very fast | <input checked="" type="checkbox"/> Implicitly guarantees integrity in a limited way |

p)* Which of the following properties are desirable properties of a cryptographic hash function?

- | | |
|---|--|
| <input type="checkbox"/> Variable-Length Output | <input type="checkbox"/> Reversibility |
| <input checked="" type="checkbox"/> Collision Resistance | <input type="checkbox"/> Input Similarity Preservation |
| <input checked="" type="checkbox"/> Second Pre-Image Resistance | <input type="checkbox"/> Pre-Image Preservation |

q)* Which of these hash functions should **not** be used for cryptography under any circumstances?

- | | | |
|---|---------------------------------|---|
| <input checked="" type="checkbox"/> MD5 | <input type="checkbox"/> BLAKE3 | <input type="checkbox"/> BLAKE2 |
| <input type="checkbox"/> SHA-3 | <input type="checkbox"/> SHA-2 | <input type="checkbox"/> KangarooTwelve |

IP Protocol and Next Header Numbers					
No / NH		Protocol			
0x01		ICMPv4 (Internet Control Message P.)			
0x06		TCP (Transmission Control Protocol)			
0x11		UDP (User Datagram Protocol)			
0x2c		Fragment Header			
0x2f		GRE (General Routing Encapsulation)			
0x3a		ICMPv6 (ICMP for IPv6)			
0x3b		No Next Header			
0x84		SCTP (Stream Control Transmission P.)			

Selected well-known Ports											
Port		Service Name		Port		Service Name		Port		Service Name	
20		ftp (data)		53		domain (dns)		115		sftp	
21		ftp (command)		67		bootps/dhcp server		143		imap	
22		ssh		68		bootpc/dhcp client		443		https	
23		telnet		69		tftp		514		syslog	
25		smtp		80		http		546		dhcpv6-client	
43		whois		110		pop3		547		dhcpv6-server	

Application Layer - DNS	
DNS Resource Records	
Record Type	Function
SOA	(Start of Authority) marks the root of a zone
NS	specifies the FQDNs of authoritative name servers of a zone
A	associates an FQDN with an IPv4 address
AAAA	associates an FQDN with an IPv6 address
CNAME	Alias that maps to a „Canonical Name“ which itself is an FQDN
MX	associates an FQDN with a mail server
TXT	associates an FQDN with a string (text)
PTR	associates an IPv4 or IPv6 address with an FQDN (Reverse DNS)

Reverse DNS Zones	
IPv4: in-addr.arpa., IPv6: ip6.arpa.	