



LUND
UNIVERSITY

Networks and Applications – Basic concepts

MARIA KIHLM



Literature

- Slides

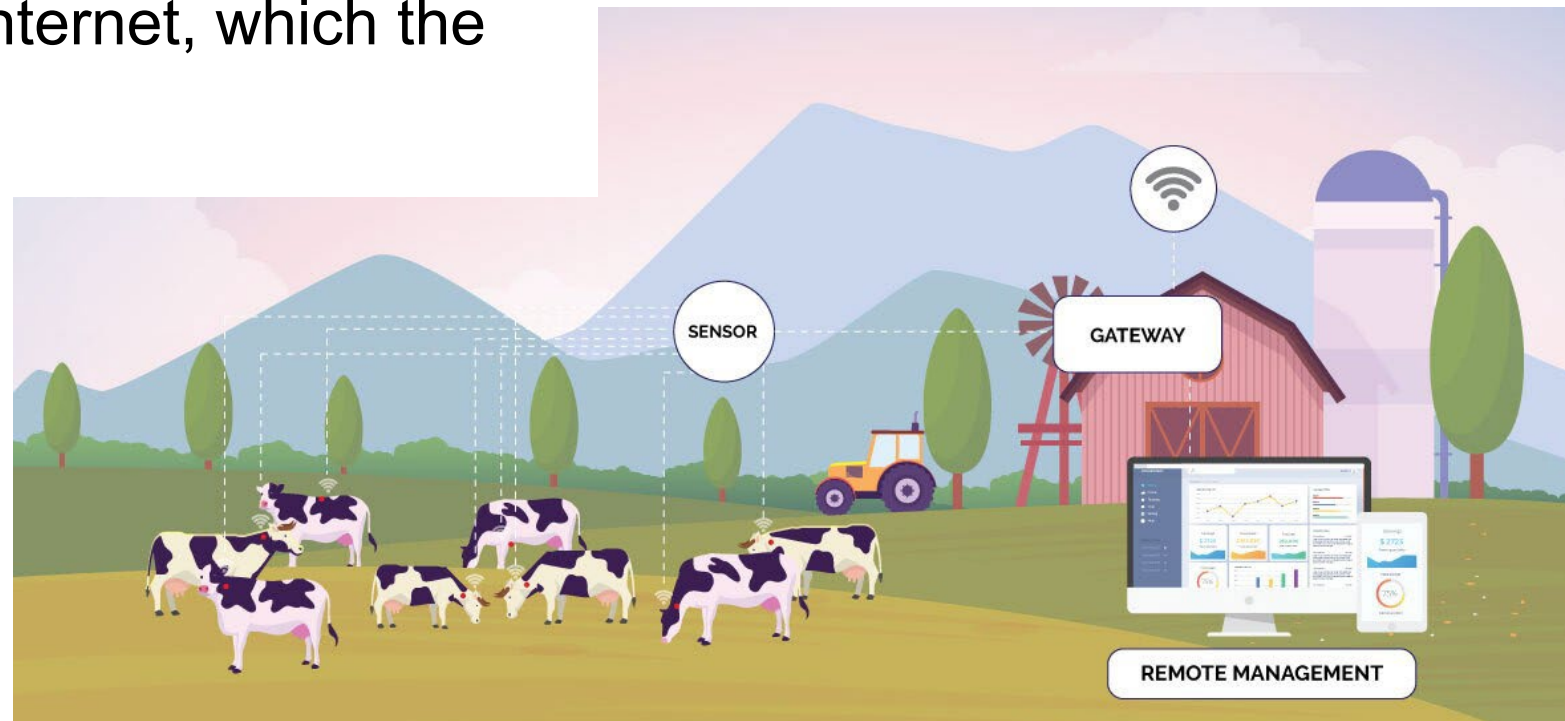
To do!

- Lectures
 - Tomorrow: Review of probability theory and statistics
- Project
 - Read document on Project Scenarios
 - Fill in project registration form (link on Canvas), deadline on Thursday!
 - Project lecture on Monday Sept 7 at 10:15

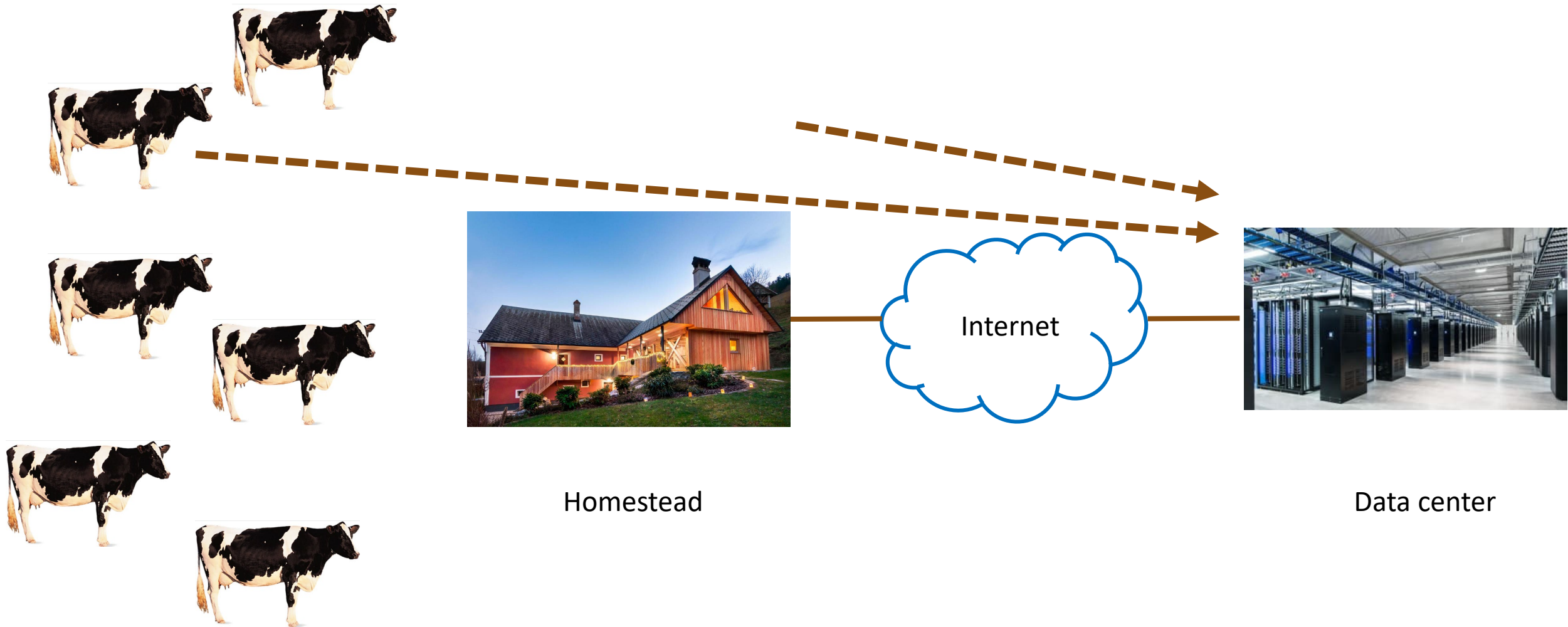
Today's scenario: The small farm

You have been given the task to design a communication system for a farmer that wants to monitor cattle including about 20 animals. The cattle are in a pasture close to the farm. Each cow carries a sensor. There should be an update from each animal with an interval of about one hour (you do not have to care about the content of the update). The update should be sent to a cloud server placed on the Internet, which the farmer can access when checking the cattle.

Describe a suitable network system for the monitoring of the cattle.



Basic network system architecture



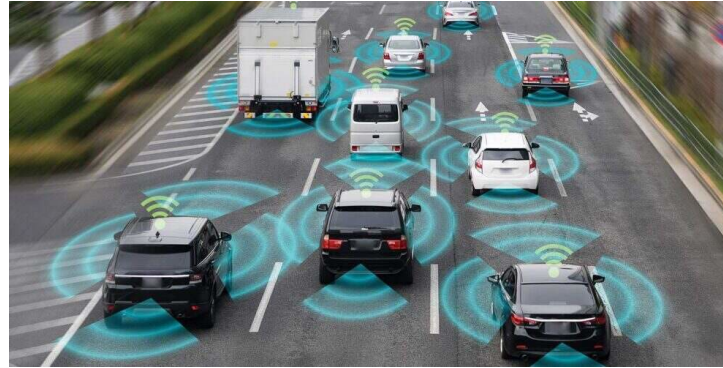
Networked applications

Networked applications

- In this course, we focus on **networked applications**. A networked application is an application that require an **Internet connection** for its operation.
 - There are two main types of networked applications: **Time-critical applications** and **Non-critical applications**.
 - **WWW, Email and Streaming** applications are examples of networked (time-critical) applications that you have seen in previous courses.
- The course focuses on networked applications that require **wireless access to the network**.
- The aim of the course is to go **beyond ordinary Internet based applications, primarily so called Internet of things (IoT), also called M2M communication**.
 - Connected intelligent machines (robots, drones, vehicles etc).
 - Animal and environmental monitoring on Earth, on land and underwater,
 - Smart homes and Smart cities.
- Also, the course includes basic knowledge about **interplanetary networks**.

Internet of Things (IoT)

The Internet of Things (IoT) is the **network of physical objects accessed through the Internet.**



Parking meters



Sensors



Utility meters



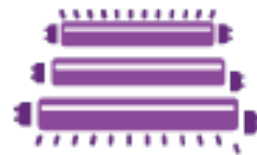
Agriculture monitors



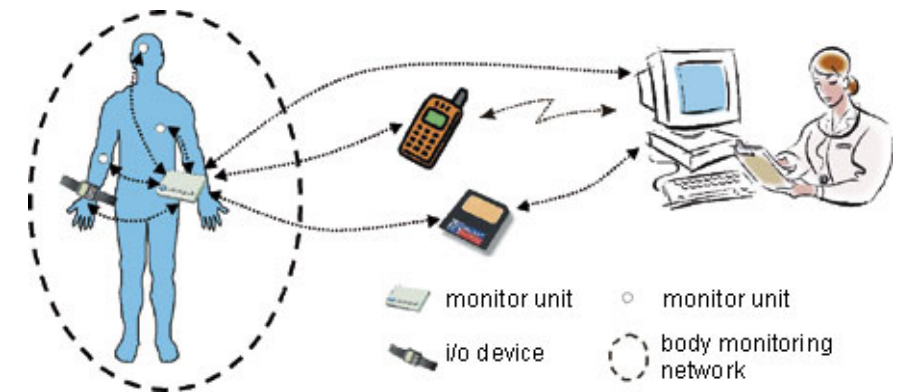
Industrial sensors



City infrastructures



Lighting/HVAC controllers



Sources: 5G Wireless Access: an Overview

<https://www.lg.com/my/about-lg/press-and-media/presenting-the-more-effective-accessible-smart-home-with-lg-thing>

https://www.ercim.eu/publication/Ercim_News/enw51/bielikova.html

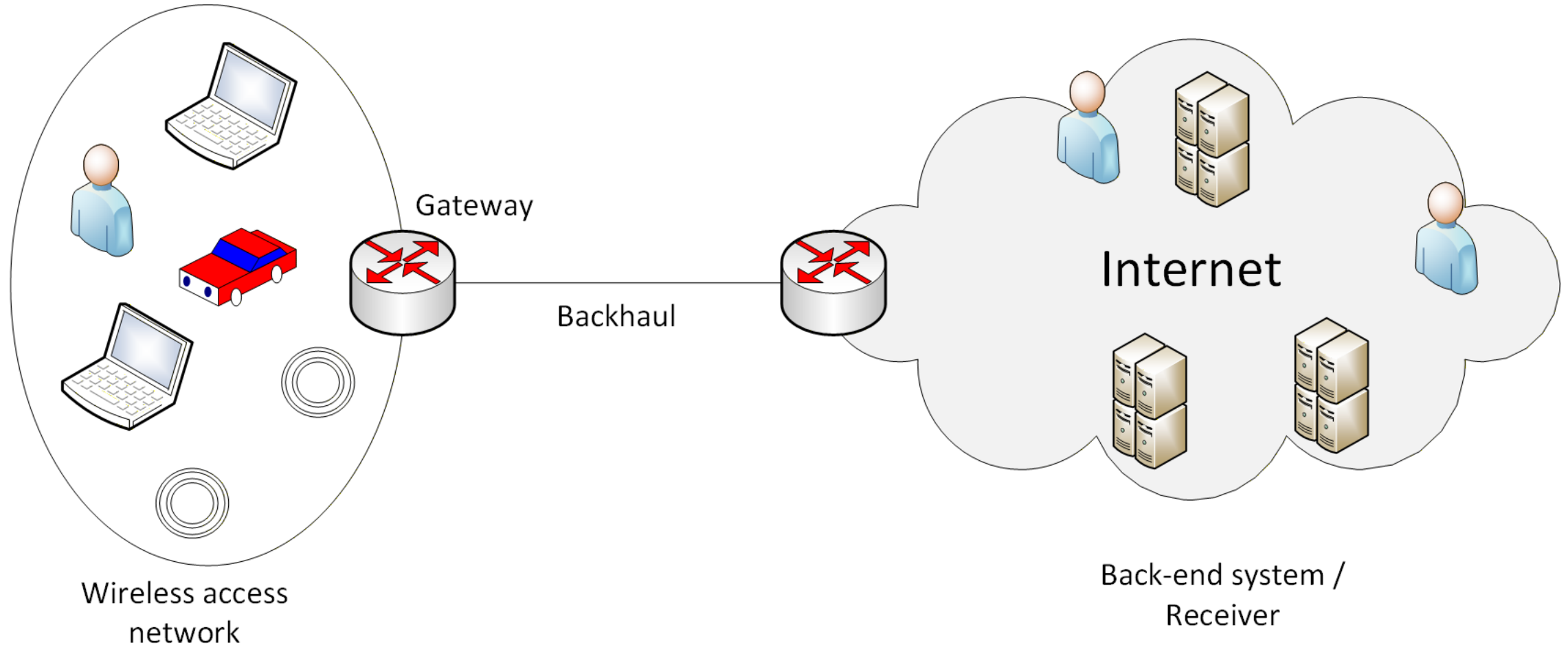
<https://www.cablefree.net/wirelesstechnology/internet-of-things-iot/>

Machine-to-Machine (M2M) communications

The IoT concept is usually connected to the concept of Machine-to-Machine (M2M) communications. Scenario examples:

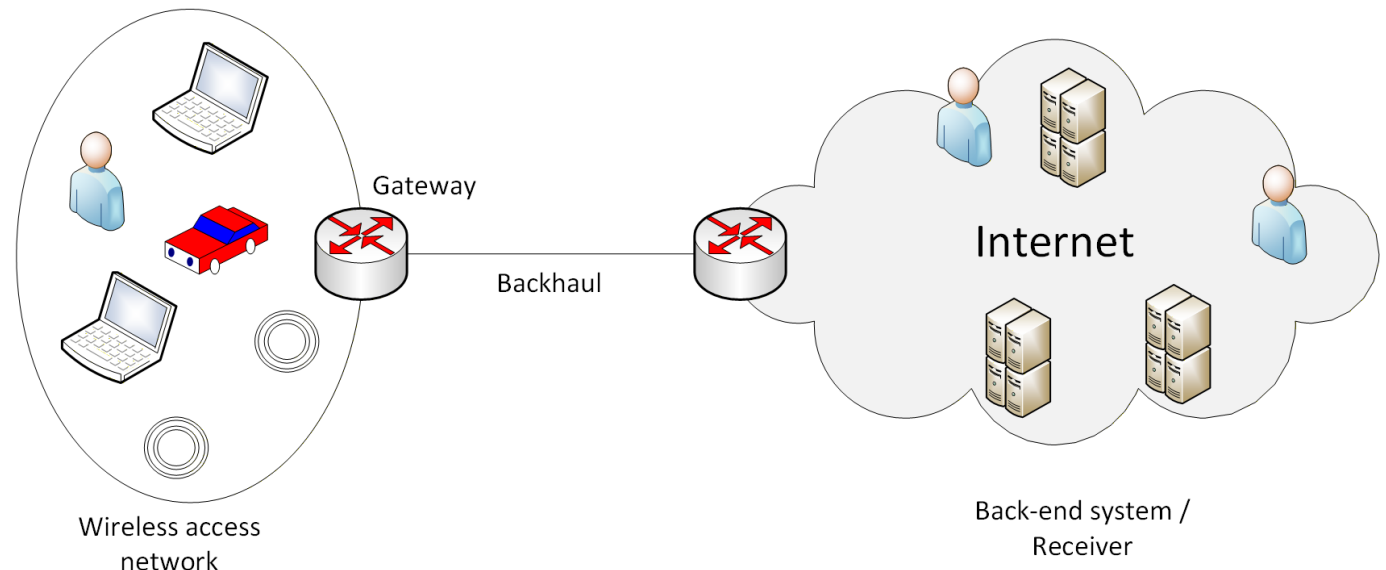
- **Direct M2M communication:** Direct communication between two devices.
 - **Application examples:** Smart wearables, smart home appliances
- **Connected intelligent machines:** Mobile machines (robots, drones, vehicles) that are connected to the Internet.
 - **Application examples:** self-driving vehicles, cloud robotics, industrial automation
- **Sensors that send data to a back-end software system**
 - **Application example:** Wireless sensor networks for monitoring of factories, animals, environment, ocean etc.

Networked systems



Hosts, routers and gateways (in this course)

- A **host** sends and receives data via a (wireless) link.
- A **router** can forward data to other routers and hosts.
 - A router is also a host in the network.
 - In some network types, a host can act as a router (but not in all networks).
- A **gateway** is connected to the Internet via a **Backhaul link**.
 - A gateway is also a router.



Network protocols

Internet protocols - TCP/IP protocol stack

The TCP/IP protocol stack is used on the Internet.

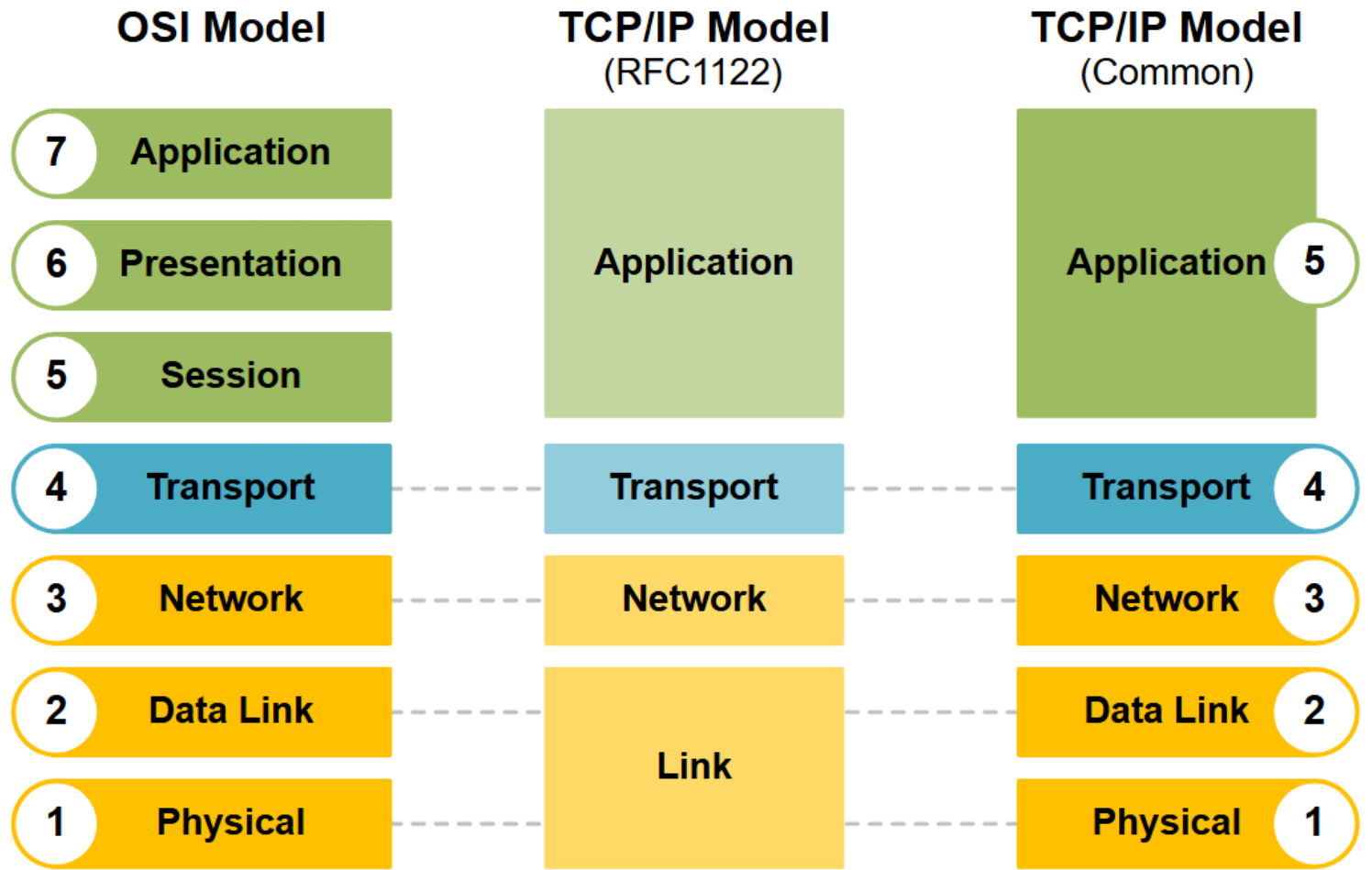
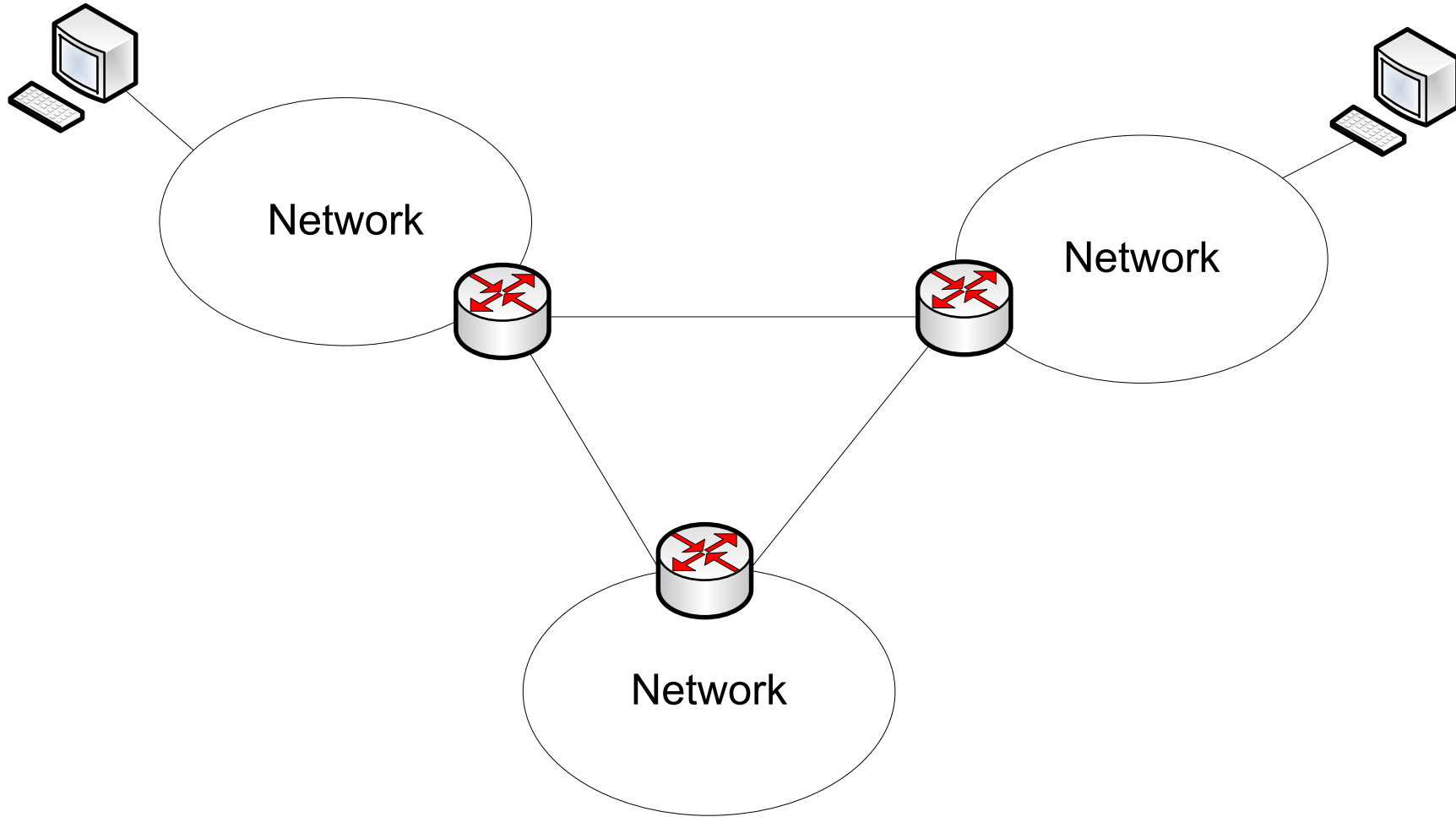


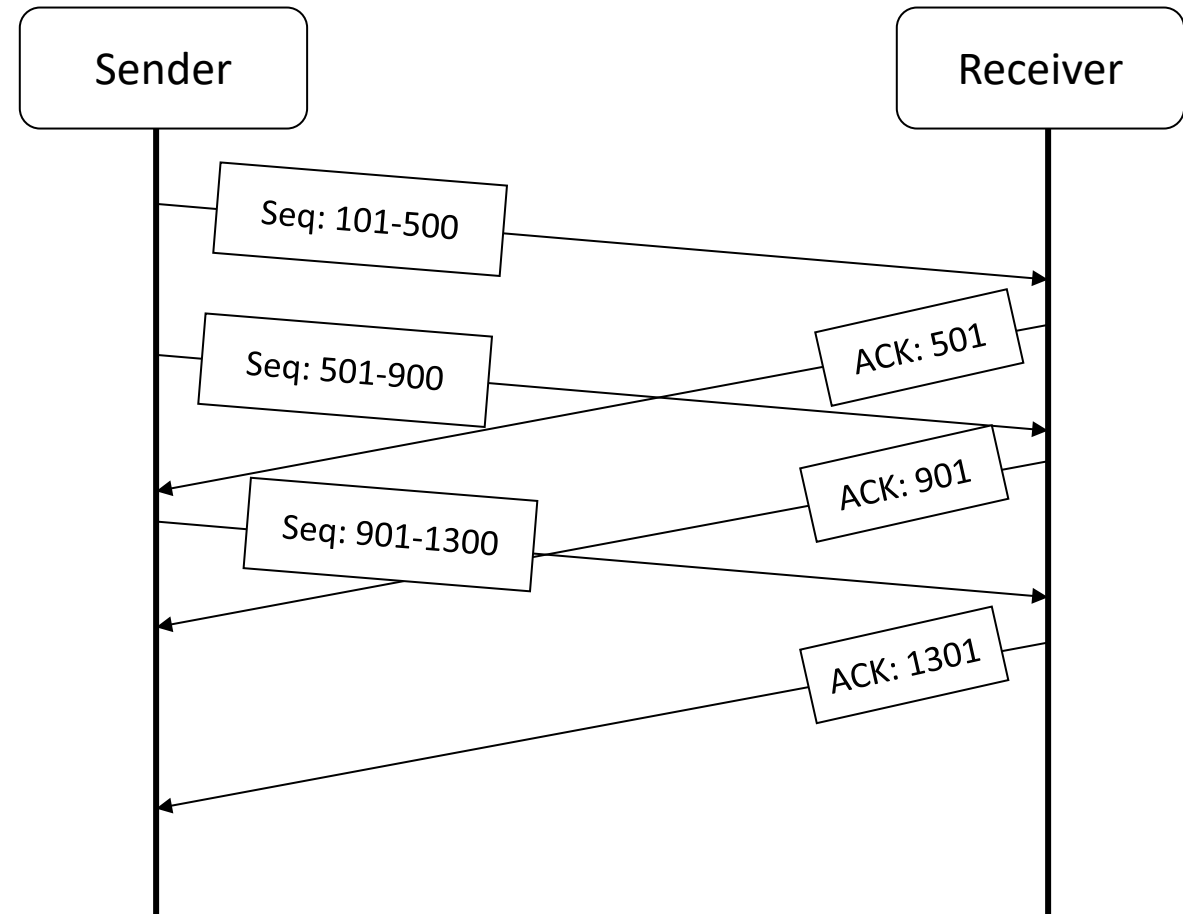
Figure 9. OSI vs. TCP/IP models.

TCP/IP protocols are for Internetworking – Data communication **between networks**

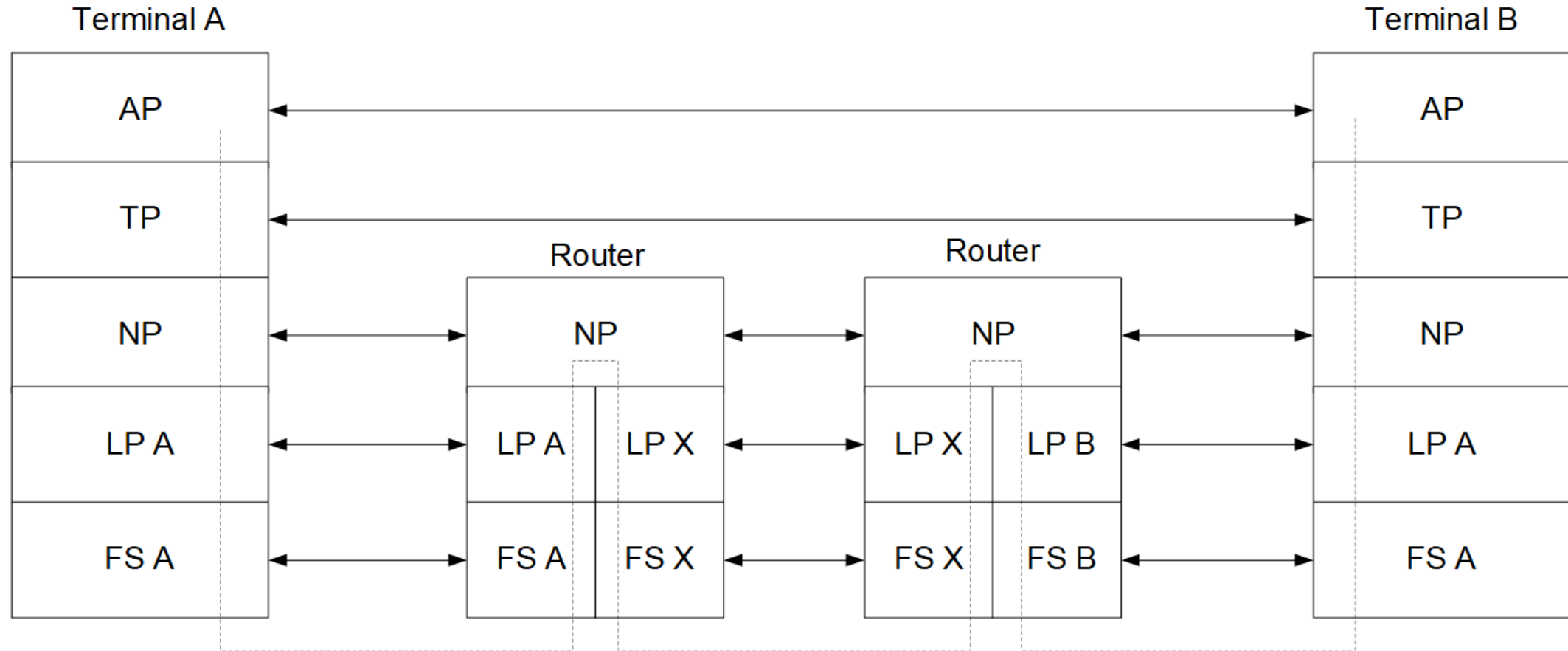


Protocols for reliable data transfer – Examples: TCP and QUIC

- TCP and QUIC provide a fast and reliable data transfer using buffers and ACK:s.
- A conversational protocol **requires an continuous end-to-end dialogue** between the sender and the receiver **over the Internet**.
- Therefore, the **data transfer requires relatively low latencies**, due to the involved timers.

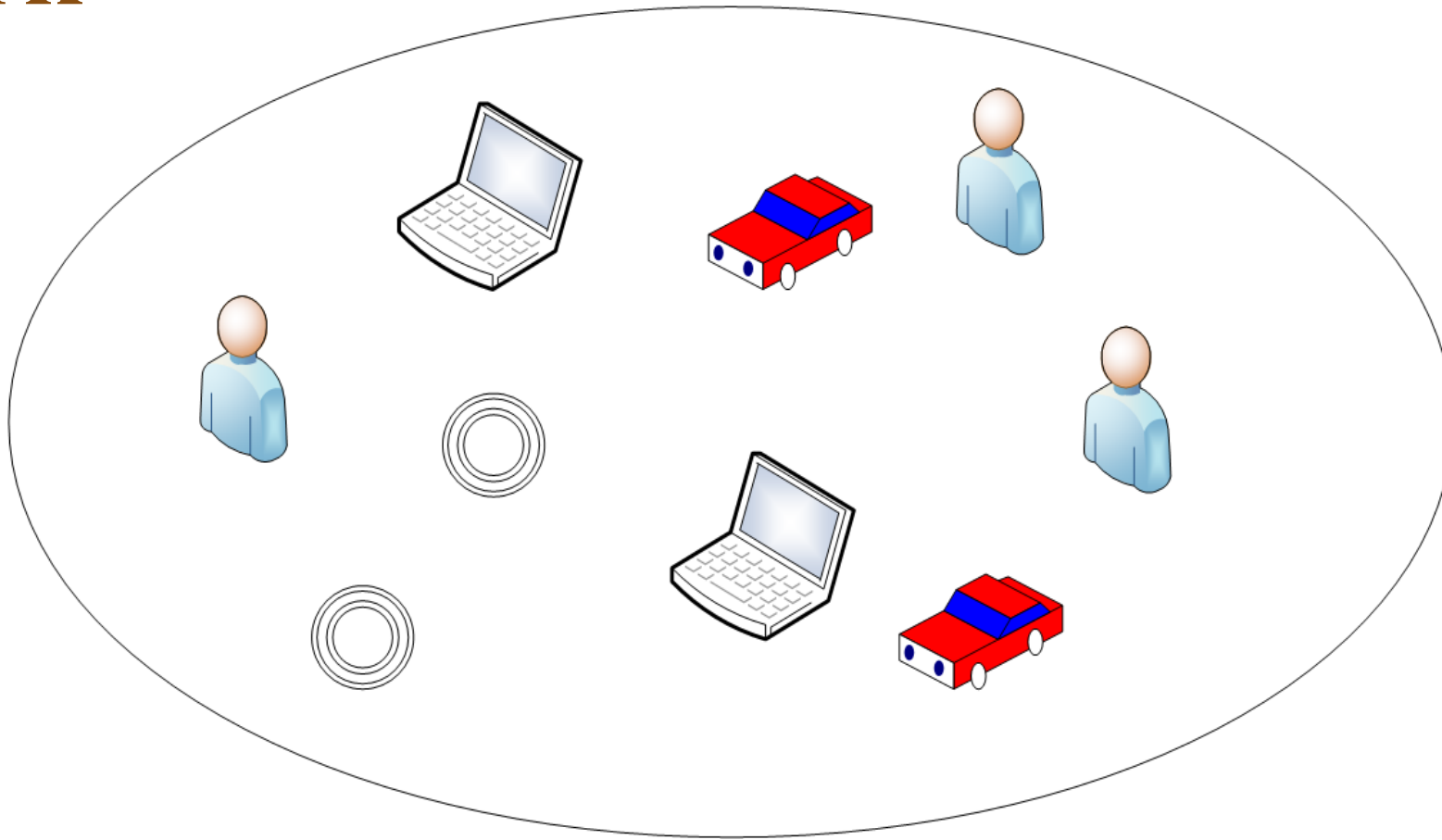


Protocol stack for reliable data transfer



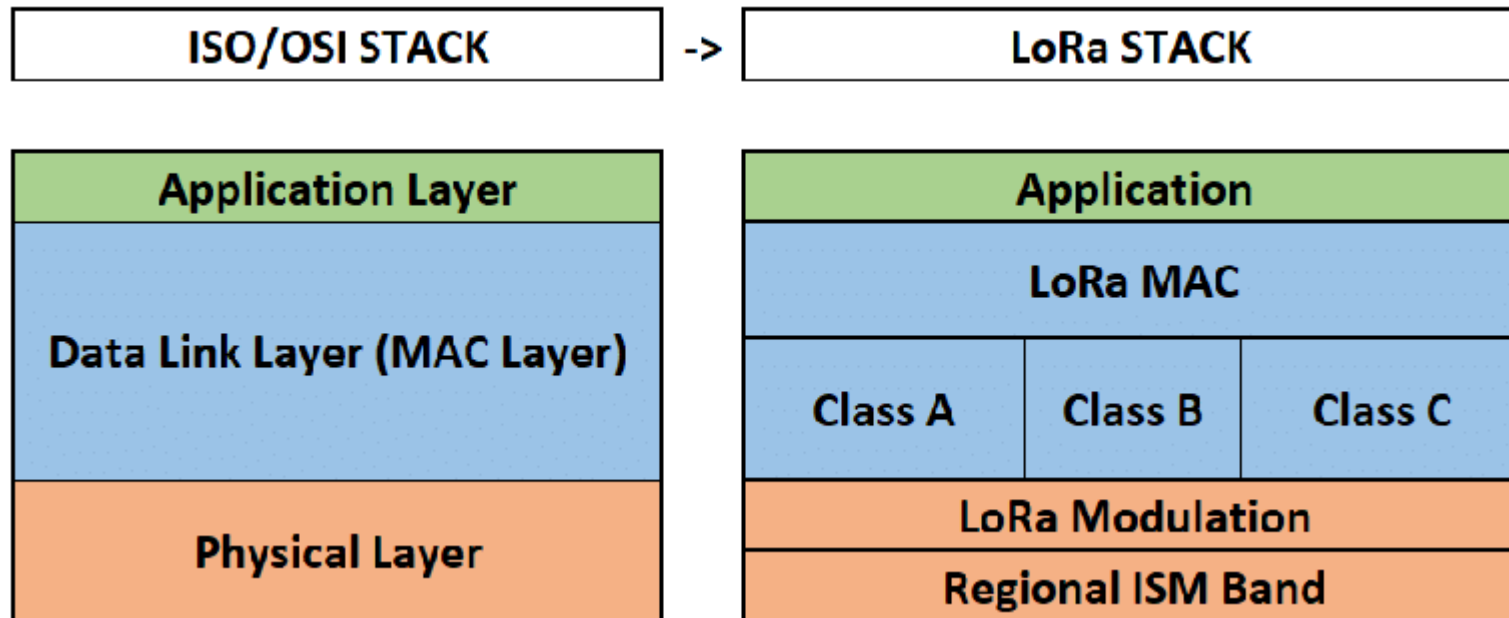
AP = Application Protocol; TP = Transport Protocol; NP = Network Protocol;
LP = Data link protocol; FS = Physical layer

Physical and Data link layers: "Intranetworking" – Protocols for data communication **within a network**



Protocols within a network?

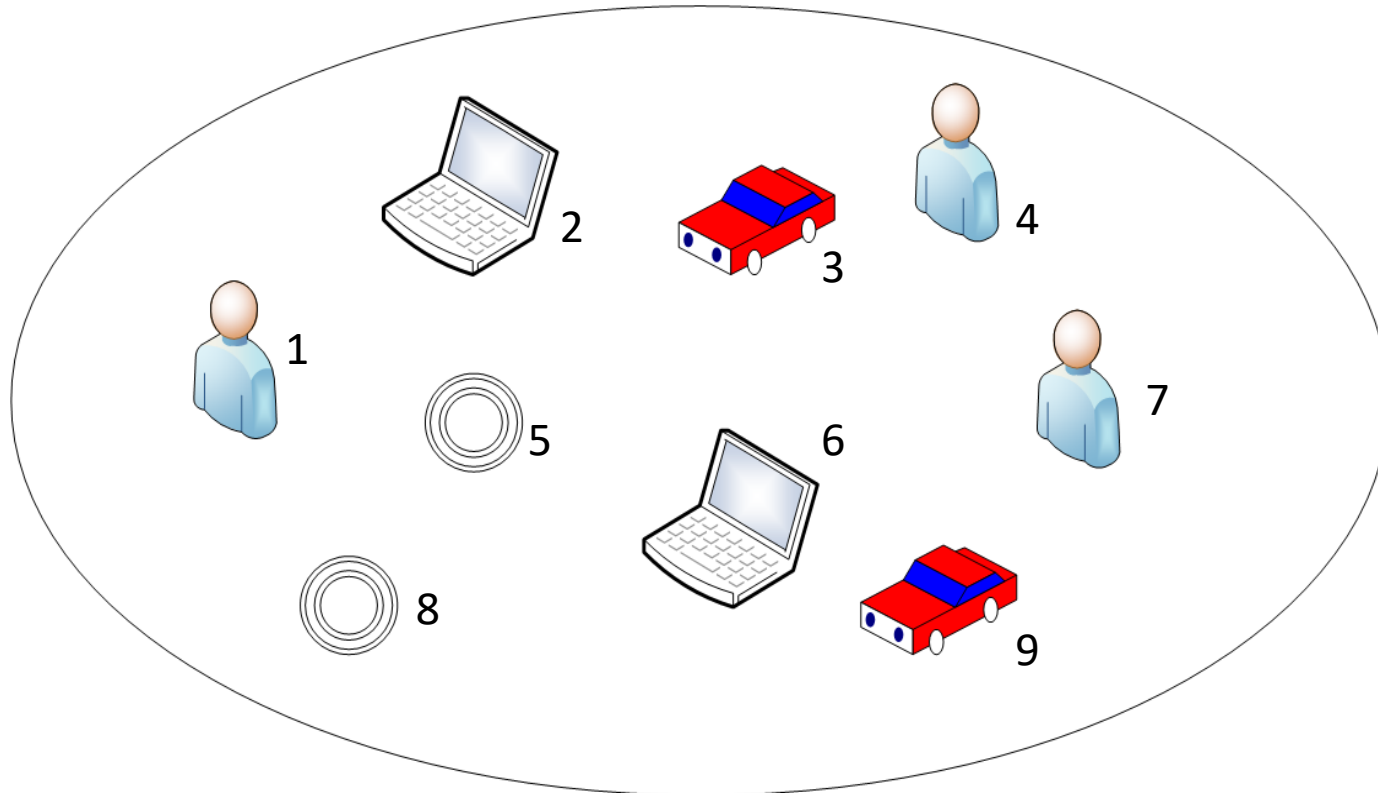
- The TCP/IP protocol stack only includes protocols for communication between networks on the Internet.
- Within each network, other protocols are used. **Communication within a network does not require TCP/IP protocols.**



The need for addresses

If you send data and there are several possible receivers of this data (hosts), you need to identify each host. Each host must be given an unique **physical address** (unique within this network).

If there is only one possible receiver, there is no need for physical addresses.

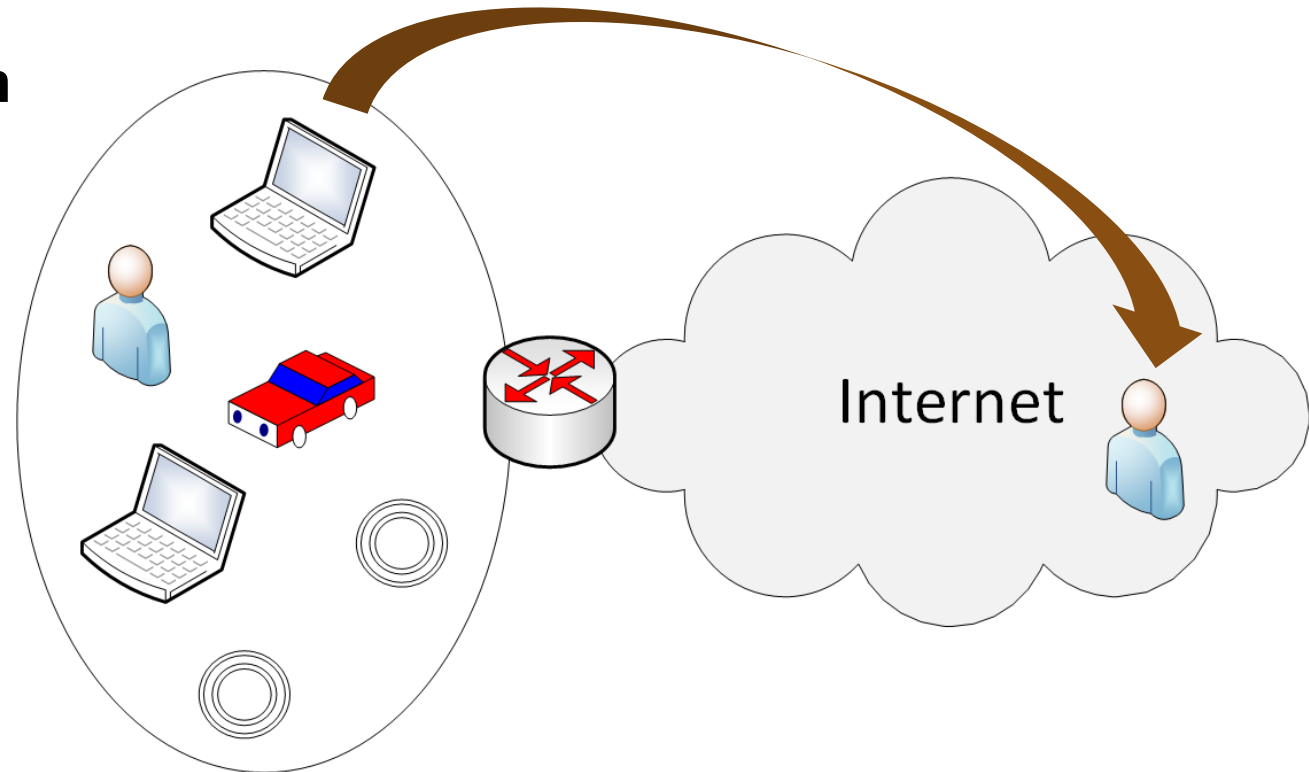


Physical addresses

- All nodes with a **network interface card (NIC)** for a specific network technology, need an unique physical address for this network interface, when connected to the network.
- Today, all standardized network technologies use standardized addresses.
Examples:
 - EUI-48 is a 48 bits physical address used in all 802.x devices (MAC address).
 - EUI-64 is a 64 bits physical address used in, for example, LoRa.
- Usually, a network technology has one broadcast address, for example FF:FF:FF:FF:FF:FF used in 802.x networks.

Access to Internet

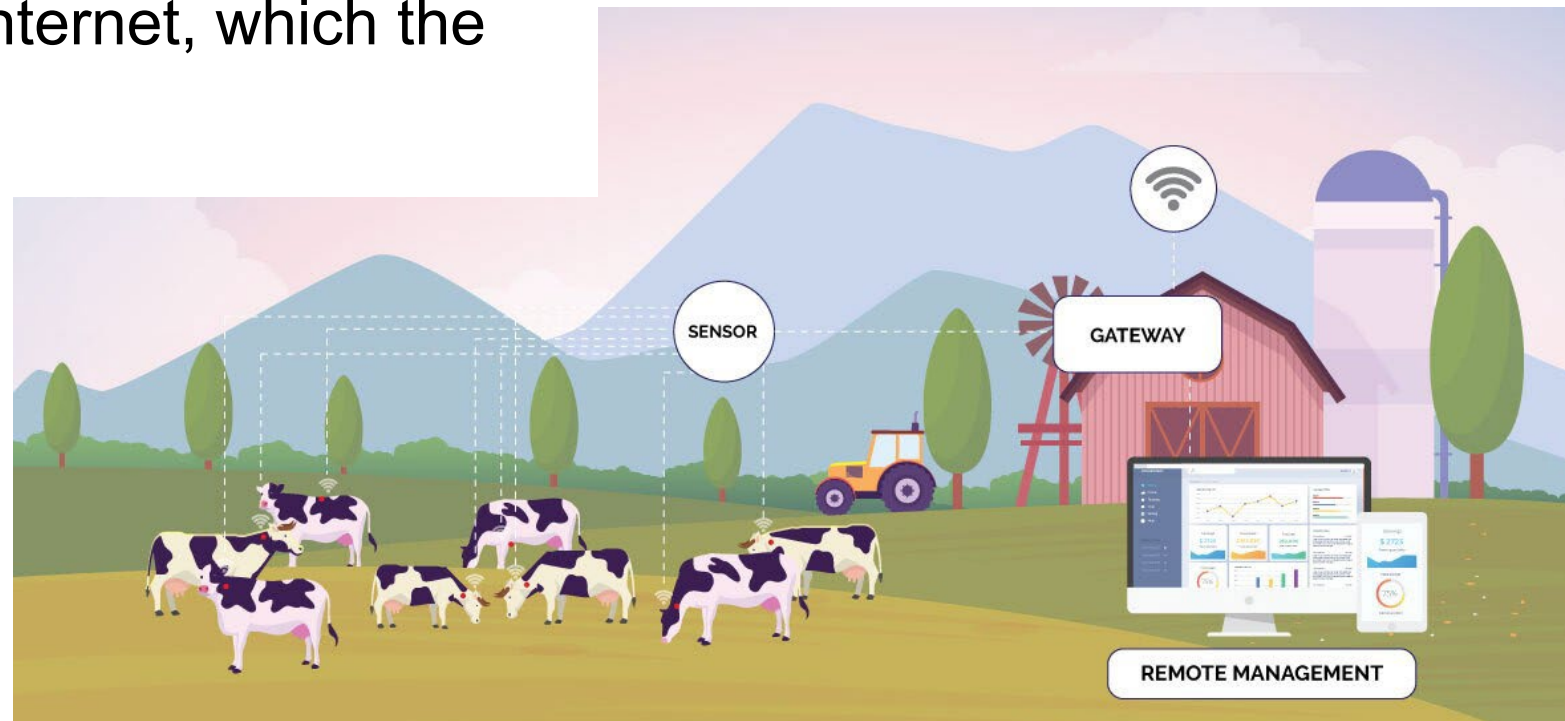
- A node that will send/receive data to/from the Internet needs an IP address.
 - **Physical addresses** are used **within** a network, on the **link layer**.
 - **IP addresses** are used **between** networks, on the **network layer**.
- The translation between a physical address and an IP address is called **address resolution**.
 - For 802.x networks, the Address Resolution Protocol (ARP) handles the address resolution.



Protocols and addresses?

You have been given the task to design a communication system for a farmer that wants to monitor cattle including about 20 animals. The cattle are in a pasture close to the farm. Each cow carries a sensor. There should be an update from each animal with an interval of about one hour (you do not have to care about the content of the update). The update should be sent to a cloud server placed on the Internet, which the farmer can access when checking the cattle.

Describe a suitable network system for the monitoring of the cattle.

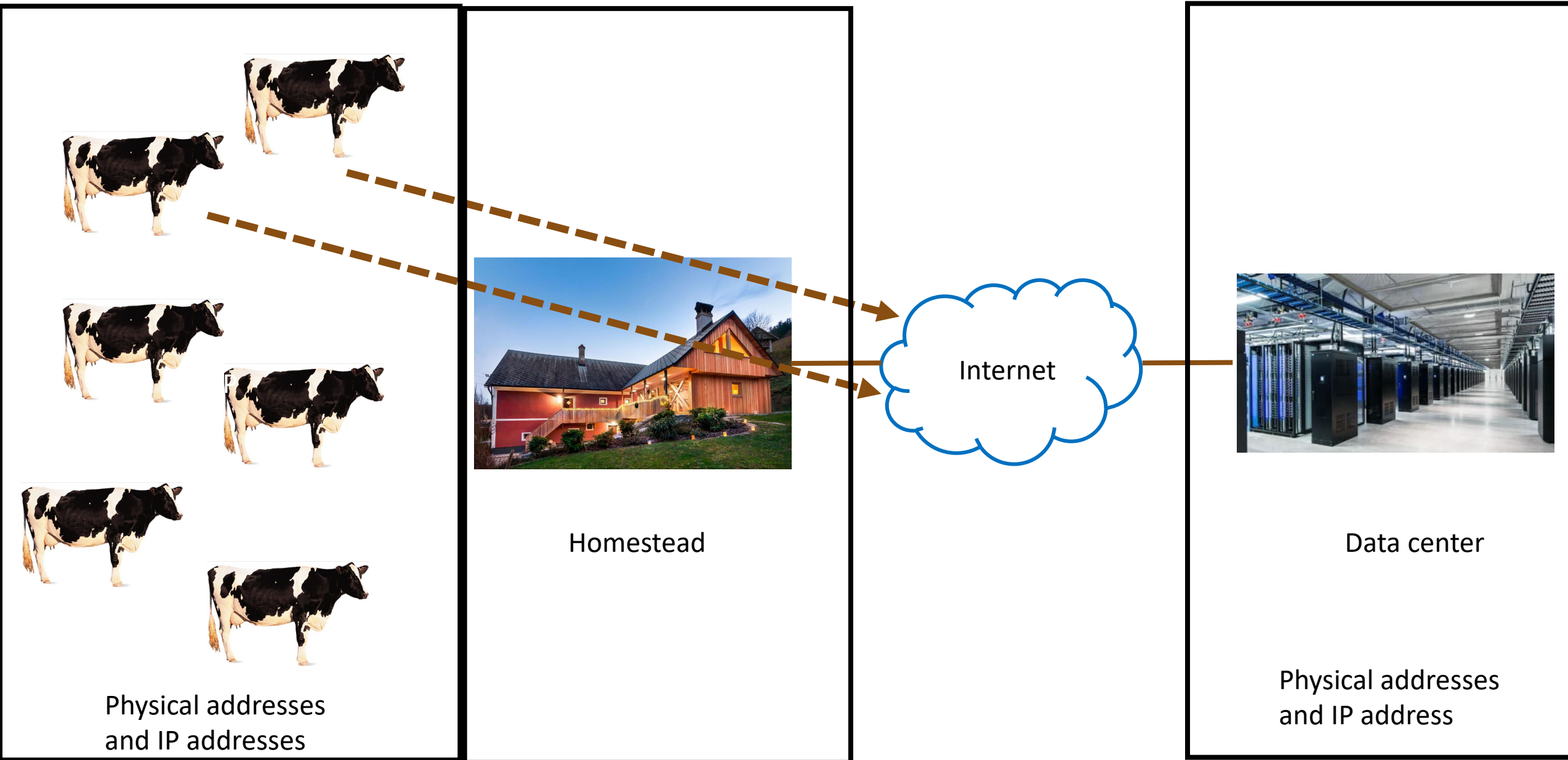


Suggested solution

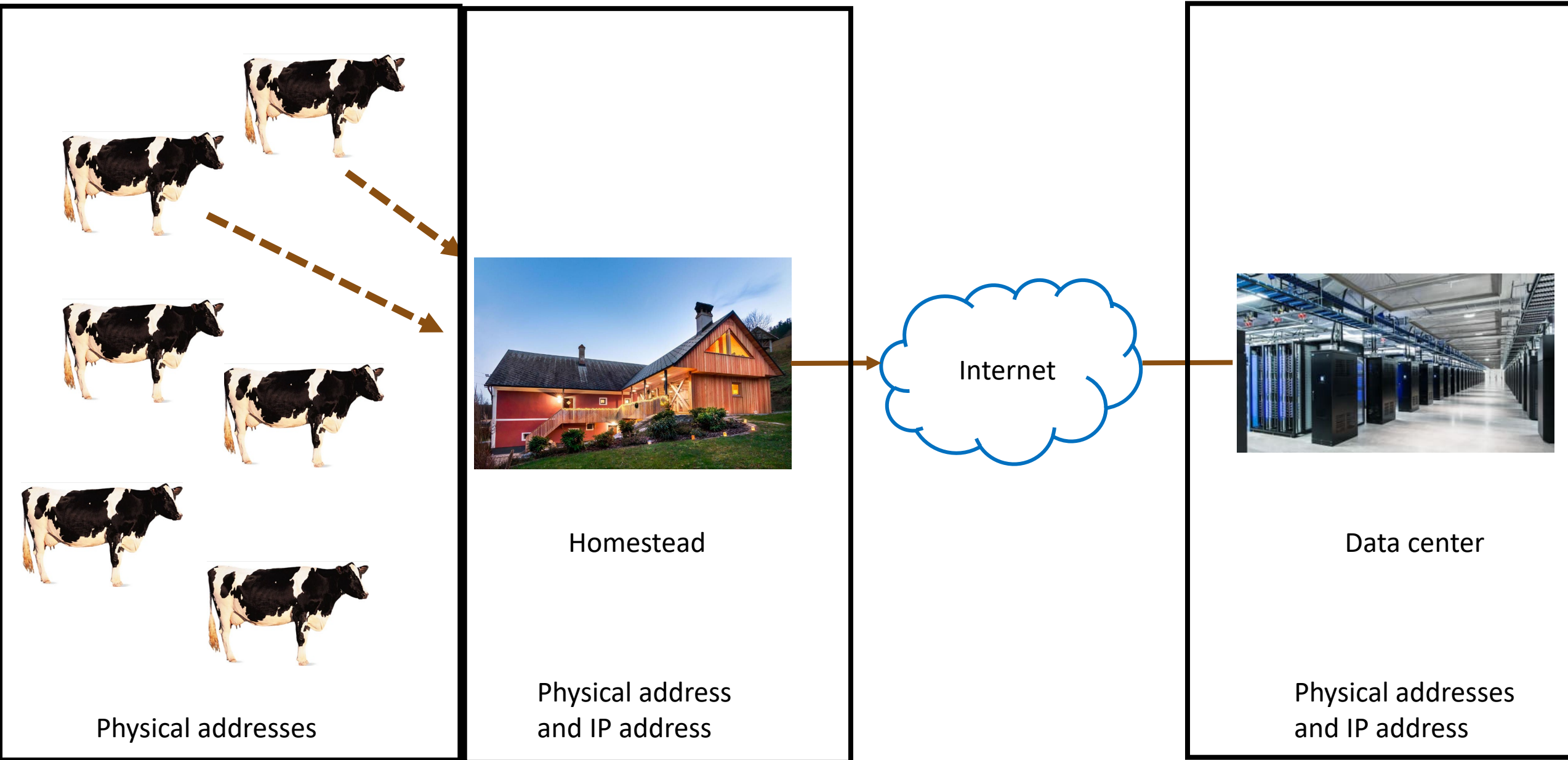
Two feasible solutions:

1. Each sensor is connected to the Internet and sends its own data to the data center.
 - This means that each sensor has a physical address (depending on the intranet technology) and Internet access with an IP address.
2. The sensors send data to an Internet-connected central unit in the homestead. This unit collects the data and sends it to the data center over the Internet.
 - This means that the central unit has a physical address and an IP address but the sensors only have physical addresses.

Scenario 1: Direct connection to the Internet



Scenario 2: Connected to a central unit

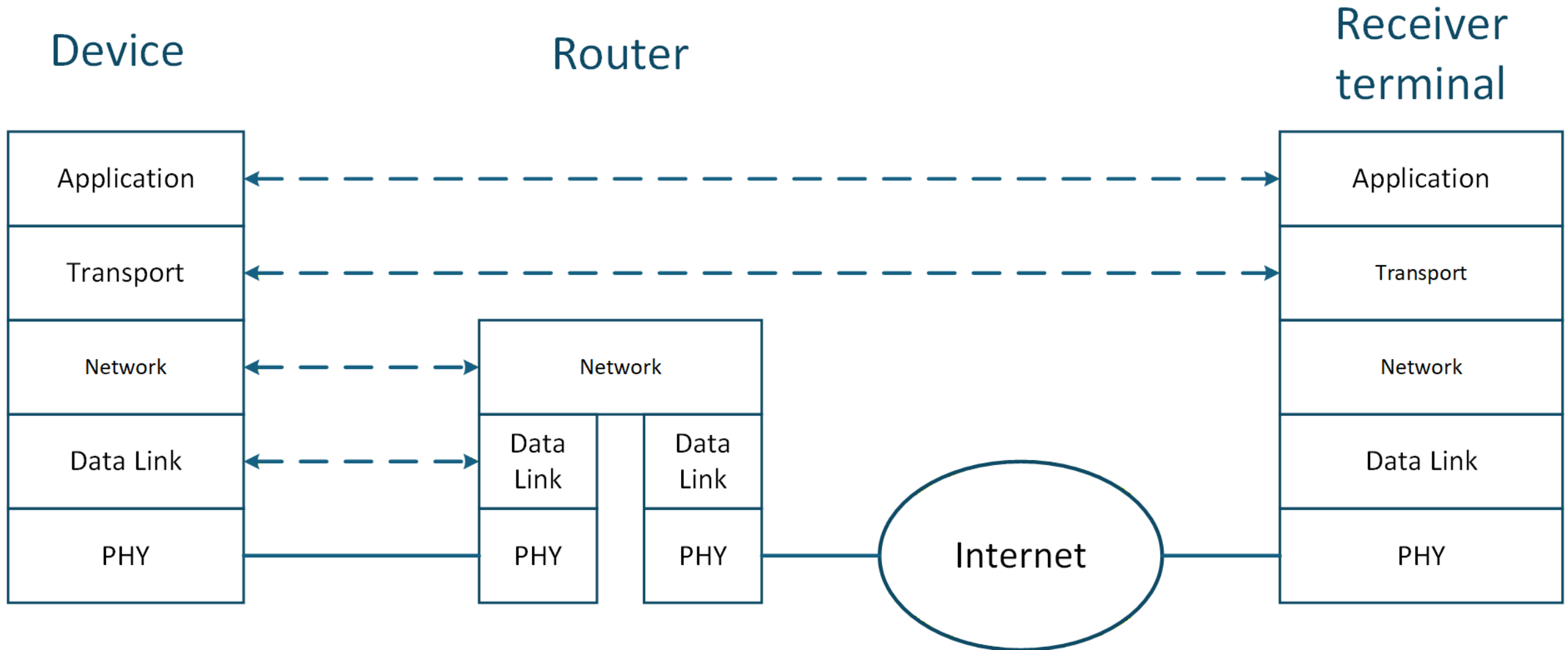


Time-critical applications

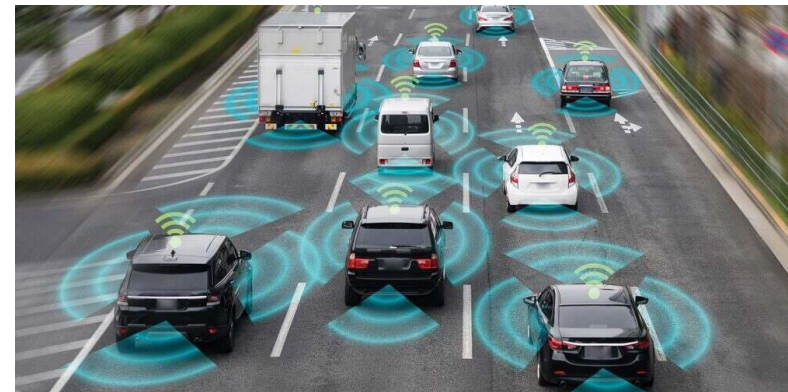
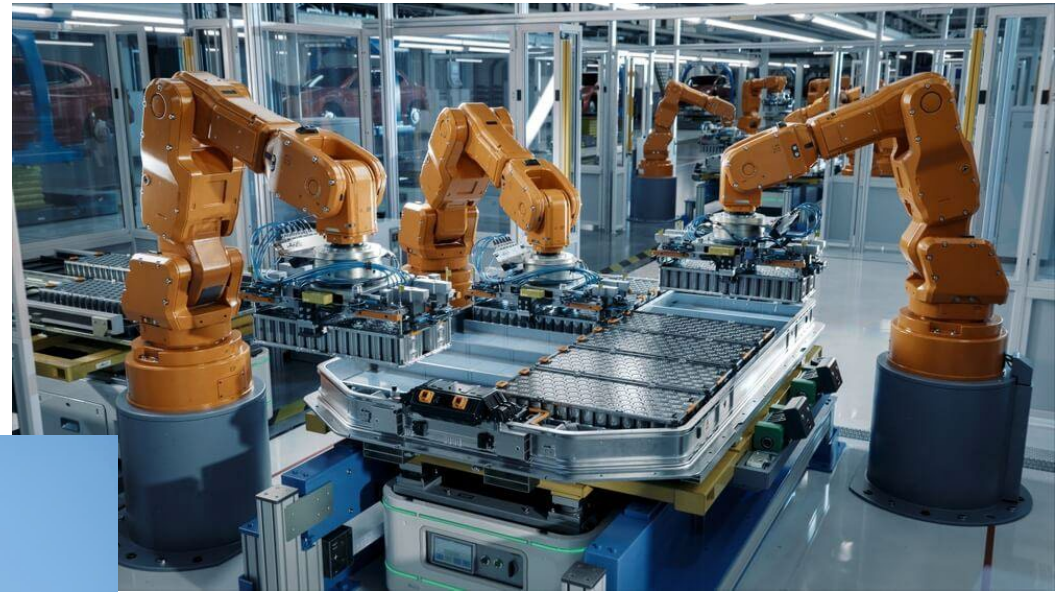
Characteristics of time-critical applications

- Time-critical applications require relatively low latencies, with low error rates.
- This means that time-critical application usually require **end-to-end (conversational) communication protocols** for reliable data transfer.
- Therefore, for time-critical applications, usually **each device is connected to the Internet and has an IP address**.
- **Examples:** Ordinary Internet applications, connected intelligent machines and various surveillance applications.

Protocol stack for time-critical applications



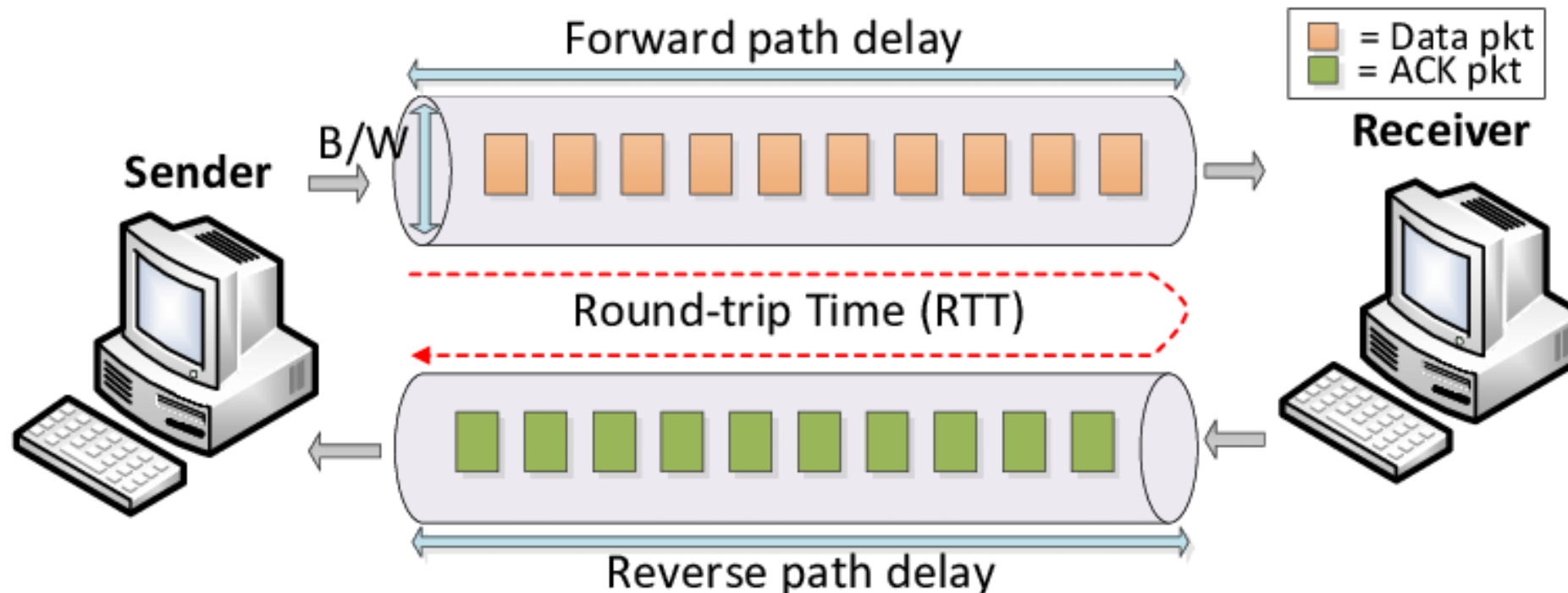
Time-critical applications - Examples



Images: <https://www.kaspersky.com/resource-center/threats/top-10-online-gaming-risks>
<https://iotbusinessnews.com/2024/03/13/06556-tele2-and-foodora-in-revolutionary-collaboration-connected-drones-deliver-food-from-the-sky-to-the-doorstep/>
<https://ibtinc.com/learn/industrial-automation-future-trends/>
<https://thenetworkinstallers.com/blog/applications-of-video-surveillance/>
<https://www.aftermarketnews.com/connected-vehicles-need-right-to-repair/>

High bit rates with High latency ?

NO! Due to the conversational transport and application layer protocols (as TCP, QUIC, HTTP etc) for error and flow control.

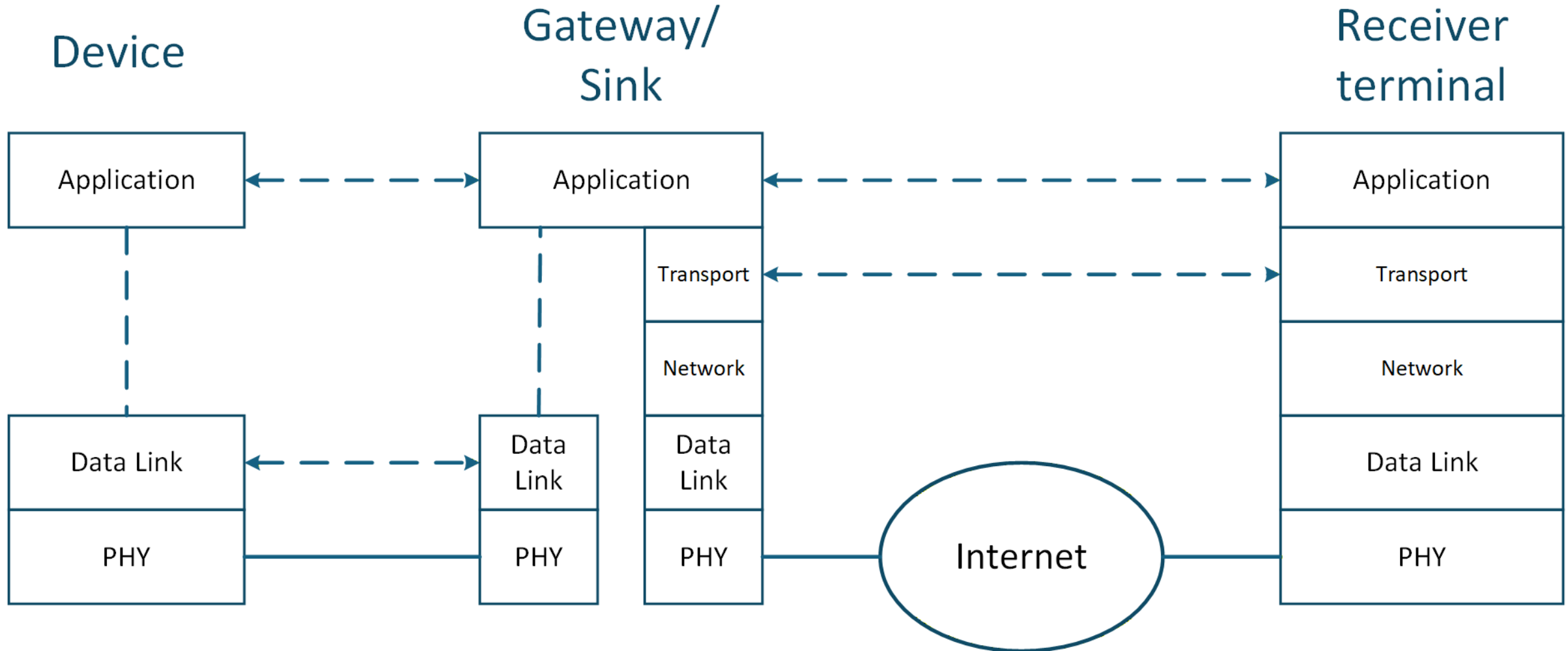


Non-critical applications

Characteristics of non-critical applications

- Applications that can tolerate some latencies and some packet (data) loss.
- Non-critical applications can operate without end-to-end protocols for reliable data transfer. In this case, **each device does not have to be connected to the Internet.**
- Instead, devices may only communicate with a unit (called gateway or sink), which is connected to the Internet (i.e. the unit has an IP address). This means that the **devices only have physical addresses.**
- Some non-critical applications (but not all!) use **resource-constrained devices** (battery-powered sensors).
 - Resource-constrained devices require communication with low energy consumption, which means low data rates.
- **Examples: Animal and environmental monitoring, sensor applications, interplanetary communication.**

Protocol stack for non-critical applications



Non-critical applications - Examples



Images:

<https://bisresearch.com/news/top-five-technological-developments-in-livestock-monitoring-and-management-system>

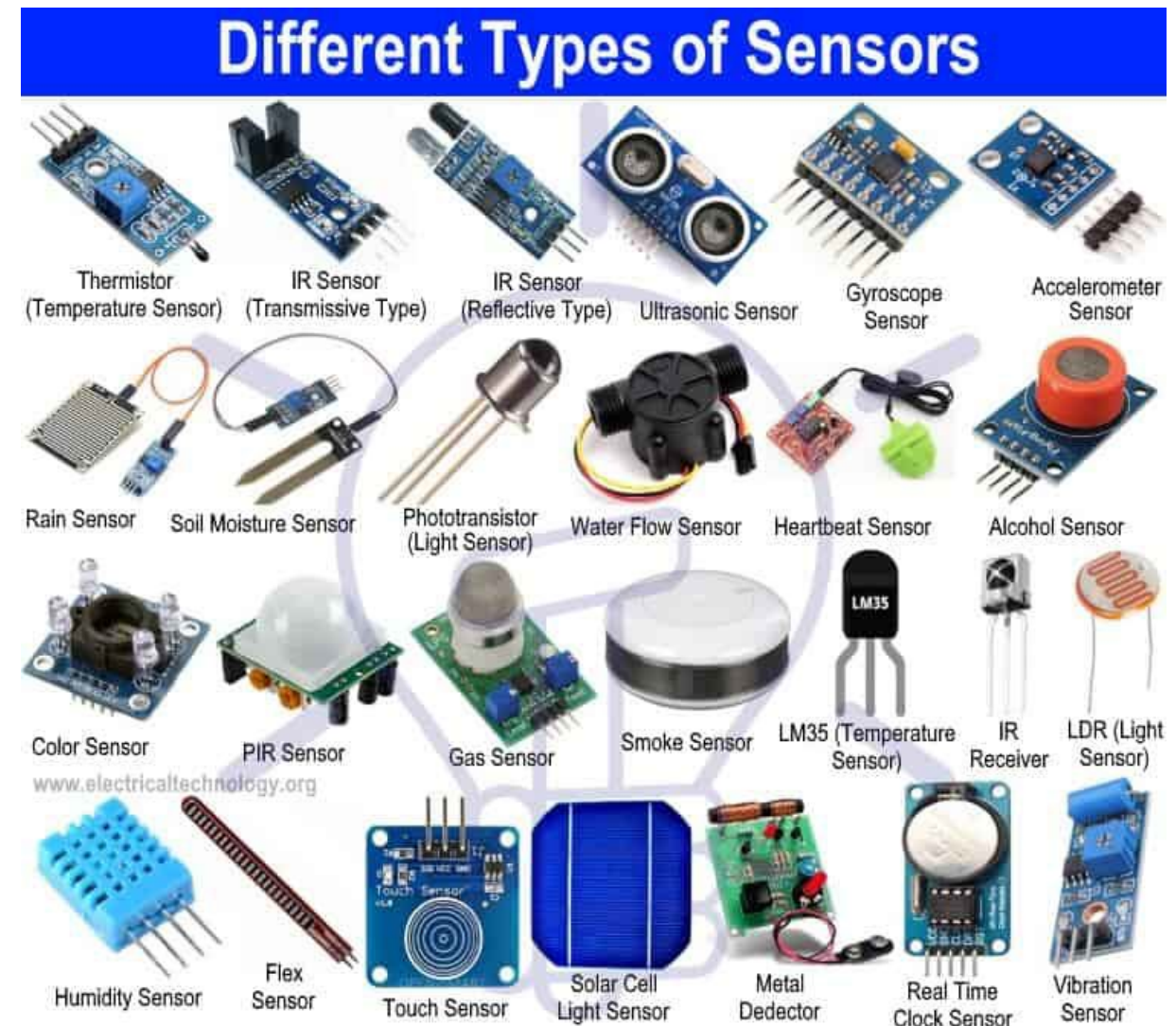
<https://hemnix.se/products/carvallo-solardrivet-4g-viltkamera-med-livestreaming-och-rrelsedetektering>

<https://infisim.com/blog/iot-in-environmental-monitoring>

<https://www.philips-hue.com/sv-se/p/hue-white-and-color-ambiance-essential-startpaket-3-e27-smarta-ljuskallor-806-lm/8721103103673>

Resource-constrained devices

- Resource-constrained devices are devices with strict limits on computing power, memory, storage, and battery life, often operating as a sensor.
- A sensor is a device that detects a physical condition or property, such as temperature, pressure, vibration, flow, or current, and converts it into a signal that can be measured, recorded, or used to trigger an action.



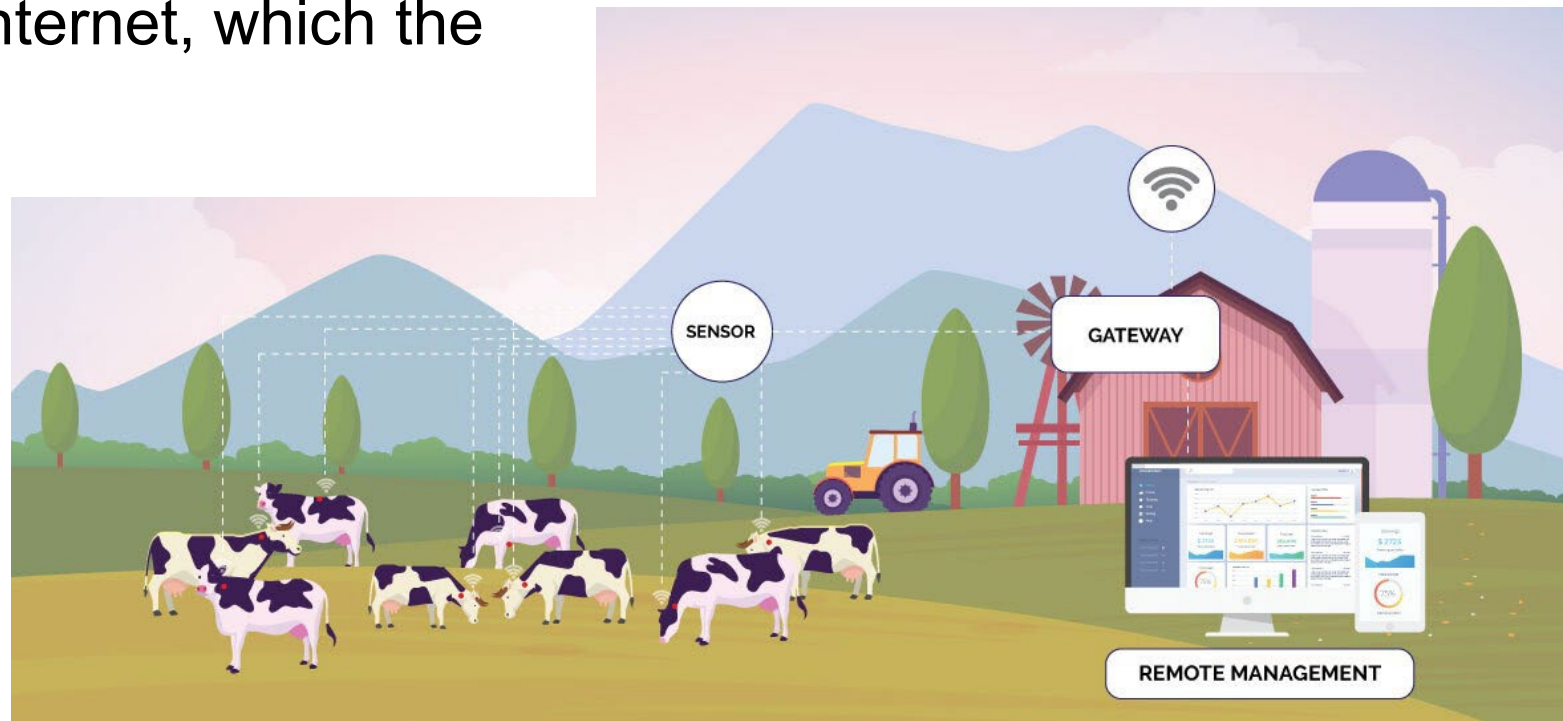
Resource-constrained devices - Properties

- Low power devices that include small batteries or energy-harvesting setups, requiring high energy efficiency.
- Devices with minimal CPU capacity and limited memory, limiting heavy processing.
- Require lightweight communication protocols, i.e not TCP/IP protocols.

Type of application?

You have been given the task to design a communication system for a farmer that wants to monitor cattle including about 20 animals. The cattle are in a pasture close to the farm. Each cow carries a sensor. There should be an update from each animal with an interval of about one hour (you do not have to care about the content of the update). The update should be sent to a cloud server placed on the Internet, which the farmer can access when checking the cattle.

Describe a suitable network system for the monitoring of the cattle.



Solution

- The farmer wants to monitor the cattle, with an update period of 1 hour.
- The data rate from each sensor is probably low. Also, it is probably ok with some data loss.
- The system can operate without end-to-end protocols for reliable data transfer.
- Each sensor does not need a direct Internet connection, which means that we do not need the sensors to have IP addresses.
- The sensors use a battery that may be hard to re-charge. If so, the sensors are resource-constrained.



Non-critical application

Wireless (access) networks

Basic network technology categories (in this course)

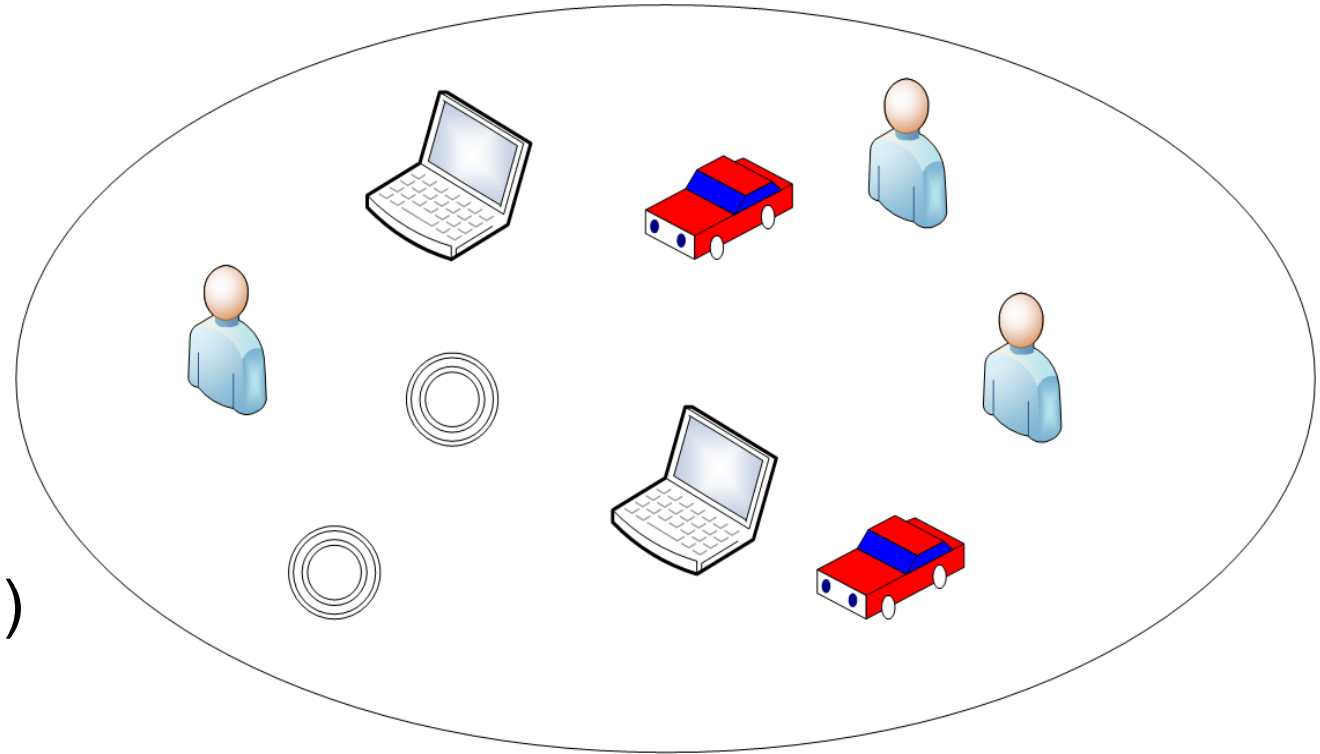
- **Fast-speed wireless networks** deliver high bit rates data with low latency.
 - Examples in the course: 4G/5G cellular networks, IEEE 802.11 (WiFi), Starlink
- **Low-power wide area networks** are designed to transmit small data packets over long distances while maximizing battery life.
 - Examples in the course: NB-IoT/LTE, LoRa, Argos, (Iridium)
- **Wireless Personal Area Networks** are designed to connect electronic devices within shorter ranges.
 - Examples in the course: Bluetooth, Bluetooth Low Energy, ZigBee

The wireless (access) network

The wireless (access) network provides **data transmission** to and from hosts.

Required for a wireless network:

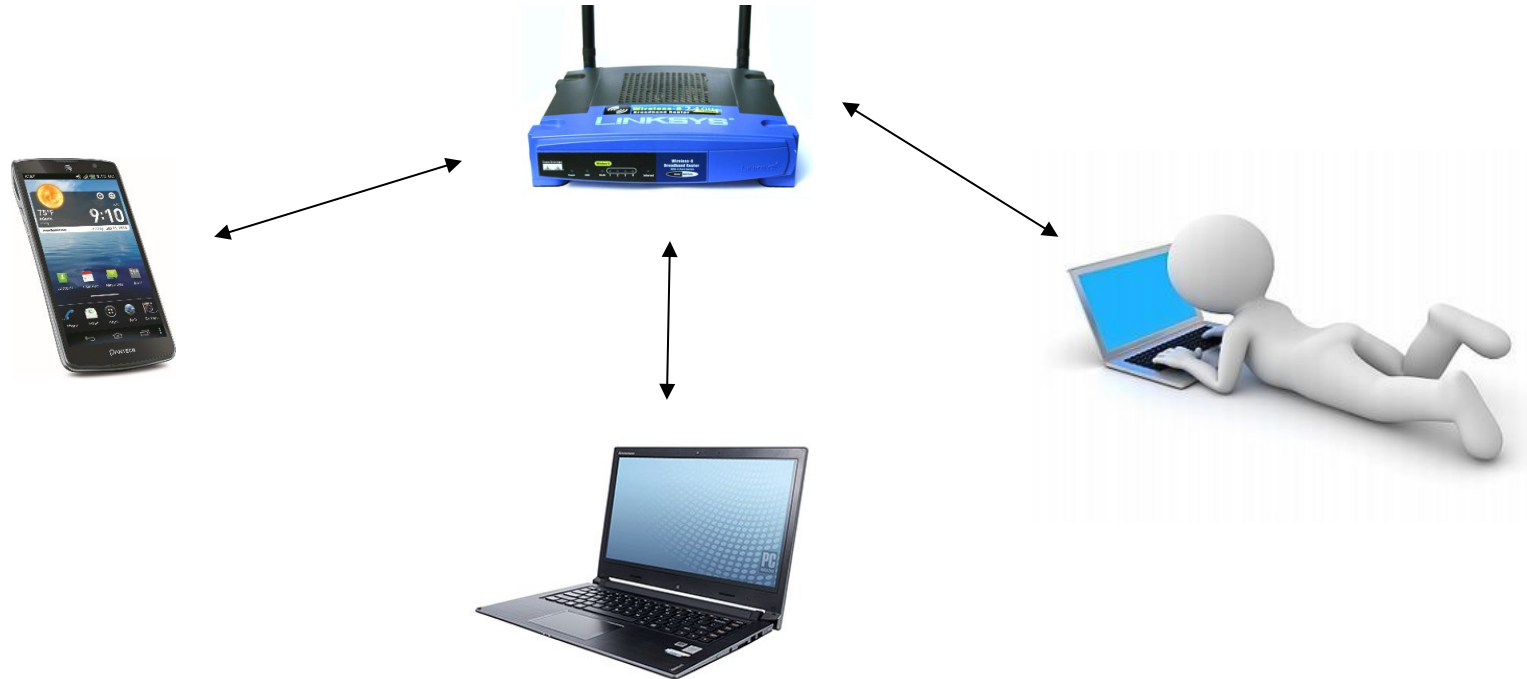
- Communication technology
- Communication protocols
- Backhaul link
- Power supply
- Optional: Positioning (Localization)



Wireless communication

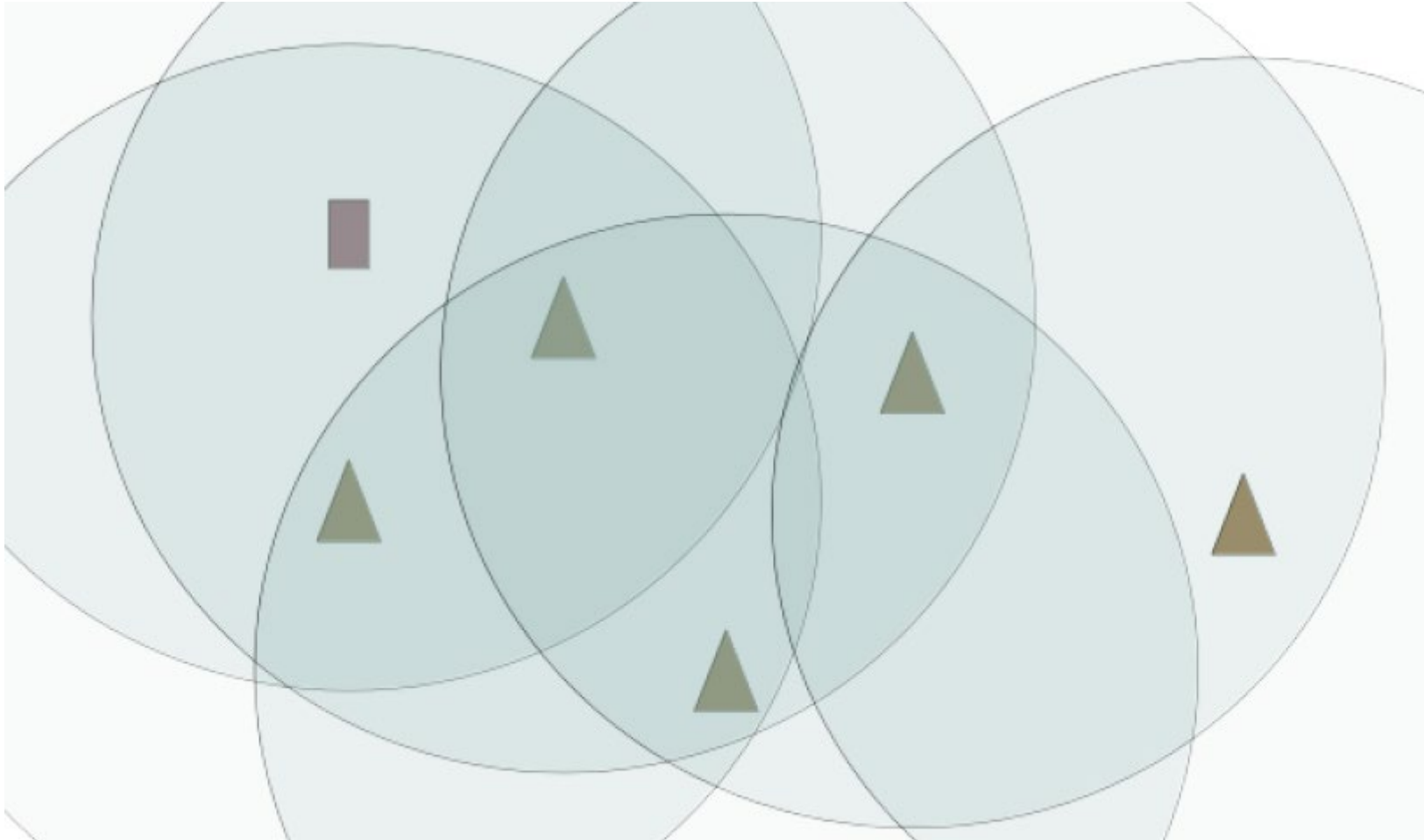
The wireless physical media is shared

A wireless link (medium, channel) is always shared with others



Interference in wireless networks

In wireless networks, overlapping regions covering multiple nodes, which cause interference.



Some key characteristics of a wireless communication channel

- All data transmitted on a wireless channel reaches all terminals (broadcast).
- Due to transmission impairments (on Earth), the **communication will have a limited range**.
 - In space, the communication range is basically unlimited.
- If two terminals send data at the same time on the same frequencies without specific coding, there will be a **data collision** and the data will be destroyed.

Wireless communication technologies

There are three basic types of **wireless** communication technologies that are used:

- **RF communication (radio)**
 - Earth, Underwater, Outer space
- **Optical communication (light)**
 - Earth (with restrictions), Underwater, Outer space
- **Acoustic communication (sound)**
 - Underwater

We will mainly discuss technologies using radio communication in this course.

However, optical and acoustic communication technologies will be discussed in the lectures about interplanetary and underwater networks.

RF communication (Radio)

- The **radio spectrum** is the part of the electromagnetic spectrum with frequencies from 3 Hz to 300 GHz.
 - The radio spectrum is divided into **radio bands** and shared according to international standards.
- A **radio band** is a small contiguous section of the radio spectrum frequencies, in which **channels** are usually used or set aside for the same purpose.
 - To prevent interference and allow for efficient use of the radio spectrum, similar services are allocated in the same radio band.

ITU standardized radio bands

Band name	Frequency band
Extremely low frequency (ELF)	3-30 Hz
Super low frequency (SLF)	30-300 Hz
Ultra low frequency (ULF)	300-3000 Hz
Very low frequency (VLF)	3-30 kHz
Low frequency (LF)	3-300 kHz
Medium frequency (MF)	300-3000 kHz
High frequency (HF)	3-30 MHz
Very high frequency (VHF)	30-300 MHz
Ultra high frequency (UHF)	300-3000 MHz
Super high frequency (SHF)	3-30 GHz
Extremely high frequency (EHF)	30-300 GHz
Terahertz (THz)	300-3000 GHz

} Used for communication with submarines

IEEE Radar bands for satellite communication

IEEE has defined the following frequency bands for satellite communication (space).

Band	Approx. Range of Wavelengths (cm)	Approximate Frequencies
UHF	100 - 10	300 - 3000 MHz
L	30 - 15	1 - 2 GHz
S	15 - 7.5	2 - 4 GHz
C	7.5 - 3.75	4 - 8 GHz
X	3.75 - 2.4	8 - 12 GHz
K	2.4 - 0.75	12 - 40 GHz
Q	0.75 - 0.6	40 - 50 GHz
V	0.6 - 0.4	50 - 80 GHz
W	0.4 - 0.3	80 - 90 GHz

Licensed v. Unlicensed frequency bands

Within each radio band, there can be licensed and/or unlicensed frequency bands.

- A **licensed frequency band** is "owned" by a specific operator. Each country has an authority that distributes these bands. In Sweden, it is the Swedish Post and Telecom Authority (PTS) that controls the radio spectrum.
 - Advantage: No disturbances from other services.
 - Disadvantage: Only open for specific operators, and with fees.
- **Unlicensed frequency bands**, the **ISM (Industrial, Scientific, Medical) bands**, are open for anyone to use.
 - Advantage: Free to use.
 - Disadvantage: Disturbances from other services.

Optical wireless communication

- Optical wireless communications (OWC) span a frequency range roughly from **300 THz to 30,000 THz**, in which unguided visible, infrared (IR), or ultraviolet (UV) light is used to carry a signal.
- Optical wireless communication usually **require line-of-sight** between transmitter and receiver, which entails some sort of direction tracking to maintain the communication link.
- There are several international standards for the use of optical wireless communication on Earth.
 - One example is **Visible light communication (VLC)**, also called LiFi, which can be used for indoor applications.

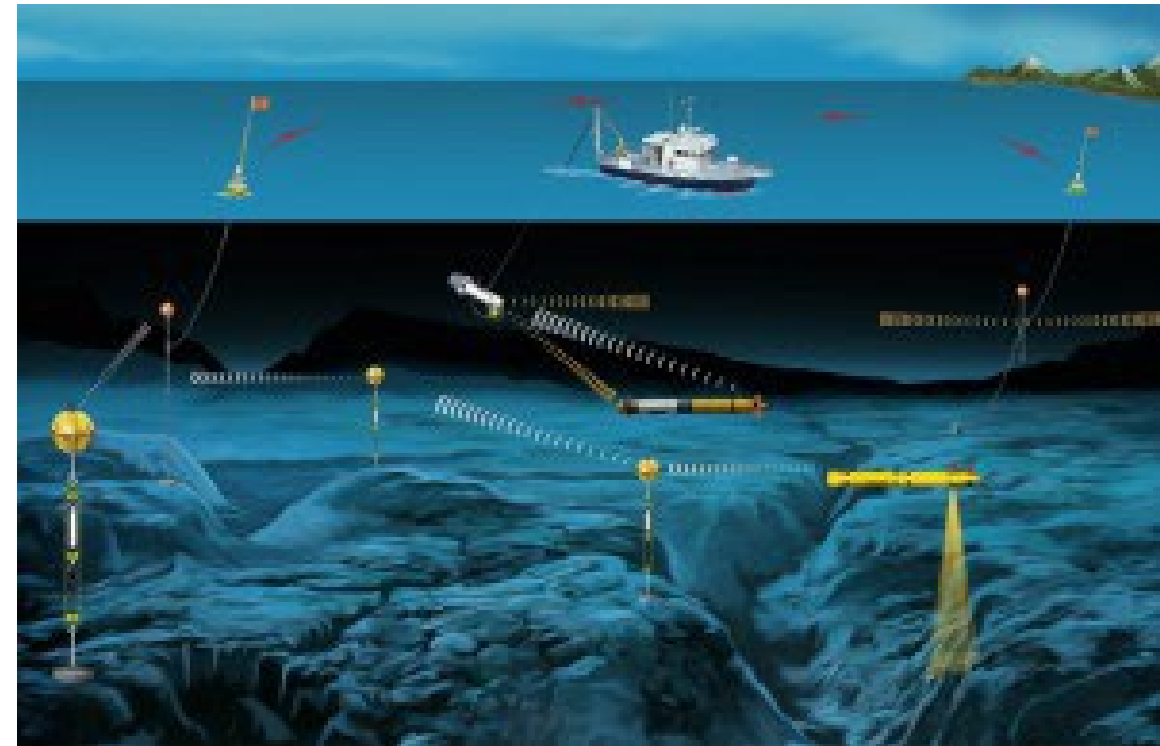


Source: https://en.wikipedia.org/wiki/Optical_wireless_communications
https://en.wikipedia.org/wiki/Visible_light_communication

Image By Volker Jungnickel - https://www.researchgate.net/profile/Volker_Jungnickel, CC BY-SA 4.0,
<https://commons.wikimedia.org/w/index.php?curid=83820047>

Acoustic communication

- Acoustic communication is currently being the dominant technology for **wireless underwater communications**.
- The speed of propagation, c , of acoustic waves in fluids is very limited, about 1500 meters per second. The parameters affecting the speed of propagation play a major role in acoustic-based communications.
- Transmission impairments increase considerably when the frequency and the distance between transmitter and receiver increases.



Data transmission modes

- **Simplex**

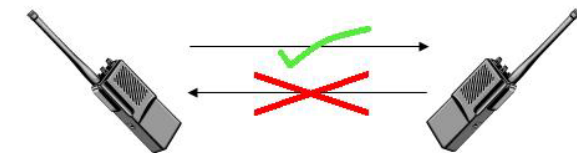
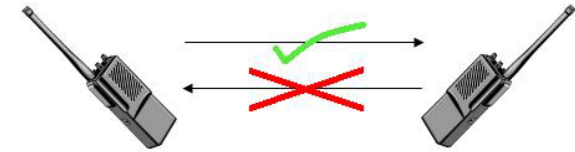
- Only one of the two devices on a link can transmit, the other can only receive.
- **One communication channel that is open to send data in one direction.**

- **Half-duplex (or semiduplex)**

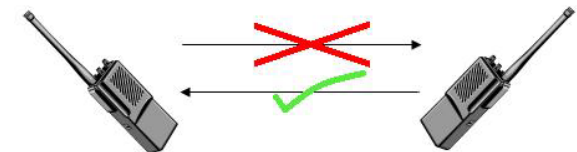
- both parties can communicate with each other, but not simultaneously.
- **One communication channel that is open in one direction at a time.**

- **Full-duplex**

- Both parties can communicate with each other simultaneously.
- There are **two open communication channels** between the sender and receiver.



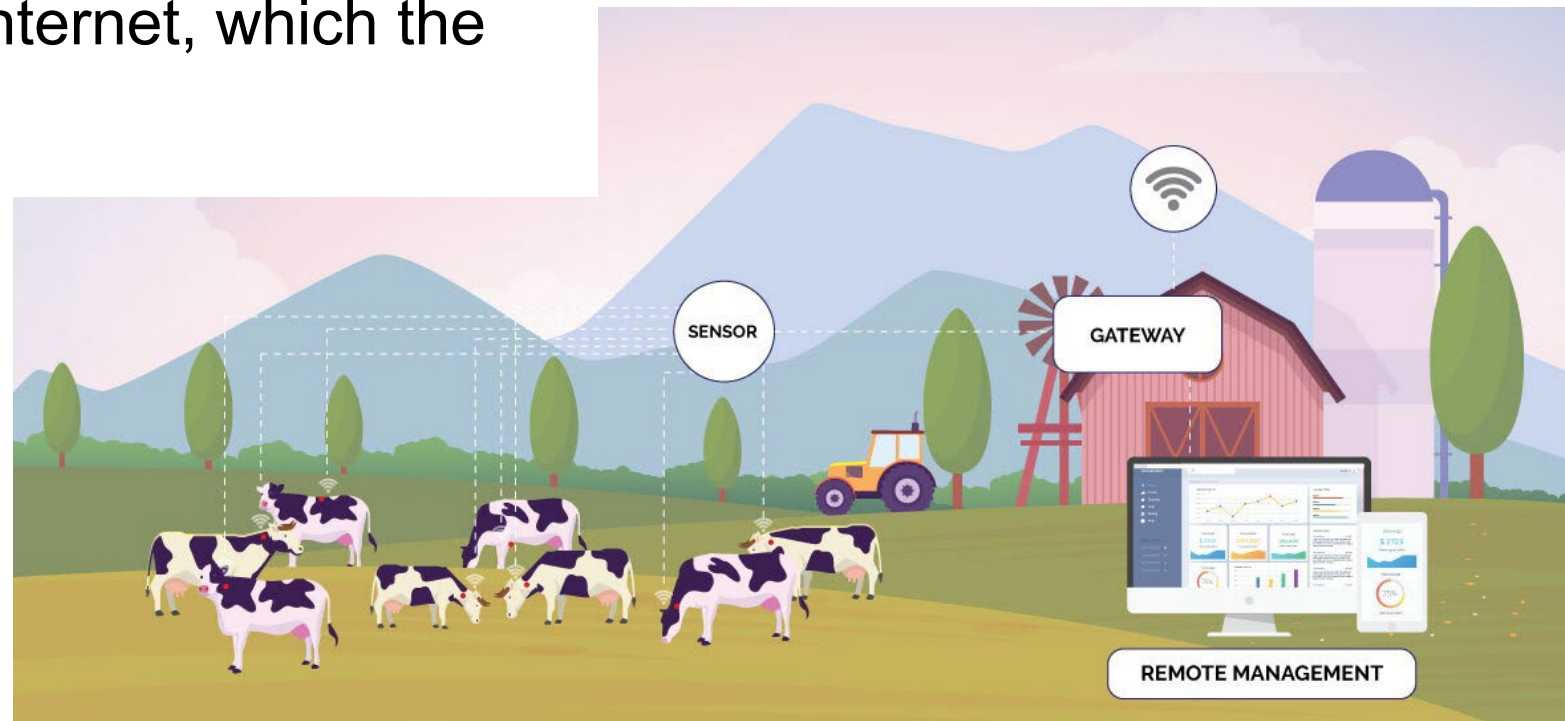
OR



Communication technology?

You have been given the task to design a communication system for a farmer that wants to monitor cattle including about 20 animals. The cattle are in a pasture close to the farm. Each cow carries a sensor. There should be an update from each animal with an interval of about one hour (you do not have to care about the content of the update). The update should be sent to a cloud server placed on the Internet, which the farmer can access when checking the cattle.

Describe a suitable network system for the monitoring of the cattle.



Suggested solution

Communication technology

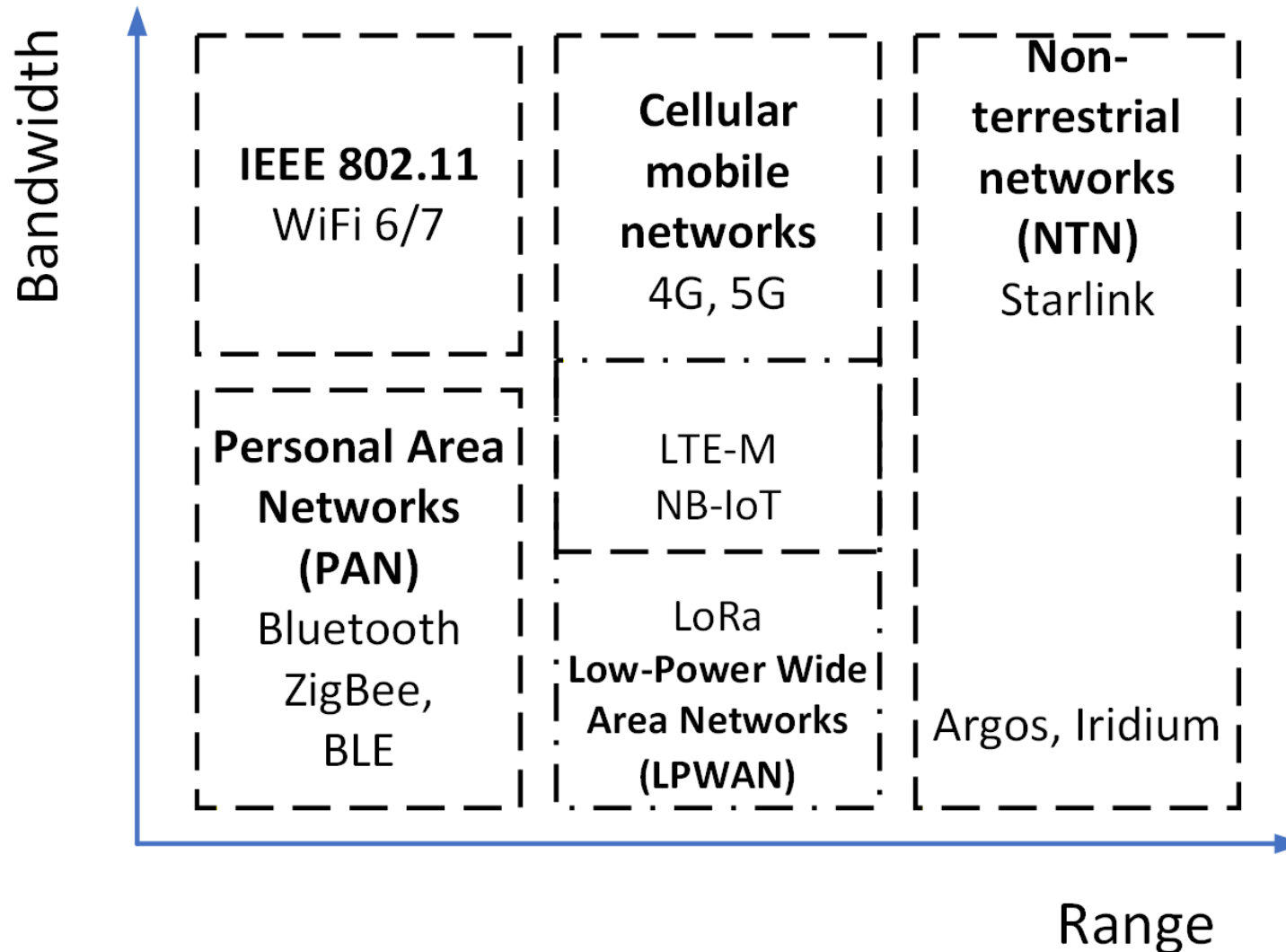
- Cows -> Homestead
 - Probably radio communication
- Homestead -> Internet and Internet -> Data center
 - Probably wired (Either copper or optical fiber)

Data transmission mode

- Cows -> Homestead
 - Could use half-duplex or simplex
- Homestead -> Data center
 - Full duplex (required for Internet protocols)

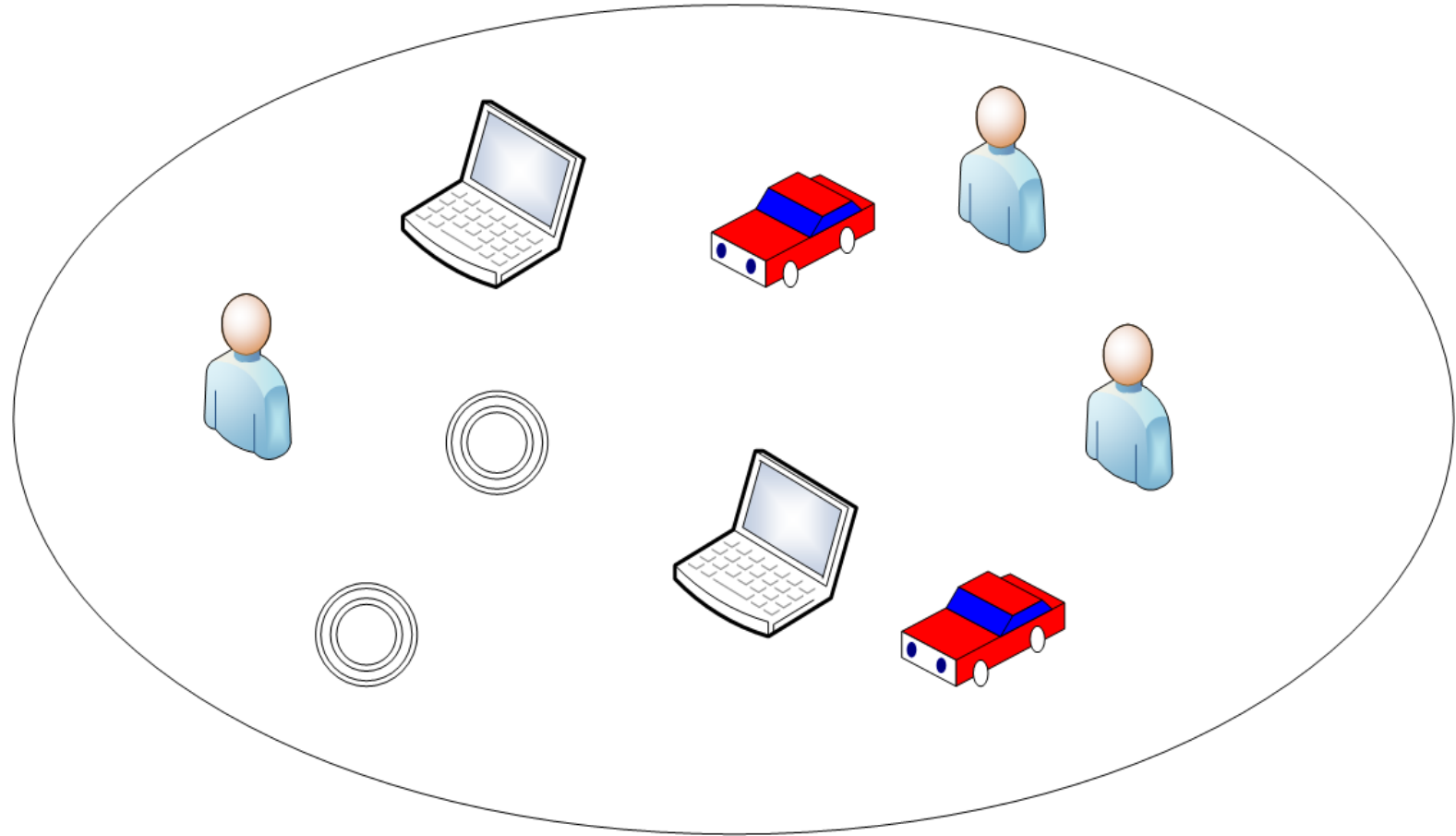
Communication protocols

Network technologies using radio communication in the course



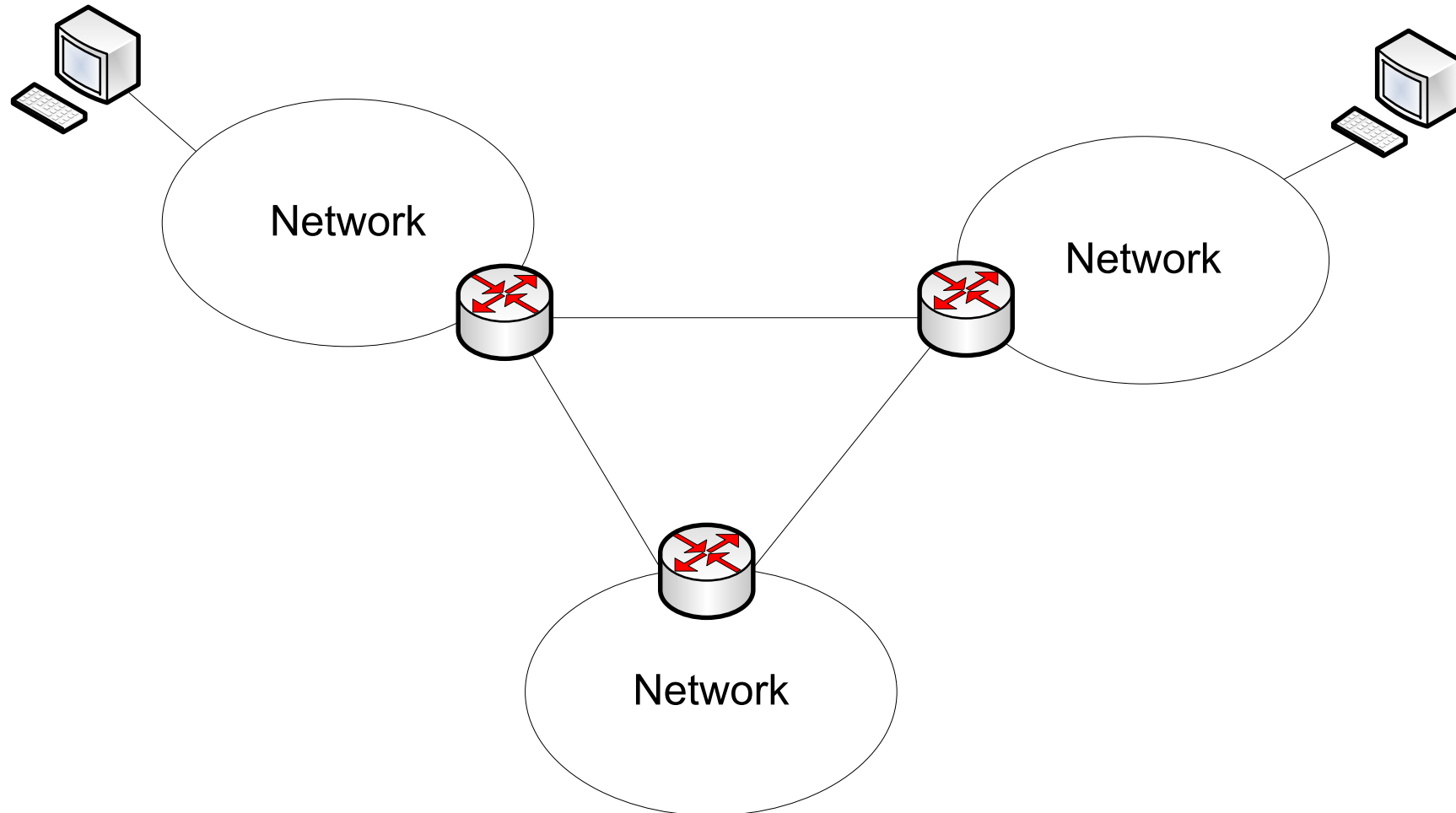
Network technology – Intranetworking protocols

- A network technology defines the protocols for communicating within a network using this network technology standard.
- All hosts within the network must follow the same communication protocols.



Internet communication

For communication between networks connected to the Internet, the TCP/IP protocols are always used.



Positioning (Localization)

Positioning of hosts

Positioning in this course refers to how to find the exact location of a host. Some common techniques:

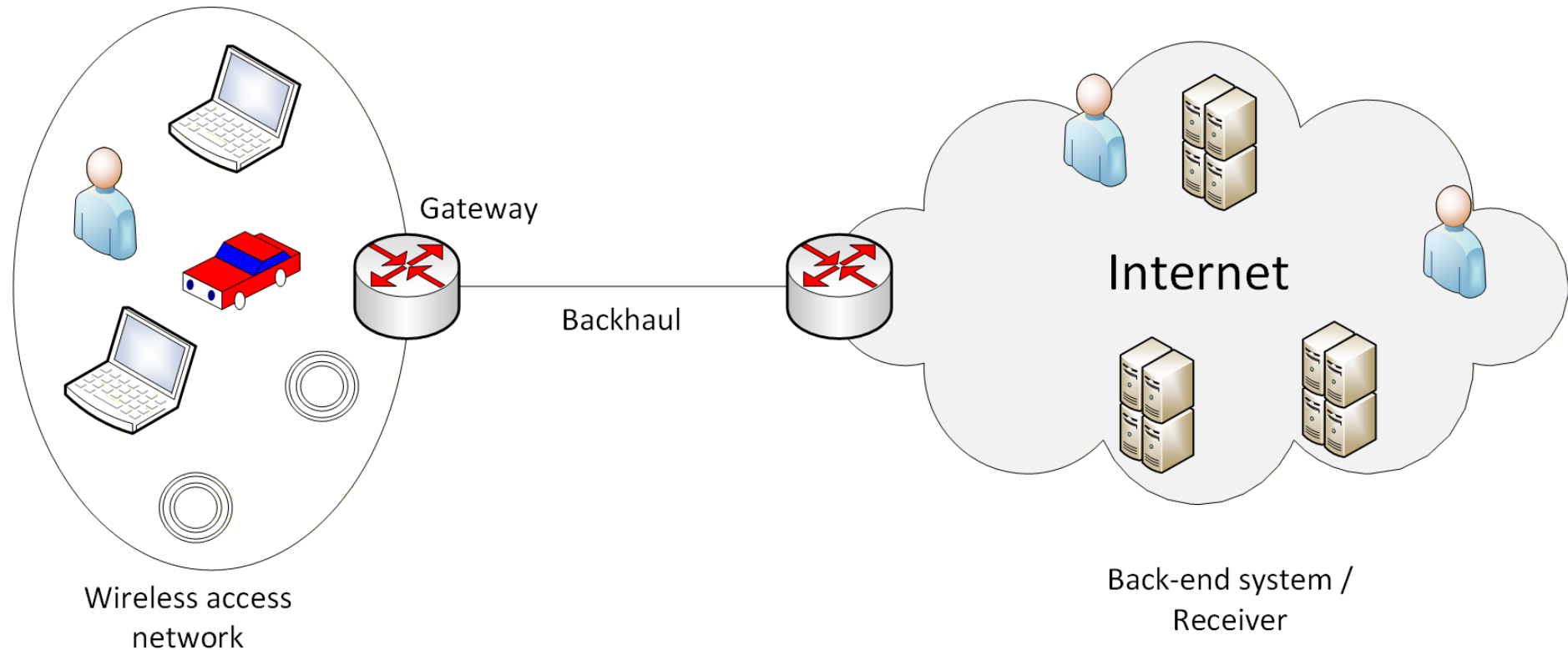
- **The Global Navigation Satellite System (GNSS)**
 - For outdoor positioning
 - Currently based of GPS (USA), GLONASS (Russia), BDS (China), and Galileo (EU)
- **An indoor positioning system (IPS)**
 - A network of devices used to locate hosts in places where GNSS does not work properly (for example, in buildings)
 - Use different technologies, including distance measurement to nearby **anchor nodes** (nodes with known fixed positions), also called **beacons**.



Backhaul link

The backhaul link

The backhaul link is required for the connection to the Internet (sometimes via a core network).



Traditional (fast-speed) backhaul

- Wired
 - **Optical fiber** (Ethernet, WDM or similar)
 - **Copper** (Ethernet)
- Wireless
 - **Microwave link**
 - Requires Line-of-sight (LOS)
 - Current commercial systems are relatively expensive and require access to power supply.
 - **Satellite link** with e.g. Starlink
 - **Cellular mobile network** (in specific scenarios)



Source: [https://en.wikipedia.org/wiki/Backhaul_\(telecommunications\)](https://en.wikipedia.org/wiki/Backhaul_(telecommunications))

Source: https://en.wikipedia.org/wiki/Microwave_transmission

Image by GeorgeLouis, CC BY 3.0, <https://commons.wikimedia.org/w/index.php?curid=34194053>

Image by Angelbo, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=3248879>

Power supply

Main methods for power supply

- **Mains powered**

- The device is connected to the electricity grid.
- Could also be another basically unlimited power source, for example a vehicle.
- **The device has unlimited power.**

- **Battery powered**

- The device has a battery.
- **The device has limited power.**

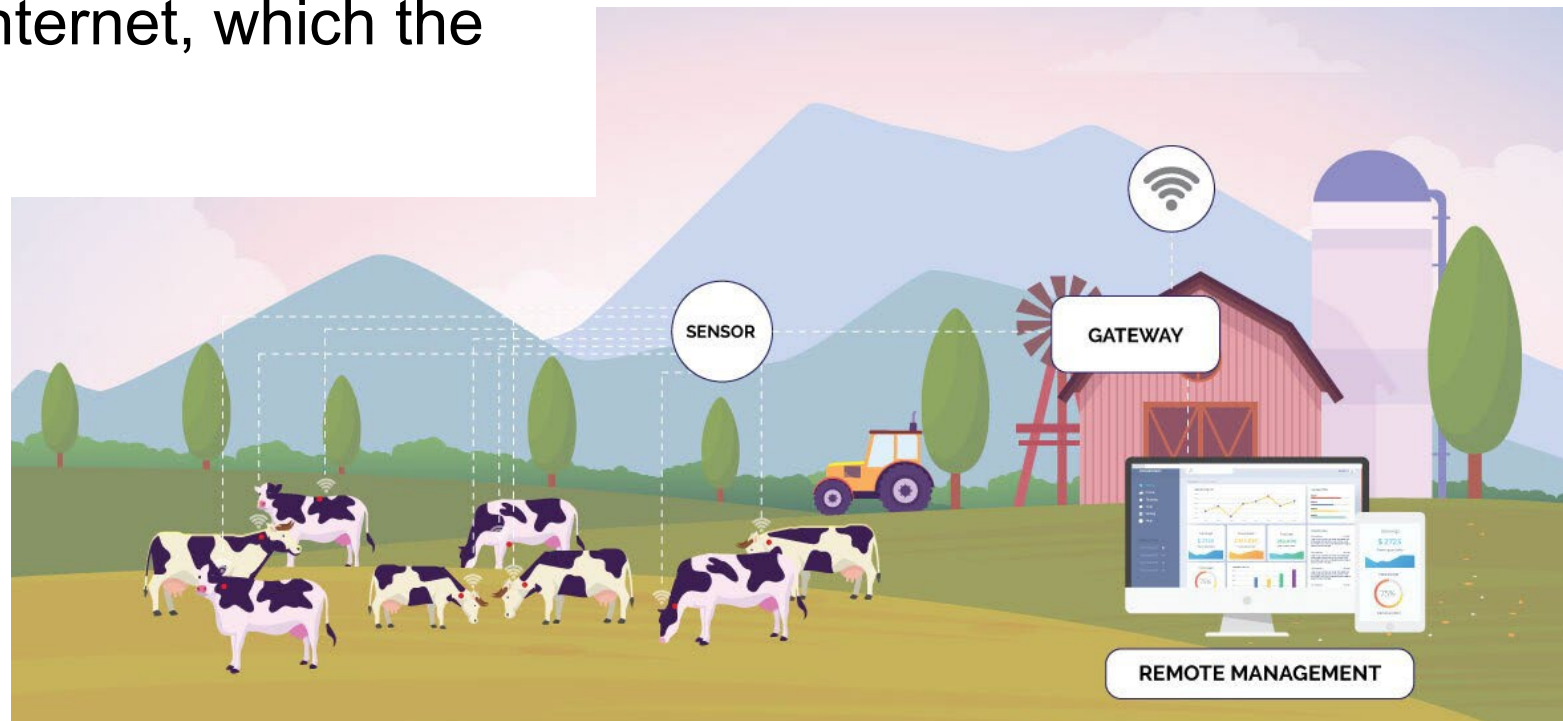
- **Energy harvesting**

- The device derives energy from an external source (but not the electricity grid), for example local solar cells.
- **The device may have very limited power depending on the external energy source.** For example, solar cells do not work during night.
- An energy harvesting can be combined with a battery for energy storage.

Positioning, Backhaul and Power supply?

You have been given the task to design a communication system for a farmer that wants to monitor cattle including about 20 animals. The cattle are in a pasture close to the farm. Each cow carries a sensor. There should be an update from each animal with an interval of about one hour (you do not have to care about the content of the update). The update should be sent to a cloud server placed on the Internet, which the farmer can access when checking the cattle.

Describe a suitable network system for the monitoring of the cattle.



Suggested solution

Positioning

- If the farmer wants to know the position of each cow, the sensors can include GPS trackers.

Backhaul

- Probably a **wired backhaul** if the farm is somewhere close to a town.
- Potentially, a wireless backhaul with e.g. **Starlink or mobile cellular networks**, if the farm is further out in a rural area.

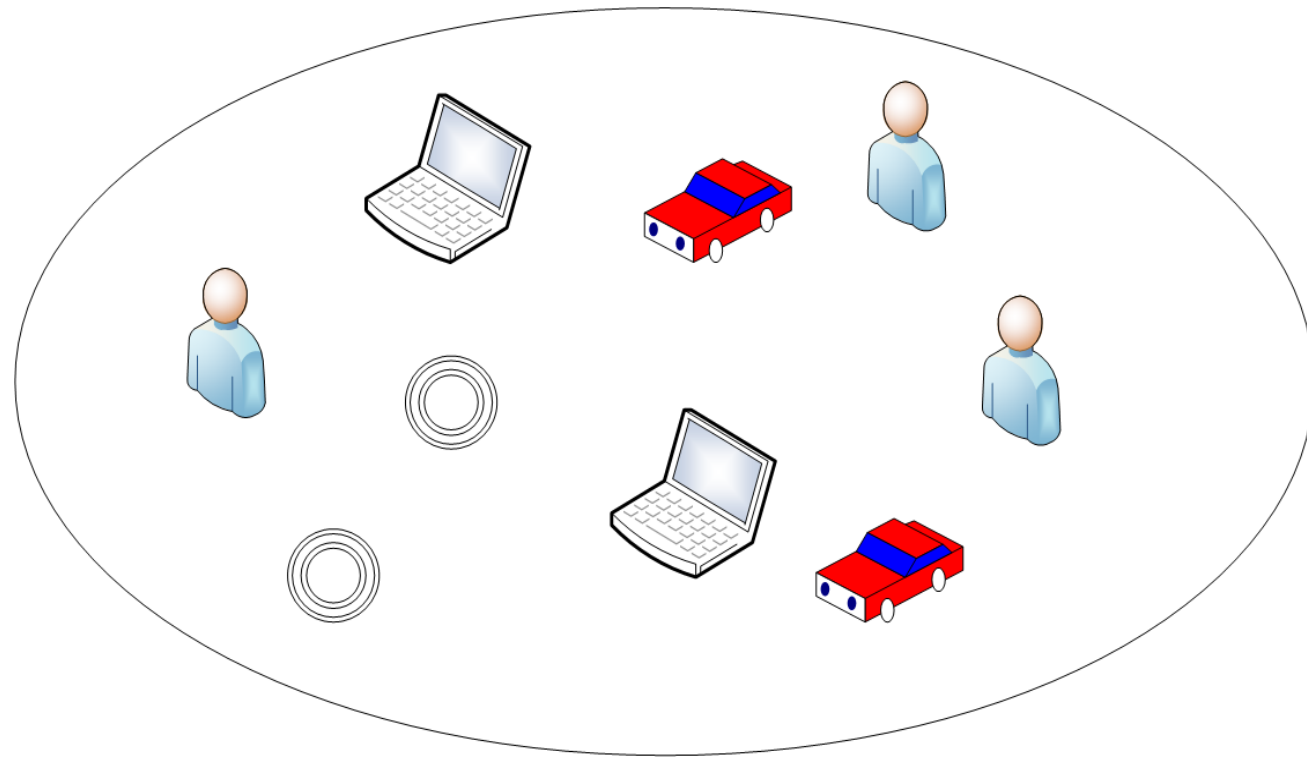
Power supply

- The **sensor devices** on each animal are probably **battery-powered**.
- The **router/gateway** and any other **infrastructure nodes** can be considered as **mains powered**, since the farm must be connected to the electricity grid.

Summary

The following mechanisms are required for all wireless networks connected to the Internet:

- Communication technology
- Communication protocols
- Backhaul link
- Power supply
- Optional: Positioning (Localization)





LUND
UNIVERSITY