Chair of Distributed Systems and Security
School of Computation, Information and Technology
Technical University of Munich

1
2
3
4
5
6
7
8
9
0

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 formulas from the cheat sheet are printed at the backside.
- 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.

a)* What is true regarding wireless security?

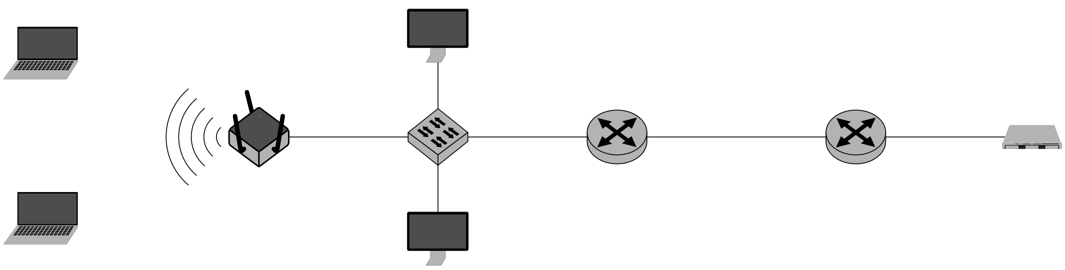
☐ Secure communication is never possible in a public WiFi network.

☐ An authenticated, but malicious host can perform denial of service attacks through deauthentication.

☐ Encrypted management frames prevent all denial of service attacks on wireless networks.

b)* What is true regarding the MAC address `2d:44:00:af:de:12`?

☐ Locally administered and Unicast ☐ Locally administered and Multicast ☐ Global unique and Unicast ☐ Global unique and Multicast



c)* How many collision domains are there in the network shown above?

☐ 2 ☐ 8 ☐ 5 ☐ 1 ☐ 4 ☐ 3 ☐ 7 ☐ 6

d)* How many broadcast domains are there in the network shown above?

☐ 7 ☐ 5 ☐ 6 ☐ 0 ☐ 4 ☐ 3 ☐ 2 ☐ 1

e)* Argue, whether collisions can occur in the **wired** part of the network shown above, which uses FastEthernet.

0
1

f)* Which frame boundary detection method must explicitly take care of code transparency?

☐ Frame buffering ☐ Code rule violations ☐ Bounding fields ☐ Control characters using the 4B4B code g)* What is true regarding media access and frame formats in WiFi?

- [ ] RTS/CTS can largely but not fully prevent collisions.
- [ ] Frames are typically shorter in WiFi because of the higher bit error probability.
- [ ] Frames are typically longer in WiFi because the media access takes more effort.
- [ ] All WiFi frames are always explicitly acknowledged on layer 2.

h)* How many usable host addresses are in the network 10.184.0.0/17?

- [ ] 15
- [ ] 32766
- [ ] 32768
- [ ] 17
- [ ] 65534
- [ ] 16384

i)* What is the broadcast address of the network corresponding to the host address 10.0.8.85/28?

- [ ] 10.0.8.80/28
- [ ] 10.0.8.85/28
- [ ] 10.0.8.95/28
- [ ] 10.0.8.87/28
- [ ] 10.0.8.91/28

Next we discuss a CRC calculation. An algorithm uses the reduction polynomial $r(x) = x^2 + x + 1$ to secure the message polynomial $m(x) = x^5 + x^3 + x + 1$.

j)* How long is the resulting CRC in bit?

- [ ] 6
- [ ] 0
- [ ] 5
- [ ] 4
- [ ] 3
- [ ] 2
- [ ] 1
- [ ] 7

k)* What is the binary representation of the message polynomial $m(x)$?

l) Calculate the checksum that is used to secure the message using the algorithm explained in the lecture.
Note: You do not need to determine the result of the division.

Checksum:

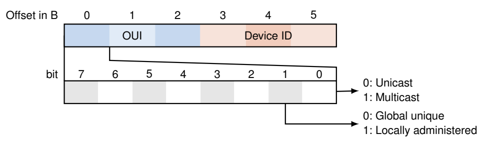
Cyclic redundancy check (CRC): addition = XOR

Checksum: $c(x) = m(x)x^n \bmod r(x)$, where $n = \deg r(x)$

Sent message: $s(x) = m(x)x^n + c(x)$

Verification: $c'(x) = (s(x) + e(x)) \bmod r(x) \overset{!}{=} 0$, with error pattern $e(x)$

Structure of MAC addresses according to IEEE 802 standards (e.g. Ethernet, WiFi, Bluetooth):



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