Computer Networks

Exercise Session 08

Prof. Dr. Oliver Hahm

Frankfurt University of Applied Sciences
Faculty 2: Computer Science and Engineering
oliver.hahm@fb2.fra-uas.de
https://teaching.dahahm.de

December 16, 2022

General Schedule

All exercises will follow this general schedule

- Identify potential understanding problems
  $\rightarrow$ Ask your questions
  $\rightarrow$ Recap of the lecture
- Address the understanding problems
  $\rightarrow$ Answer your questions
  $\rightarrow$ Repeat certain topics
- Walk through the exercises/solutions $\rightarrow$ Some hints and guidance
  $\rightarrow$ Work time or presentation of results

IP Packet Structure

You have seen . . .

- the packet structure of IPv4 packets
- the packet structure of IPv6 packets

ICMP

You have seen ...

- the purpose of the Internet Control Message Protocol
- typical situations where ICMP messages are sent
- which ICMP message types are frequently used

Address Autoconfiguration

You have seen ...

- how to use Reverse ARP to automatically configure IPv4 addresses
- DHCP was introduced as a more feature-reach replacement
- that in any case a device may generate a link-local address
- how SLAAC is used for IPv6 networks to autoconfigure a network device

Inter-Networking

You have seen ...

- how different networks are connected via a router
- which mechanisms are involved when forwarding a packet to a different network
- what an AS is
- the difference between routing and forwarding

Routing Schemes

You have seen . . .

- the requirements for a routing protocol
- how routing algorithms can be categorized
- flooding and hot-potato as examples for local routing algorithms
- the difference between source routing and hop-by-hop routing
- the difference between reactive and proactive routing algorithms
- how metrics are used to calculate the path costs

Exercise 1: Error Control

1. An upper-layer packet is split into 16 frames, each of which has a 75 percent chance of arriving undamaged. If no error control is done by the data link protocol, how many frames are required to be sent on average to get the entire thing through?

Exercise 1: Error Control

1. An upper-layer packet is split into 16 frames, each of which has a 75 percent chance of arriving undamaged. If no error control is done by the data link protocol, how many frames are required to be sent on average to get the entire thing through?
   - The probability for the first frame to arrive error-free at the destination is $75\,\% = 0.75$
   - The probability that both of the first two frames are received without an error is $0.75 * 0.75 = 0.5625 = 56.25\,\%$
   - The probability that all first three frames arrive error-free is $0.75 * 0.75 * 0.75 = 0.75^3 = 42.1875\,\%$

   ⇒ the probability that all $n = 16$ frames arrive undamaged is $p = 0.75^{16} \approx 1\,\%$!
   - $E = n * \frac{1}{p} \approx 16 * 99.77 \approx 1596$

Exercise 1: Error Control

1. An upper-layer packet is split into 16 frames, each of which has a 75 percent chance of arriving undamaged. If no error control is done by the data link protocol, how many frames are required to be sent on average to get the entire thing through?
   - The probability for the first frame to arrive error-free at the destination is $75\,\% = 0.75$
   - The probability that both of the first two frames are received without an error is $0.75 * 0.75 = 0.5625 = 56.25\,\%$
   - The probability that all first three frames arrive error-free is $0.75 * 0.75 * 0.75 = 0.75^3 = 42.1875\,\%$

   ⇒ the probability that all $n = 16$ frames arrive undamaged is $p = 0.75^{16} \approx 1\,\%$!
   - $E = n * \frac{1}{p} \approx 16 * 99.77 \approx 1596$

$$
\begin{aligned}
E &= \sum_{i=1}^{\infty} ip(1-p)^{(i-1)} \\
&= p \sum_{i=1}^{\infty} i(1-p)^{(i-1)}
\end{aligned}
$$

Exercise 1: Error Control

1. An upper-layer packet is split into 16 frames, each of which has a 75 percent chance of arriving undamaged. If no error control is done by the data link protocol, how many frames are required to be sent on average to get the entire thing through?
   - The probability for the first frame to arrive error-free at the destination is $75\,\% = 0.75$
   - The probability that both of the first two frames are received without an error is $0.75 * 0.75 = 0.5625 = 56.25\,\%$
   - The probability that all first three frames arrive error-free is $0.75 * 0.75 * 0.75 = 0.75^3 = 42.1875\,\%$

   ⇒ the probability that all $n = 16$ frames arrive undamaged is $p = 0.75^{16} \approx 1\,\%$!
   - $E = n * \frac{1}{p} \approx 16 * 99.77 \approx 1596$

$$E = \sum_{i=1}^{\infty} ip(1-p)^{(i-1)}$$
$$= p \sum_{i=1}^{\infty} i(1-p)^{(i-1)}$$

Geometric series

$$S = \sum_{i=1}^{\infty} a^i = \frac{1}{1-\alpha}$$
$$\Rightarrow \sum_{i=1}^{\infty} i\alpha^{(i-1)} = \frac{1}{(1-\alpha)^2}$$

Exercise 1: Error Control

1. An upper-layer packet is split into 16 frames, each of which has a 75 percent chance of arriving undamaged. If no error control is done by the data link protocol, how many frames are required to be sent on average to get the entire thing through?
   - The probability for the first frame to arrive error-free at the destination is $75\,\% = 0.75$
   - The probability that both of the first two frames are received without an error is $0.75 * 0.75 = 0.5625 = 56.25\,\%$
   - The probability that all first three frames arrive error-free is $0.75 * 0.75 * 0.75 = 0.75^3 = 42.1875\,\%$

   ⇒ the probability that all $n = 16$ frames arrive undamaged is $p = 0.75^{16} \approx 1\,\%$!
   - $E = n * \frac{1}{p} \approx 16 * 99.77 \approx 1596$

$$E = \sum_{i=1}^{\infty} ip(1-p)^{(i-1)}$$

$$= p \sum_{i=1}^{\infty} i(1-p)^{(i-1)}$$

Substitute α with $(1-p)$

$$\Rightarrow E = \frac{1}{p} \Rightarrow \frac{1}{0.01} \approx 99.77$$

Geometric series

$$S = \sum_{i=1}^{\infty} a^i = \frac{1}{1-\alpha}$$

$$\Rightarrow \sum_{i=1}^{\infty} i\alpha^{(i-1)} = \frac{1}{(1-\alpha)^2}$$

Exercise 1: Error Control

2. If error detection is done by the data link protocol, how many frames are required?

Exercise 1: Error Control

2 If error detection is done by the data link protocol, how many frames are required?
$\frac{16}{0.75} \approx 21.3$

Exercise 1: Error Control

2. If error detection is done by the data link protocol, how many frames are required?
   $\frac{16}{0.75} \approx 21.3$
3. If forward error correction is done, how many frames are required?

Exercise 1: Error Control

2. If error detection is done by the data link protocol, how many frames are required?
   $\frac{16}{0.75} \approx 21.3$
3. If forward error correction is done, how many frames are required?
   16

Exercise 1: Error Control

2. If error detection is done by the data link protocol, how many frames are required?
   $\frac{16}{0.75} \approx 21.3$
3. If forward error correction is done, how many frames are required?
   16
4. Given the following valid codewords on the data link layer:
   - $w_1 = 0001\ 1111$
   - $w_2 = 0111\ 1111$
   - $w_3 = 1100\ 1111$
   - $w_4 = 1011\ 1111$
   - $w_5 = 0001\ 0000$
   - $w_6 = 0111\ 0000$
   - $w_7 = 1100\ 0000$
   - $w_8 = 1011\ 0000$

   What is the minimum Hamming distance of this code? How many flipped bits could be detected? How many of them could be automatically be corrected?

Exercise 1: Error Control

2 If error detection is done by the data link protocol, how many frames are required?
$\frac{16}{0.75} \approx 21.3$

3 If forward error correction is done, how many frames are required?
16

4 Given the following valid codewords on the data link layer:

- $w_1 = 0001\ 1111$
- $w_2 = 0111\ 1111$
- $w_3 = 1100\ 1111$
- $w_4 = 1011\ 1111$
- $w_5 = 0001\ 0000$
- $w_6 = 0111\ 0000$
- $w_7 = 1100\ 0000$
- $w_8 = 1011\ 0000$

What is the minimum Hamming distance of this code? How many flipped bits could be detected? How many of them could be automatically be corrected?

- The minimum Hamming distance between any two words is 2.
- One bit errors can be detected.
- No errors can be corrected.

Exercise 1: Error Control

5. Most data link layer protocols put the CRC in the end of a frame (*trailer*) rather than in the beginning (*header*). Why?

Exercise 1: Error Control

5. Most data link layer protocols put the CRC in the end of a frame (*trailer*) rather than in the beginning (*header*). Why?
   The CRC is computed during transmission and appended to the output stream as soon as the last bit goes out onto the wire. If the CRC were in the header, it would be necessary to make a pass over the frame to compute the CRC before transmitting. This would require each byte to be handled twice—once for checksumming and once for transmitting. Using the trailer cuts the work in half.

Exercise 1: Error Control

6 For the data 0xDE 0xAD 0xBE 0xEF the *CRC16-CCITT* results in 0x19 0x15. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?

- 0xDE 0xAD 0xBE 0xFF
- 0xDE 0xAD 0xBE 0xE8
- 0xFF 0xFD 0xBE 0xEF
- 0x9E 0xAD 0xBE 0xED
- 0xDE 0xAD 0xBE 0xD0

Exercise 1: Error Control

6 For the data `0xDE 0xAD 0xBE 0xEF` the *CRC16-CCITT* results in `0x19 0x15`. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?

- `0xDE 0xAD 0xBE 0xFF`
  1 bit error → can be detected by CRC16-CCITT
- `0xDE 0xAD 0xBE 0xE8`
- `0xFF 0xFD 0xBE 0xEF`
- `0x9E 0xAD 0xBE 0xED`
- `0xDE 0xAD 0xBE 0xD0`

Exercise 1: Error Control

6 For the data 0xDE 0xAD 0xBE 0xEF the *CRC16-CCITT* results in 0x19 0x15. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?

- 0xDE 0xAD 0xBE 0xFF
  1 bit error → can be detected by CRC16-CCITT
- 0xDE 0xAD 0xBE 0xE8
  3 bit error → can be detected by CRC16-CCITT
- 0xFF 0xFD 0xBE 0xEF
- 0x9E 0xAD 0xBE 0xED
- 0xDE 0xAD 0xBE 0xD0

Exercise 1: Error Control

6. For the data 0xDE 0xAD 0xBE 0xEF the *CRC16-CCITT* results in 0x19 0x15. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?
   - 0xDE 0xAD 0xBE 0xFF
     1 bit error → can be detected by CRC16-CCITT
   - 0xDE 0xAD 0xBE 0xE8
     3 bit error → can be detected by CRC16-CCITT
   - 0xFF 0xFD 0xBE 0xEF
     4 bit error → may not be detected by CRC16-CCITT
   - 0x9E 0xAD 0xBE 0xED
   - 0xDE 0xAD 0xBE 0xD0

Exercise 1: Error Control

6 For the data 0xDE 0xAD 0xBE 0xEF the *CRC16-CCITT* results in 0x19 0x15. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?

- 0xDE 0xAD 0xBE 0xFF
  1 bit error → can be detected by CRC16-CCITT
- 0xDE 0xAD 0xBE 0xE8
  3 bit error → can be detected by CRC16-CCITT
- 0xFF 0xFD 0xBE 0xEF
  4 bit error → may not be detected by CRC16-CCITT
- 0x9E 0xAD 0xBE 0xED
  2 bit error → can be detected by CRC16-CCITT
- 0xDE 0xAD 0xBE 0xD0

Exercise 1: Error Control

6 For the data `0xDE 0xAD 0xBE 0xEF` the *CRC16-CCITT* results in `0x19 0x15`. Which of the following blocks of data will certainly result in a different CRC16-CCITT checksum?

- `0xDE 0xAD 0xBE 0xFF`
  1 bit error → can be detected by CRC16-CCITT
- `0xDE 0xAD 0xBE 0xE8`
  3 bit error → can be detected by CRC16-CCITT
- `0xFF 0xFD 0xBE 0xEF`
  4 bit error → may not be detected by CRC16-CCITT
- `0x9E 0xAD 0xBE 0xED`
  2 bit error → can be detected by CRC16-CCITT
- `0xDE 0xAD 0xBE 0xD0`
  burst error with less than 16 bits → can be detected by CRC16-CCITT

Exercise 2: Error Detection – CRC

1. `Generator polynomial: 100101`
   `Payload: 11010011`

Exercise 2: Error Detection – CRC

1. `Generator polynomial: 100101`
   `Payload: 11010011`
   The generator polynomial has 6 digits $\Longrightarrow$ five 0 bits are appended
   Frame with appended 0 bits: 1101001100000

```
1101001100000
100101|||||||
------v||||||
 100011||||||
 100101||||||
 ------vvv|||
    110100|||
    100101|||
    ------v||
     100010||
     100101||
     ------vv
        11100 = Remainder
```

Remainder: 11100
Transferred frame: **1101001111100**

Exercise 2: Error Detection – CRC

2. `Transferred frame: 1101001110100`
   `Generator polynomial: 100101`

Exercise 2: Error Detection – CRC

2 Transferred frame: 1101001110100
Generator polynomial: 100101

```
1101001110100
100101|||||||
------v||||||
 100011||||||
 100101||||||
 ------vvv|||
    110110|||
    100101|||
    ------v||
     100111||
     100101||
     ------vv
         1000 => Error
```

Exercise 2: Error Detection – CRC

3. `Transferred frame: 1101001111100`
   `Generator polynomial: 100101`

Exercise 2: Error Detection – CRC

3 Transferred frame: 1101001111100
Generator polynomial: 100101

```
1101001111100
100101|||||||
------v||||||
 100011||||||
 100101||||||
 ------vvv|||
    110111|||
    100101|||
    ------v||
     100101||
     100101||
     ------vv
           00 => Transmission was error-free
```

Exercise 2: Error Detection – CRC

4. `Generator polynomial: 100101`
   `Payload: 10110101`

Exercise 2: Error Detection – CRC

4. Generator polynomial: 100101
Payload: 10110101
The generator polynomial has 6 digits $\Longrightarrow$ five 0 bits are appended.
Frame with appended 0 bits: 1011010100000

```
1011010100000
100101|||||||
------vv|||||
  100001|||||
  100101|||||
  ------vv|||
     100000||
     100101||
     ------vv
        10100 = Remainder
```

Remainder: 10100
Transferred frame: **1011010110100**

Exercise 2: Error Detection – CRC

5. `Transferred frame: 1011010110110`
   `Generator polynomial: 100101`

Exercise 2: Error Detection – CRC

5. **Transferred frame: 1011010110110**
   Generator polynomial: 100101

```
1011010110110
100101|||||||
------vv|||||
  100001|||||
  100101|||||
  ------vvv||
     100101||
     100101||
     ------vv
           10 => Error
```

Exercise 2: Error Detection – CRC

6 Transferred frame: 1011010110100
Generator polynomial: 100101

Exercise 2: Error Detection – CRC

6 **Transferred frame: 1011010110100**
Generator polynomial: 100101

```
1011010110100
100101|||||||
------vv|||||
  100001|||||
  100101|||||
  ------vvv||
     100101||
     100101||
     ------vv
           00 => Transmission was error-free
```

Exercise 2: Error Detection – CRC

7. `Transferred frame: 1010010110100`
   `Generator polynomial: 100101`

Exercise 2: Error Detection – CRC

7 Transferred frame: 1010010110100
Generator polynomial: 100101

```
1010010110100
100101|||||||
------vv|||||
  110001|||||
  100101|||||
  ------v||||
   101001||||
   100101||||
   ------vv||
     110001||
     100101||
     ------v|
      101000|
      100101|
      ------v
        11010 => Error
```

Exercise 2: Error Detection – CRC

8

```
Generator polynomial: 100000111
Payload: 1101010101110101
```

Exercise 2: Error Detection – CRC

8 Generator polynomial: 100000111
Payload: 1101010101110101
The generator polynomial has 9 digits
$\Longrightarrow$ eight 0 bits are appended.
Frame with appended 0 bits:
110101010111010100000000

Remainder: 10110111
Transferred frame:
110101010111010110110111

```
110101010111010100000000
100000111|||||||||||||||
---------v||||||||||||||
 101011011||||||||||||||
 100000111||||||||||||||
 ---------vv||||||||||||
   101110011||||||||||||
   100000111||||||||||||
   ---------vv||||||||||
     111010001||||||||||
     100000111||||||||||
     ---------v|||||||||
      110101100|||||||||
      100000111|||||||||
      ---------v||||||||
       101010111||||||||
       100000111||||||||
       ---------vv||||||
         101000000||||||
         100000111||||||
         ---------vv||||
           100011100||||
           100000111||||
           ---------vvvv
               110110000
               100000111
               ---------
                10110111 = Remainder
```

Exercise 2: Error Detection – CRC

9

```
Transferred frame: 110101010111110110110111
Generator polynomial: 100000111
```

Exercise 2: Error Detection – CRC

9 Transferred frame: 1101010101111110110110111
Generator polynomial: 100000111

```
1101010101111110110110111
100000111||||||||||||||||
---------v|||||||||||||||
 101011011||||||||||||||
 100000111||||||||||||||
 ---------vv|||||||||||||
   101110011
   100000111
   ---------
     111010011
     100000111
     ---------
      110101000
      100000111
      ---------
       101011111
       100000111
       ---------
         101100010
         100000111
         ---------
           110010111
           100000111
           ---------
            100100000
            100000111
            ---------
               100111111
               100000111
               ---------
                  111000 => Error
```

Exercise 2: Error Detection – CRC

10

```
Transferred frame: 1101010101110101101101111
Generator polynomial: 100000111
```

Exercise 2: Error Detection – CRC

10 Transferred frame: 110101010111010110110111
Generator polynomial: 100000111

```
110101010111010110110111
100000111|||||||||||||||
---------v||||||||||||||
 101011011||||||||||||||
 100000111||||||||||||||
 ---------vv||||||||||||
   101110011||||||||||||
   100000111||||||||||||
   ---------vv||||||||||
     111010001||||||||||
     100000111||||||||||
     ---------v|||||||||
      110101100|||||||||
      100000111|||||||||
      ---------v||||||||
       101010111||||||||
       100000111||||||||
       ---------vv||||||
         101000010||||||
         100000111||||||
         ---------vv||||
           100010111||||
           100000111||||
           ---------vvvv
               100000111
               100000111
               ---------
                       0 => Transmission was error-free
```

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.
3. Which media access control method is implemented by **Ethernet**?

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.
3. Which media access control method is implemented by **Ethernet**?
   Non-deterministic media access control

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.
3. Which media access control method is implemented by **Ethernet**?
   Non-deterministic media access control
4. Which media access control method is implemented by **Token Ring**?

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.
3. Which media access control method is implemented by **Ethernet**?
   Non-deterministic media access control
4. Which media access control method is implemented by **Token Ring**?
   Deterministic media access control
5. Which media access control method is implemented by **WLAN**?

Exercise 3: Media Access Control

1. Why do computer networks use protocols for **media access control**?
   When a shared transmission medium is used it coordinates the access to this medium and shall avoid collisions.
2. Describe the **differences** between deterministic and non-deterministic media access control.
   In a deterministic MAC the data rate and latency for each station can be predicted because the resources are pre-allocated, a non-deterministic MAC follows a best-effort principle.
3. Which media access control method is implemented by **Ethernet**?
   Non-deterministic media access control
4. Which media access control method is implemented by **Token Ring**?
   Deterministic media access control
5. Which media access control method is implemented by **WLAN**?
   Non-deterministic media access control

Exercise 3: Media Access Control

6 What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?

Exercise 3: Media Access Control

6. What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?
   In contrast to Token Ring, for Ethernet it is impossible to clearly predict the waiting time and amount of data that can be transmitted. For Ethernet, all participants are related to the medium access in direct competition.

Exercise 3: Media Access Control

6. What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?
   In contrast to Token Ring, for Ethernet it is impossible to clearly predict the waiting time and amount of data that can be transmitted. For Ethernet, all participants are related to the medium access in direct competition.
7. Why use Ethernet and WLAN different **media access control methods**?

Exercise 3: Media Access Control

6. What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?
   In contrast to Token Ring, for Ethernet it is impossible to clearly predict the waiting time and amount of data that can be transmitted. For Ethernet, all participants are related to the medium access in direct competition.
7. Why use Ethernet and WLAN different **media access control methods**?
   With wireless networks, it is not guaranteed that all stations can detect all collisions. In wired networks with a shared transmission medium, each participant receives the transmissions of all other participants.

Exercise 3: Media Access Control

6. What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?
   In contrast to Token Ring, for Ethernet it is impossible to clearly predict the waiting time and amount of data that can be transmitted. For Ethernet, all participants are related to the medium access in direct competition.
7. Why use Ethernet and WLAN different **media access control methods**?
   With wireless networks, it is not guaranteed that all stations can detect all collisions. In wired networks with a shared transmission medium, each participant receives the transmissions of all other participants.
8. How do Ethernet devices react, when they detect a **collision**?

Exercise 3: Media Access Control

6. What is the advantage of the media access control method of **Token Ring** in contrast to the media access control method of **Ethernet**?
   In contrast to Token Ring, for Ethernet it is impossible to clearly predict the waiting time and amount of data that can be transmitted. For Ethernet, all participants are related to the medium access in direct competition.
7. Why use Ethernet and WLAN different **media access control methods**?
   With wireless networks, it is not guaranteed that all stations can detect all collisions. In wired networks with a shared transmission medium, each participant receives the transmissions of all other participants.
8. How do Ethernet devices react, when they detect a **collision**?
   If a collision is detected, the sender stops the frame transmission and sends the jam signal to announce the collision. If the maximum number of transmission attempts is not yet reached, the sender tries to transmit the frame again after a random time.

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.
   Otherwise, the network device might already be finished with the transmission and believes the transmission was successful.

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.
   Otherwise, the network device might already be finished with the transmission and believes the transmission was successful.
10. Explain what is done to ensure that the transmission of a frame is not completed when a collision occurs in an **Ethernet** network.

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.
   Otherwise, the network device might already be finished with the transmission and believes the transmission was successful.
10. Explain what is done to ensure that the transmission of a frame is not completed when a collision occurs in an **Ethernet** network.
    Each frame must have a certain minimum length. It must be dimensioned in a way, that the transmission duration for a frame with minimum length does not fall below the maximum RTT (round trip time). This ensures that a collision reaches the sender before its transmission is finished. If a sender detects a collision, it knows that its frame has not arrived correctly at the receiver, and can try the transmission again later.

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.
   Otherwise, the network device might already be finished with the transmission and believes the transmission was successful.
10. Explain what is done to ensure that the transmission of a frame is not completed when a collision occurs in an **Ethernet** network.
    Each frame must have a certain minimum length. It must be dimensioned in a way, that the transmission duration for a frame with minimum length does not fall below the maximum RTT (round trip time). This ensures that a collision reaches the sender before its transmission is finished. If a sender detects a collision, it knows that its frame has not arrived correctly at the receiver, and can try the transmission again later.
11. Why is the MAC protocol less relevant for modern Ethernet networks?

Exercise 3: Media Access Control

9. Explain why it is important that the transmission of a frame is not completed when a collision occurs in an Ethernet network.
   Otherwise, the network device might already be finished with the transmission and believes the transmission was successful.
10. Explain what is done to ensure that the transmission of a frame is not completed when a collision occurs in an **Ethernet** network.
    Each frame must have a certain minimum length. It must be dimensioned in a way, that the transmission duration for a frame with minimum length does not fall below the maximum RTT (round trip time). This ensures that a collision reaches the sender before its transmission is finished. If a sender detects a collision, it knows that its frame has not arrived correctly at the receiver, and can try the transmission again later.
11. Why is the MAC protocol less relevant for modern Ethernet networks?
    Modern Ethernet networks are typically switched, i.e., the stations do not share a transmission medium.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?
   If the utilization is low and the latency is most important.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of *p* determines the performance of the network. In which cases is preferable to use a higher value for *p*?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.
   After a detected collision each station will use the exponential backoff algorithm to determine period until the next transmission attempt. This algorithm includes a random component.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.
   After a detected collision each station will use the exponential backoff algorithm to determine period until the next transmission attempt. This algorithm includes a random component.
4. The maximum number of transmission attempts may be configurable. What are the consequences of an increased number?

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of *p* determines the performance of the network. In which cases is preferable to use a higher value for *p*?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.
   After a detected collision each station will use the exponential backoff algorithm to determine period until the next transmission attempt. This algorithm includes a random component.
4. The maximum number of transmission attempts may be configurable. What are the consequences of an increased number?
   In a network with high utilization, the success rate for sending attempts on the Data Link Layer may become bigger, but the latency will also go up.

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.
   After a detected collision each station will use the exponential backoff algorithm to determine period until the next transmission attempt. This algorithm includes a random component.
4. The maximum number of transmission attempts may be configurable. What are the consequences of an increased number?
   In a network with high utilization, the success rate for sending attempts on the Data Link Layer may become bigger, but the latency will also go up.
5. In CSMA/CD only data frames and JAM signals are required. In CSMA/CA an additional frame type is needed. Which one? Why is it required?

Exercise 4: CSMA

1. Which prerequisite needs to be fulfilled to use a CSMA MAC protocol?
   Each station must be able to sense the medium.
2. For p-persistent CSMA the size of p determines the performance of the network. In which cases is preferable to use a higher value for p?
   If the utilization is low and the latency is most important.
3. Explain how the actual delay of a network with CSMA/CD as MAC protocol is affected by the random number generator of the host.
   After a detected collision each station will use the exponential backoff algorithm to determine period until the next transmission attempt. This algorithm includes a random component.
4. The maximum number of transmission attempts may be configurable. What are the consequences of an increased number?
   In a network with high utilization, the success rate for sending attempts on the Data Link Layer may become bigger, but the latency will also go up.
5. In CSMA/CD only data frames and JAM signals are required. In CSMA/CA an additional frame type is needed. Which one? Why is it required?
   The ACK frame is used to tell the sender that the frame was successfully received, i.e., that no collision has occurred.

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?
   ARP uses broadcast on the Data Link Layer, NDP is Network Layer protocol (e.g., it uses logical addresses) and uses multicast. Consequently, ARP requests do interrupt every station in the network, while NDP requests will only interrupt the requested station.

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?
   ARP uses broadcast on the Data Link Layer, NDP is Network Layer protocol (e.g., it uses logical addresses) and uses multicast. Consequently, ARP requests do interrupt every station in the network, while NDP requests will only interrupt the requested station.
3. Which effect does *MAC spoofing* have on ARP and NDP?

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?
   ARP uses broadcast on the Data Link Layer, NDP is Network Layer protocol (e.g., it uses logical addresses) and uses multicast. Consequently, ARP requests do interrupt every station in the network, while NDP requests will only interrupt the requested station.
3. Which effect does *MAC spoofing* have on ARP and NDP?
   A requesting node may get the same MAC address for multiple IP addresses.

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?
   ARP uses broadcast on the Data Link Layer, NDP is Network Layer protocol (e.g., it uses logical addresses) and uses multicast. Consequently, ARP requests do interrupt every station in the network, while NDP requests will only interrupt the requested station.
3. Which effect does *MAC spoofing* have on ARP and NDP?
   A requesting node may get the same MAC address for multiple IP addresses.
4. What is the **ARP cache**?

Exercise 5: Address Resolution Protocol

1. What is the function of the **Address Resolution Protocol**?
   The Address Resolution Protocol (ARP) is used to convert IP address of the Network Layer to MAC address of the Data Link Layer.
2. What are the main differences between **ARP** and **NDP**?
   ARP uses broadcast on the Data Link Layer, NDP is Network Layer protocol (e.g., it uses logical addresses) and uses multicast. Consequently, ARP requests do interrupt every station in the network, while NDP requests will only interrupt the requested station.
3. Which effect does *MAC spoofing* have on ARP and NDP?
   A requesting node may get the same MAC address for multiple IP addresses.
4. What is the **ARP cache**?
   The ARP cache is a table, which contains IP addresses and MAC addresses, that belong together. It is used to speed up the address resolution.

Exercise 6: Do some research

1. For **Wireless Sensor Networks** MAC protocols have played an important role. Elaborate on its impact for these networks and name at least two WSN specific MAC protocols.

Exercise 6: Do some research

1. For **Wireless Sensor Networks** MAC protocols have played an important role. Elaborate on its impact for these networks and name at least two WSN specific MAC protocols.
   In WSNs energy consumption is typically most important. The MAC protocol has an major impact on the energy consumption. It determines, for instance, how long each station has to listen to the medium and how many transmissions are required on average. Examples are S-MAC, T-MAC, PAMAS, TRAMAS, LEACH, Contiki-MAC . . .

Exercise 6: Do some research

1. For **Wireless Sensor Networks** MAC protocols have played an important role. Elaborate on its impact for these networks and name at least two WSN specific MAC protocols.
   In WSNs energy consumption is typically most important. The MAC protocol has an major impact on the energy consumption. It determines, for instance, how long each station has to listen to the medium and how many transmissions are required on average. Examples are S-MAC, T-MAC, PAMAS, TRAMAS, LEACH, Contiki-MAC ...
2. Why can CRC not be used for digital signatures?

Exercise 6: Do some research

1. For **Wireless Sensor Networks** MAC protocols have played an important role. Elaborate on its impact for these networks and name at least two WSN specific MAC protocols.
   In WSNs energy consumption is typically most important. The MAC protocol has an major impact on the energy consumption. It determines, for instance, how long each station has to listen to the medium and how many transmissions are required on average. Examples are S-MAC, T-MAC, PAMAS, TRAMAS, LEACH, Contiki-MAC . . .
2. Why can CRC not be used for digital signatures?
   Digital signatures describe a methods to prove the **authenticity** of a message by calculating a hash value over the message. The idea is similar to CRC checksums: any change to the message shall result in a different signature/checksum value. However, for an error detection algorithm it is of importance to require little computing time. For a digital signature it is most important that the reverse direction (from the hash to the message) is as expensive as possible.

Exercise 6: Do some research

3. As a convention for configuration you may find **7E1**. Explore the context of this configuration setting and explain its meaning.

Exercise 6: Do some research

3. As a convention for configuration you may find **7E1**. Explore the context of this configuration setting and explain its meaning.
   This describes configuration for serial connections, e.g., for an external modem. **7E1** stands for **7 bit data, even parity, 1 stop bit**

Exercise 6: Do some research

3. As a convention for configuration you may find **7E1**. Explore the context of this configuration setting and explain its meaning.
   This describes configuration for serial connections, e.g., for an external modem. **7E1** stands for **7 bit data, even parity, 1 stop bit**
4. Explain why it sometimes happen that a host sends an ARP request for its own IPv4 address.

Exercise 6: Do some research

3. As a convention for configuration you may find **7E1**. Explore the context of this configuration setting and explain its meaning.
   This describes configuration for serial connections, e.g., for an external modem. **7E1** stands for **7 bit data, even parity, 1 stop bit**
4. Explain why it sometimes happen that a host sends an ARP request for its own IPv4 address.
   A so called *gratuitous ARP* can be used for duplicate address detection, to update the ARP caches of the other nodes, or to announce the existence of a node.