



LUND
UNIVERSITY

Network architectures (in the course)

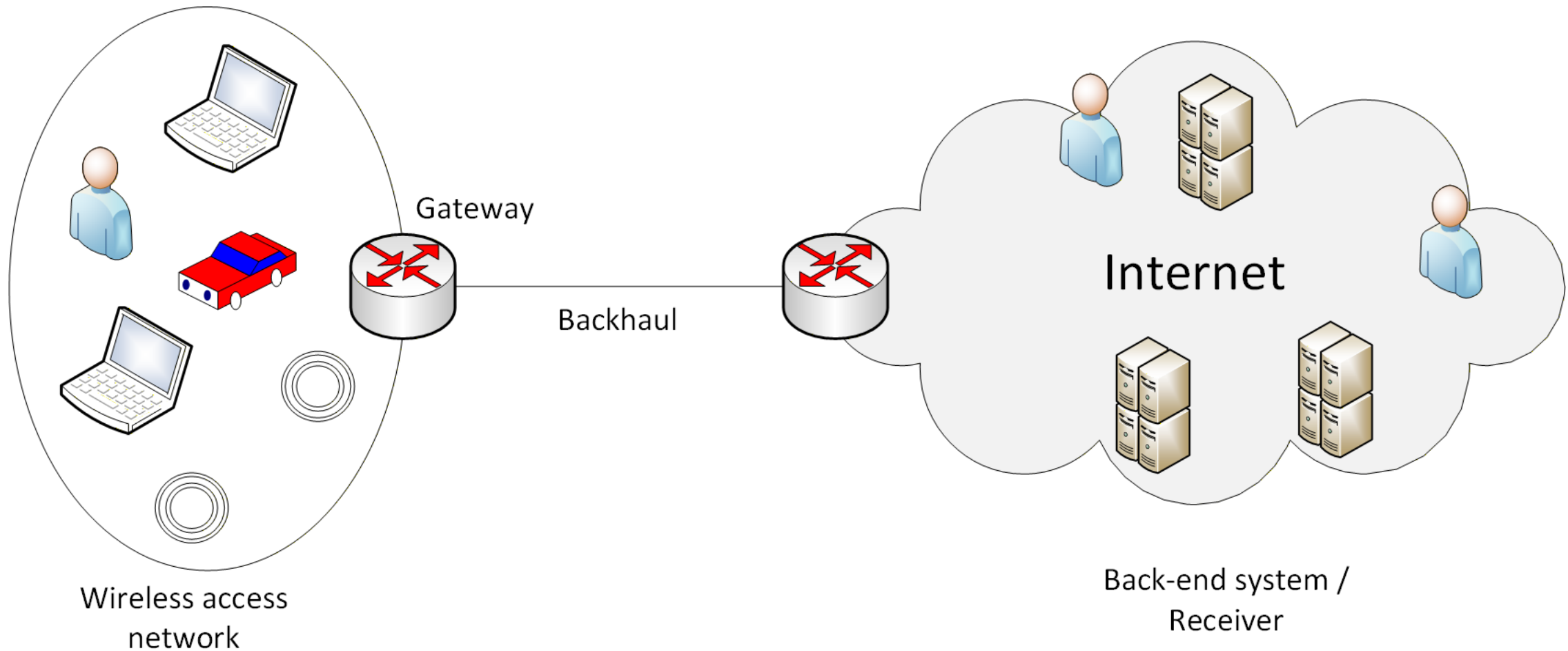
MARIA KIHLM



Literature

- Slides

This lecture: Network architectures



Today's scenario: The Greenhouse

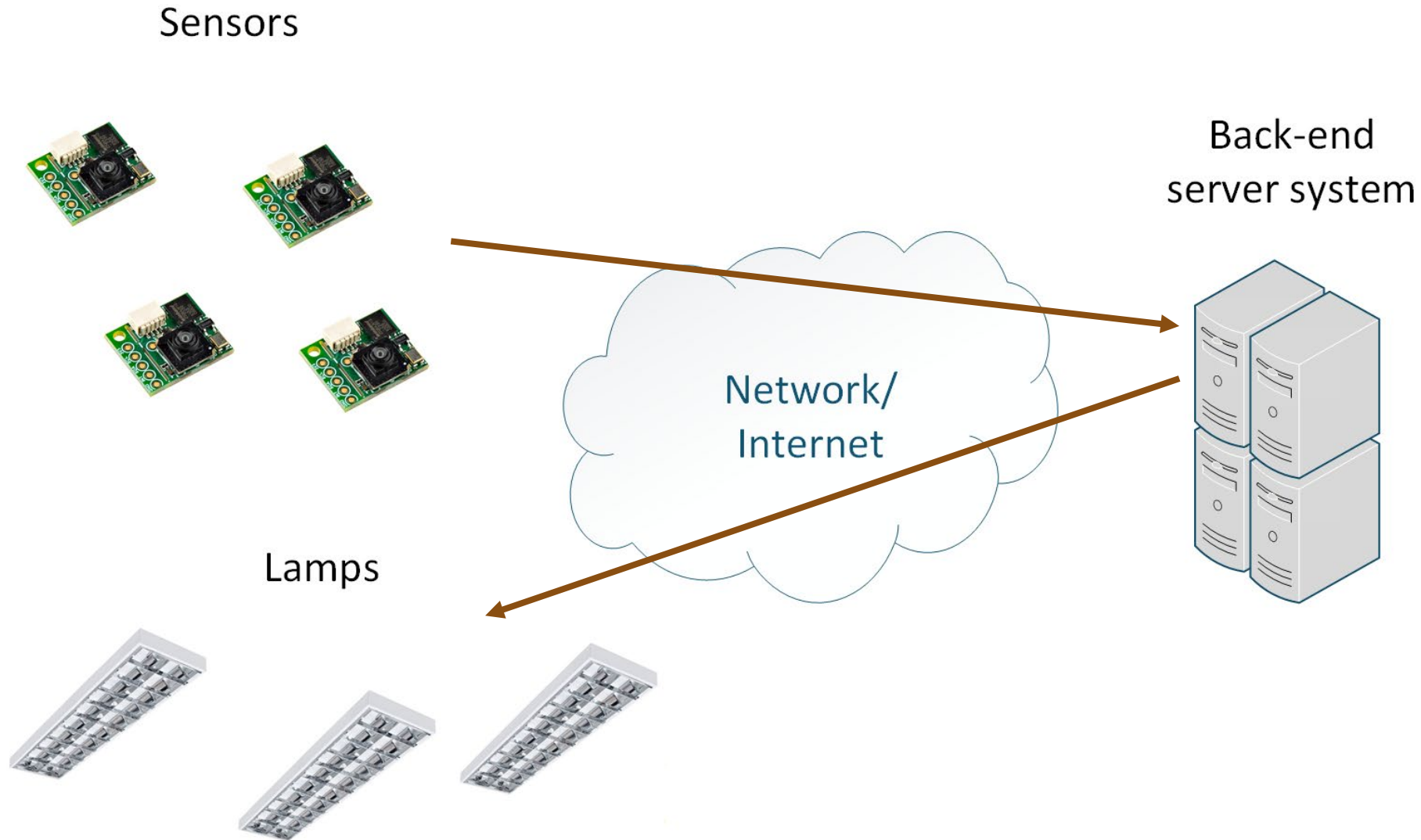
You have been given the task to help a friend that wants to install a smart lighting system for their greenhouse. The system includes about 10 sensors distributed in the greenhouse. Also, the system includes smart lamps that can be controlled via the Internet. The sensors collect and send data to a back-end server system.

The back-end server system includes an AI system that processes the data and then adjusts the lamps in the greenhouse so that the plants always have optimal light.

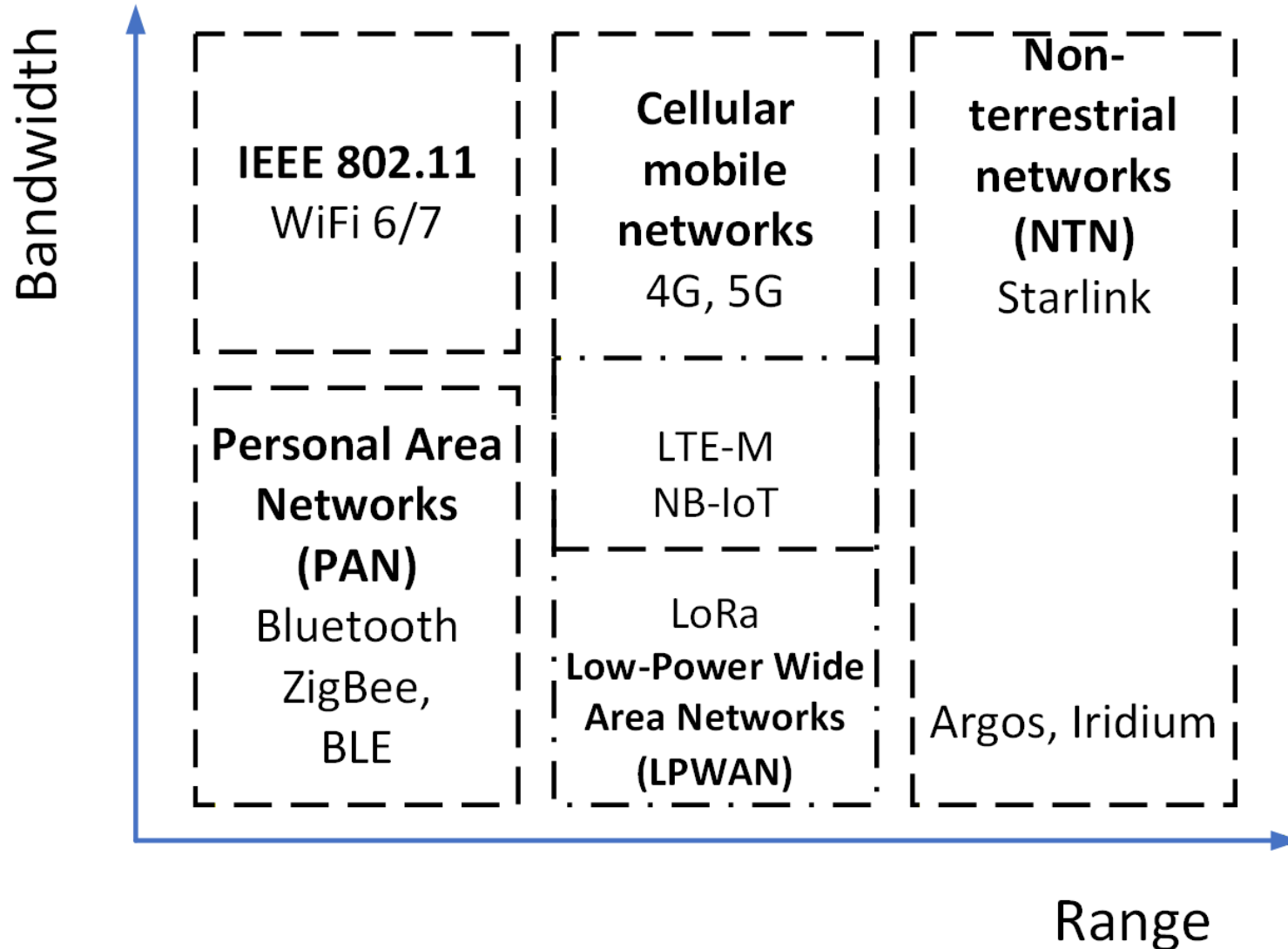
Your task is to suggest a solution for the complete networked system.



Basic networked system architecture



Network technologies in the course



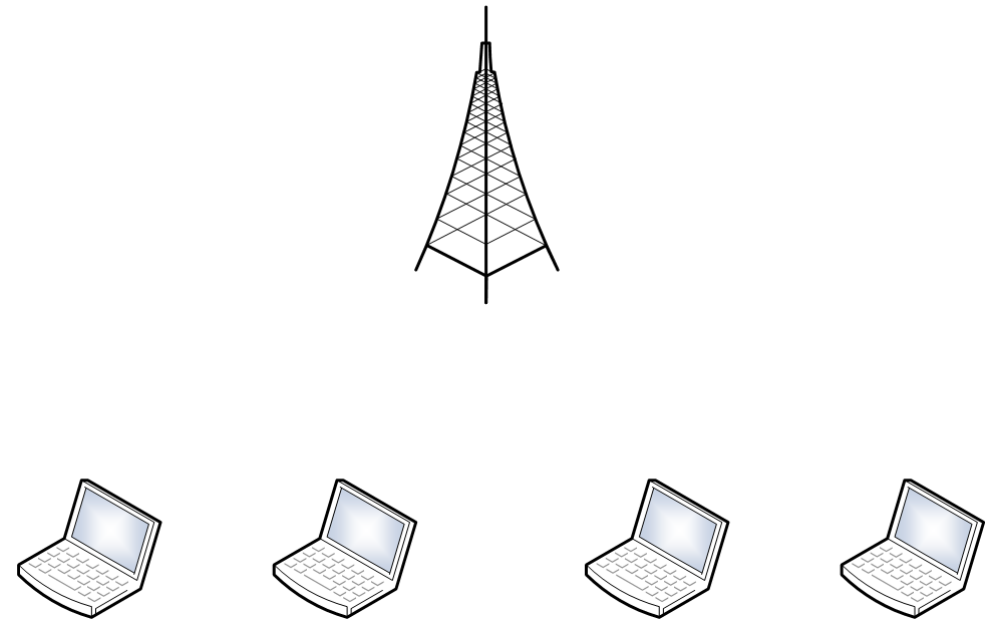
Basic wireless network architectures

- **Centralized architectures**
 - A Base station / Access point controls the data transmission.
- **Decentralized architectures**
 - Self-organized (ad-hoc) networks

Centralized network architectures

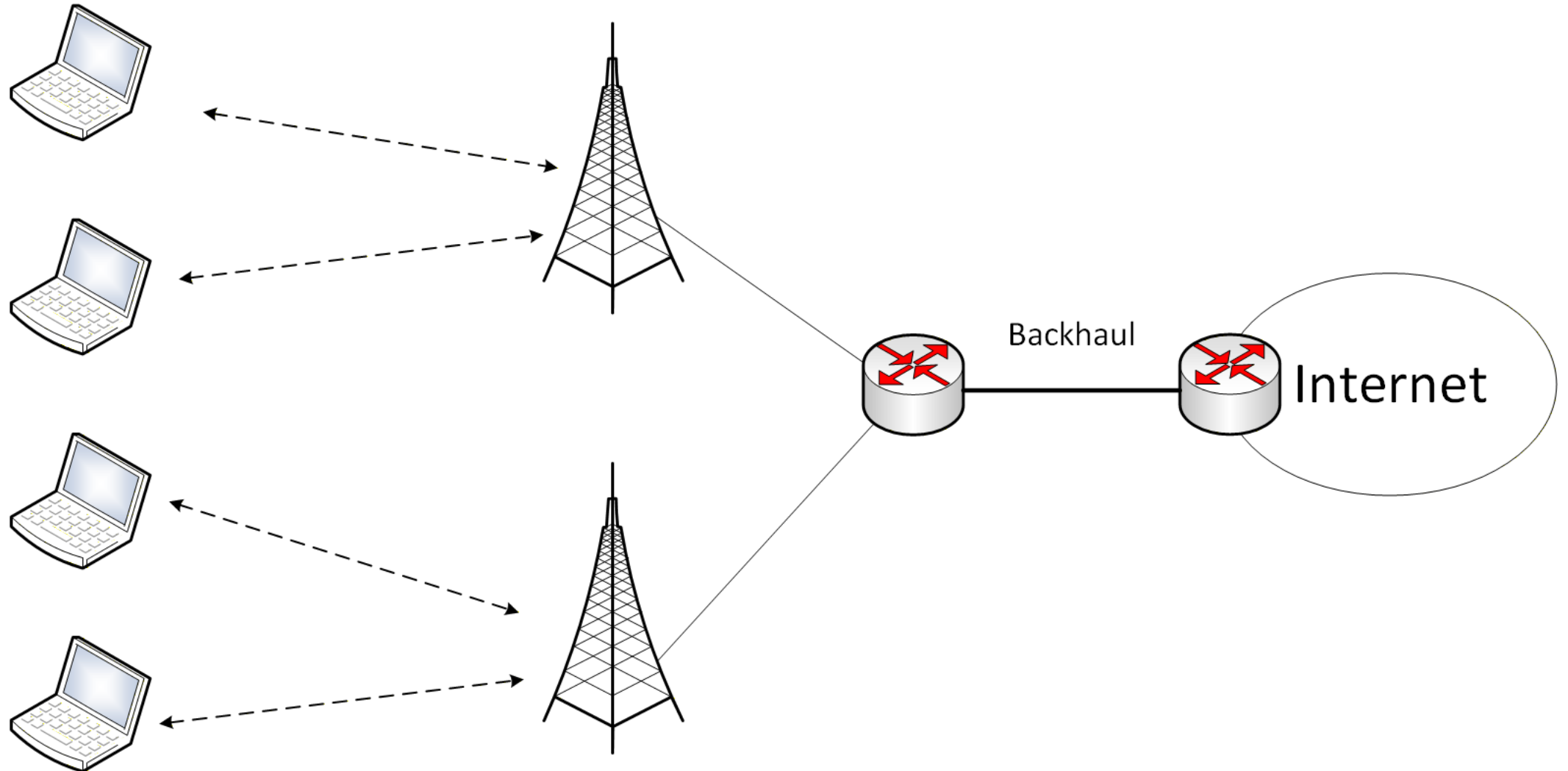
Centralized architectures – Main characteristics

- Connected devices communicates with a Base station / Access point.
- The base station is connected to a gateway/router that has access to the Internet.
- Depending on network technology, a host can send data to one or more base stations.
- A host usually need to set up a connection with the base station before the host can send data, i.e. connection-oriented data transfer.



Centralized architecture – basic structure

Not all centralized network technologies have exactly the same structure



Decentralized network architectures

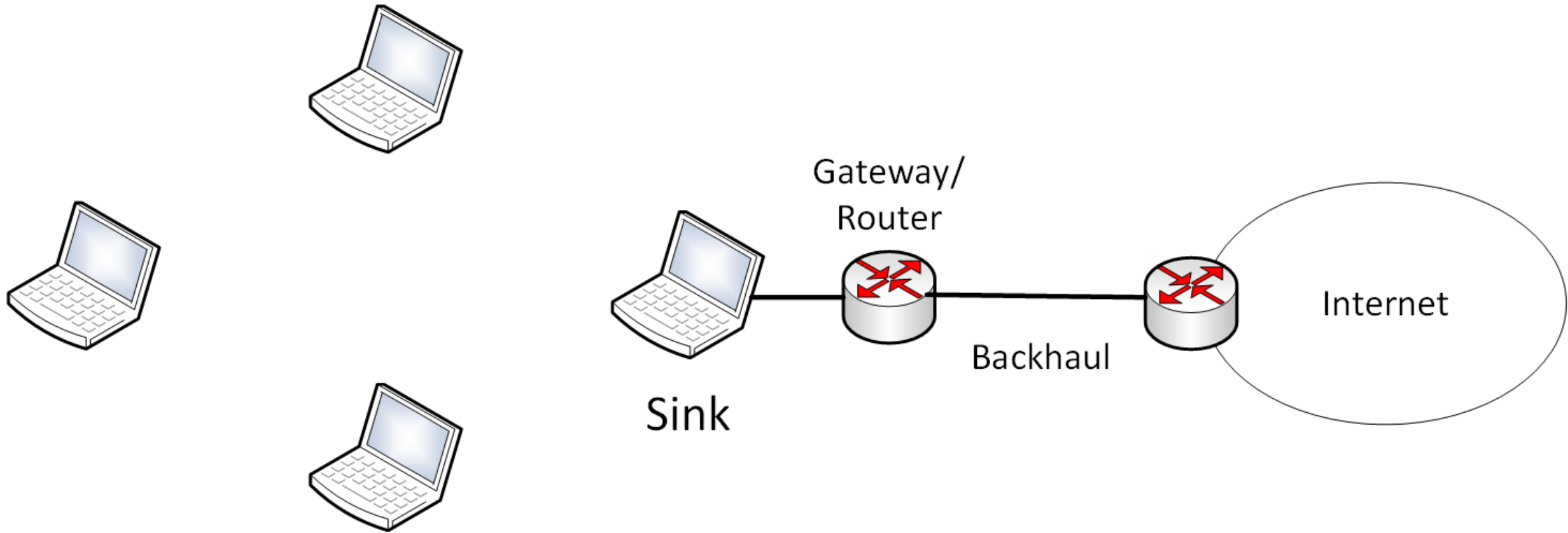
Decentralized architectures – Main characteristics

- Self-organized (ad-hoc) networks where hosts dynamically connect with each other.
- One or more hosts act as so called sinks or portals. A sink or portal has access to the Internet via a gateway (or act as a gateway itself).
- There is a **link between two hosts** if they are within radio range of each other.
- There needs to be common rules for how to forward data between hosts in the network, called a **routing protocol**.



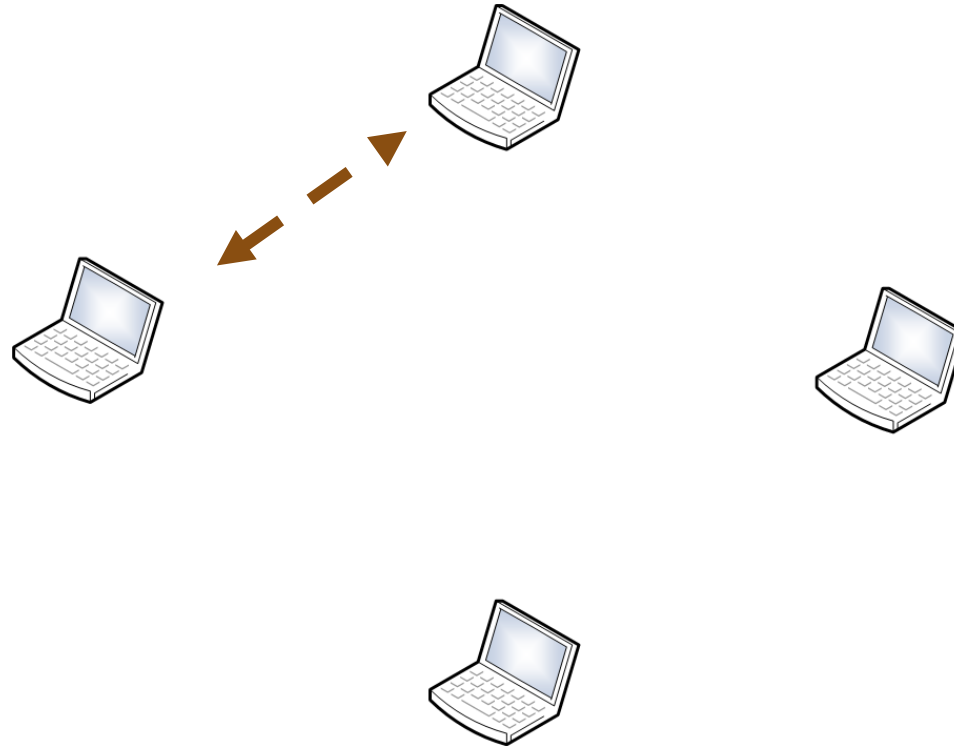
Decentralized architecture – Basic structure

Depending on network technology, not all hosts must have the same role in the data transfer.



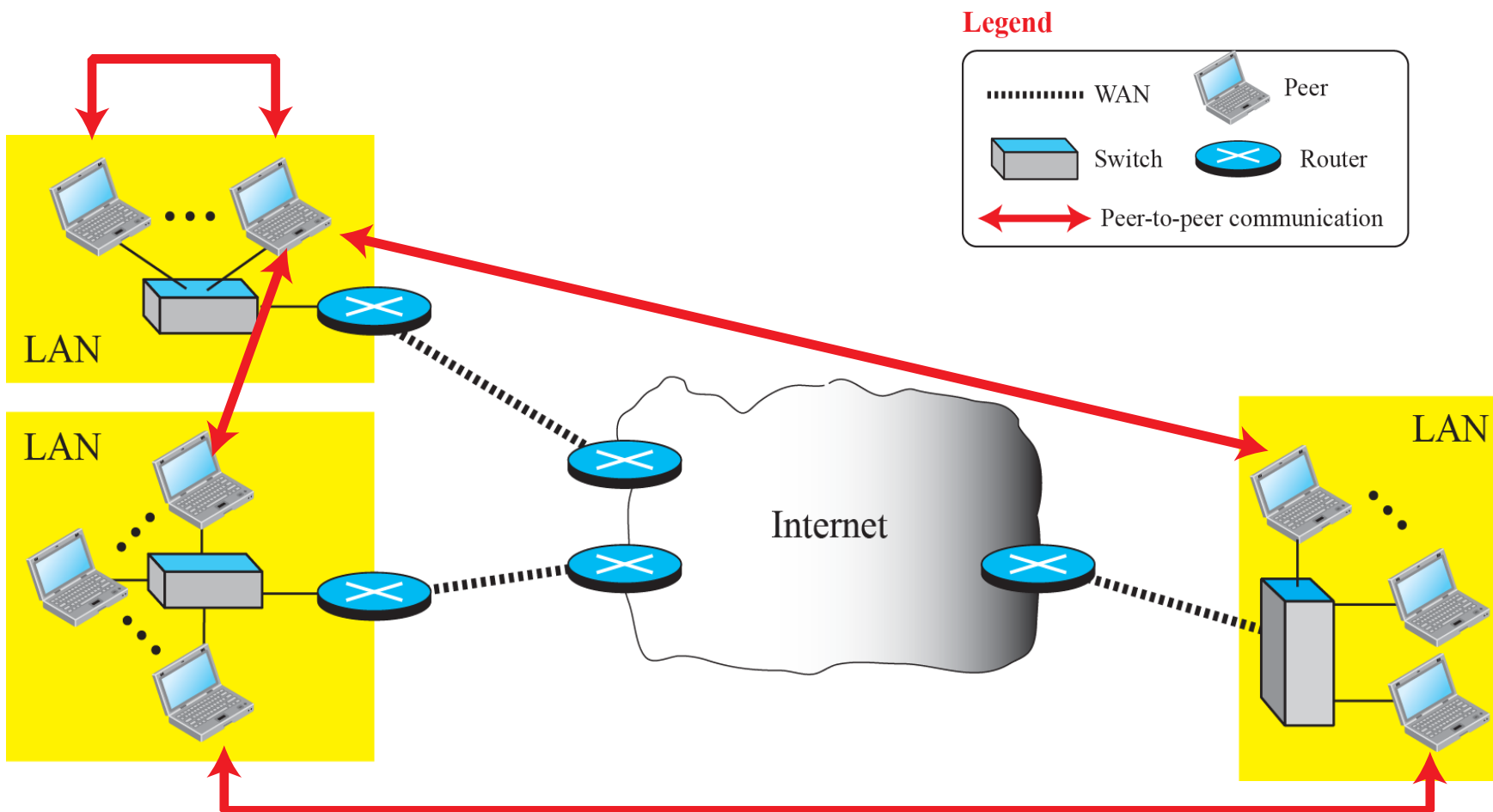
Ad-hoc connection (peer-to-peer connection)

- Using an **ad-hoc** / **peer-to-peer connection**, two nodes can connect directly with each other, without a base station.
- A decentralized network architecture uses ad-hoc connections, so that nodes can communicate directly without a base station.



Peer-to-peer application model

A peer-to-peer connection is **not the same** as the peer-to-peer application model.



Wireless ad-hoc networks

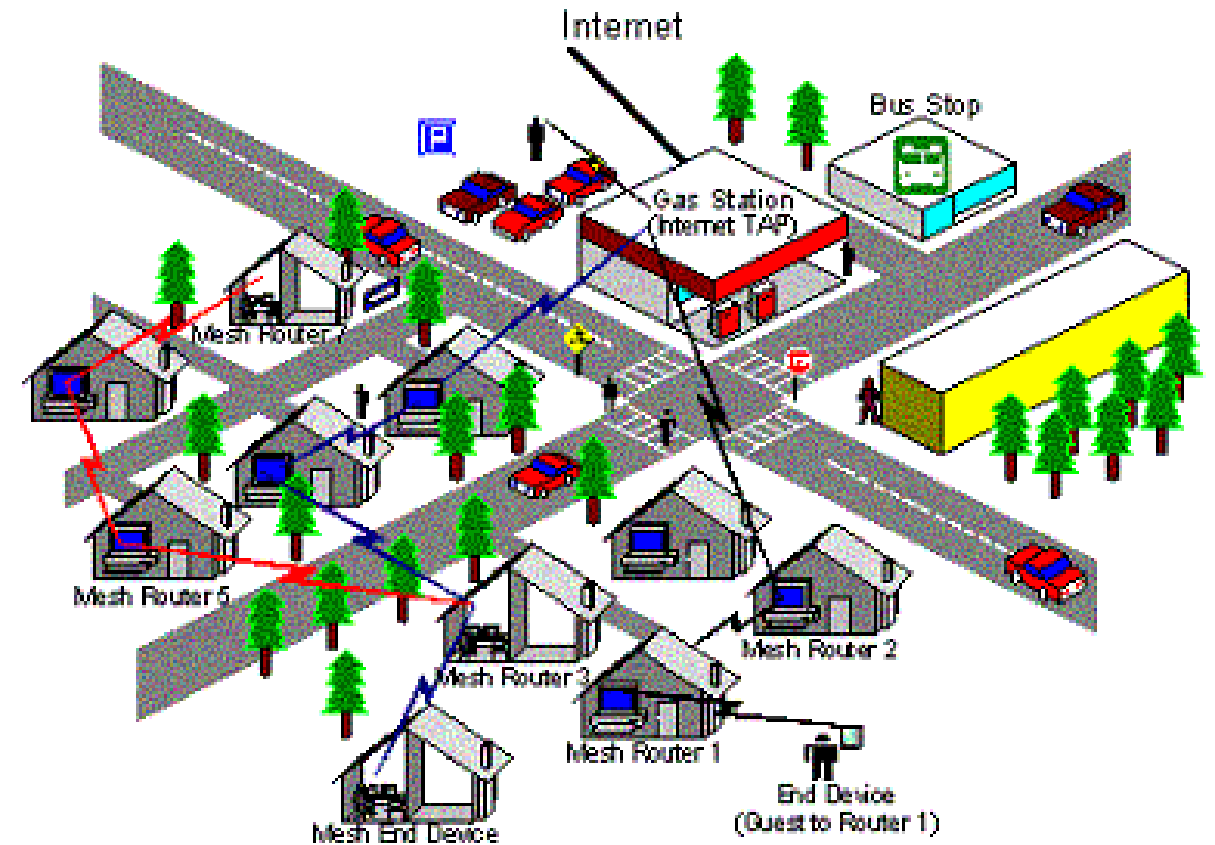
Wireless networks that use a decentralized network architecture are usually called **Wireless ad-hoc networks**.

There are two basic types of wireless ad-hoc network architectures:

- In an **mobile ad-hoc network (MANET)**, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use. The nodes are usually assumed to be mobile, however, they could of course also be stationary.
- A **wireless mesh network (WMN)** is a local network topology in which the infrastructure nodes (i.e. switches, routers, and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients.

Wireless mesh networks

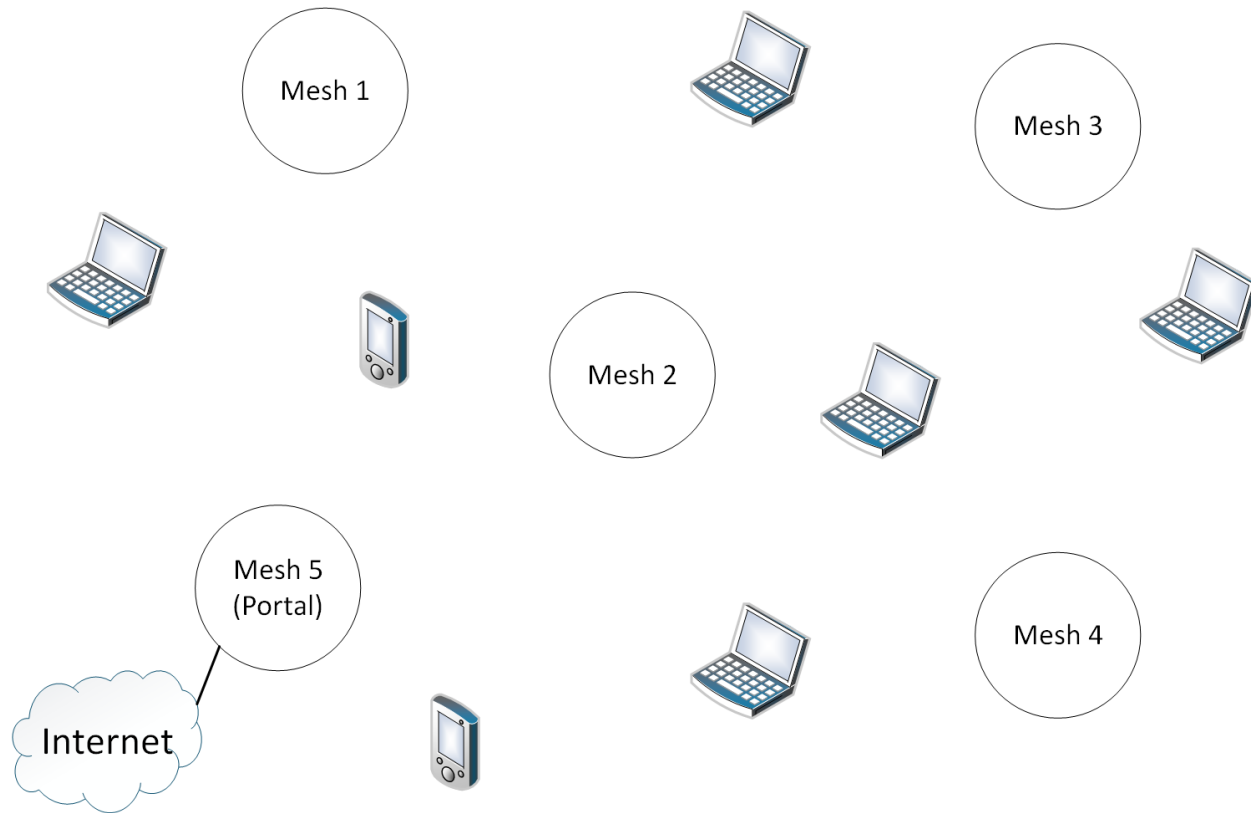
- In a **wireless mesh network**, data hops from **one infrastructure node to another** until it eventually reaches its destination node.
- In a wireless mesh network, the infrastructure topology must be relatively static, so that routes computation can converge and delivery of data to their destinations can occur.



Wireless mesh networks

In a wireless mesh network, there are **two (three) types of nodes with different roles:**

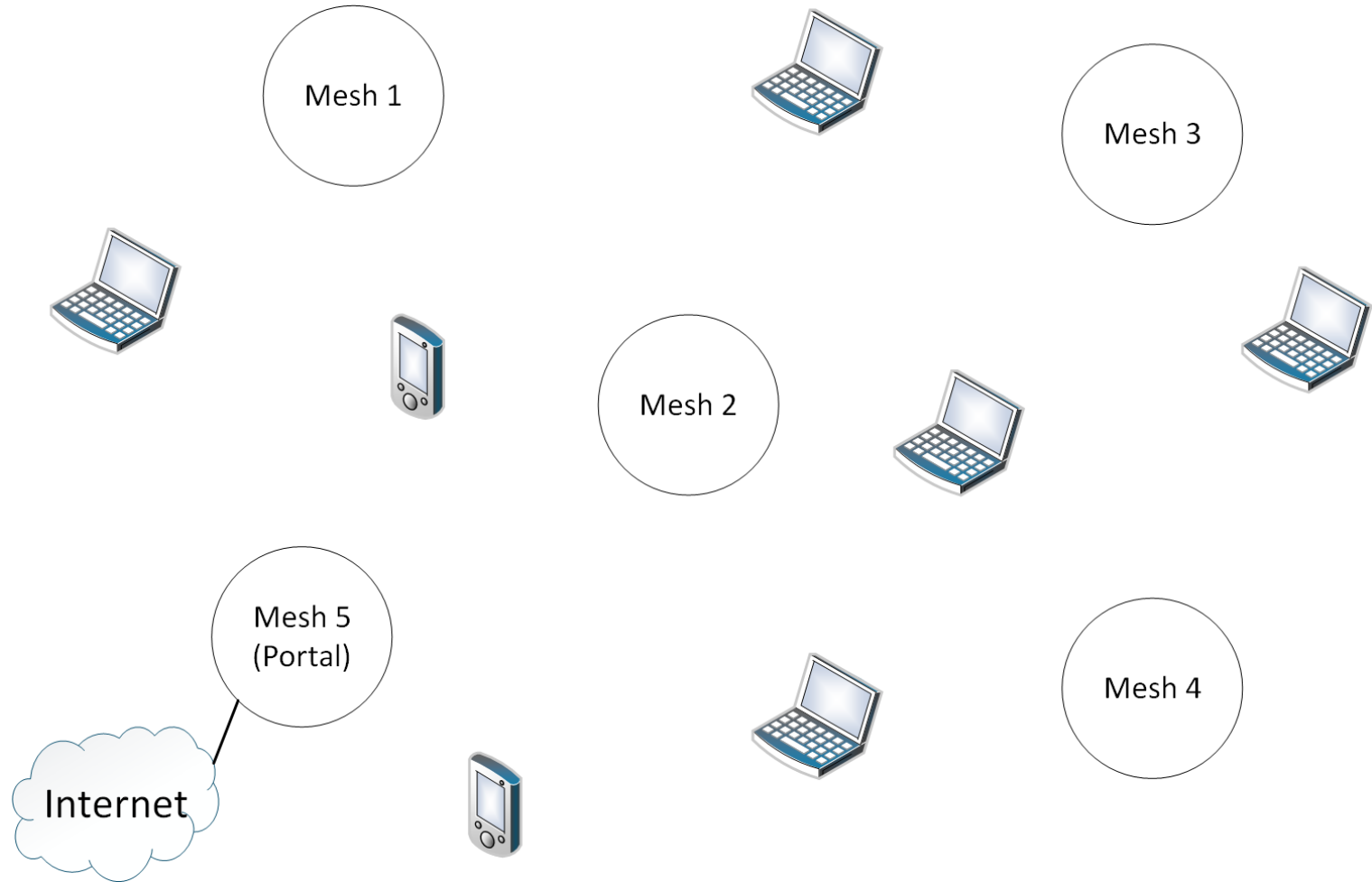
- **Mesh routers** can forward data to other mesh nodes.
- There must be at least one mesh router that act as **sink** and is connected to the Internet. Also called **portal** or **gateway**.
- **Hosts** connect to one of the mesh routers, usually the mesh router with the best connectivity conditions.
 - **From a host's perspective, the network architecture is centralized.**



Mesh networks

Three basic elements of a mesh network:

- Mesh identifier (**Mesh ID**) is the identification of a mesh router in the network.
- **Routing protocol** for multi-hop data forwarding.
- **Node discovery protocol** for the mesh nodes.



Centralized or decentralized network architecture?

You have been given the task to help a friend that wants to install a smart lighting system for their greenhouse. The system includes about 10 sensors distributed in the greenhouse. Also, the system includes smart lamps that can be controlled via the Internet. The sensors collect and send data to a back-end server system.

The back-end server system includes an AI system that processes the data and then adjusts the lamps in the greenhouse so that the plants always have optimal light.

Your task is to suggest a solution for the complete networked system.



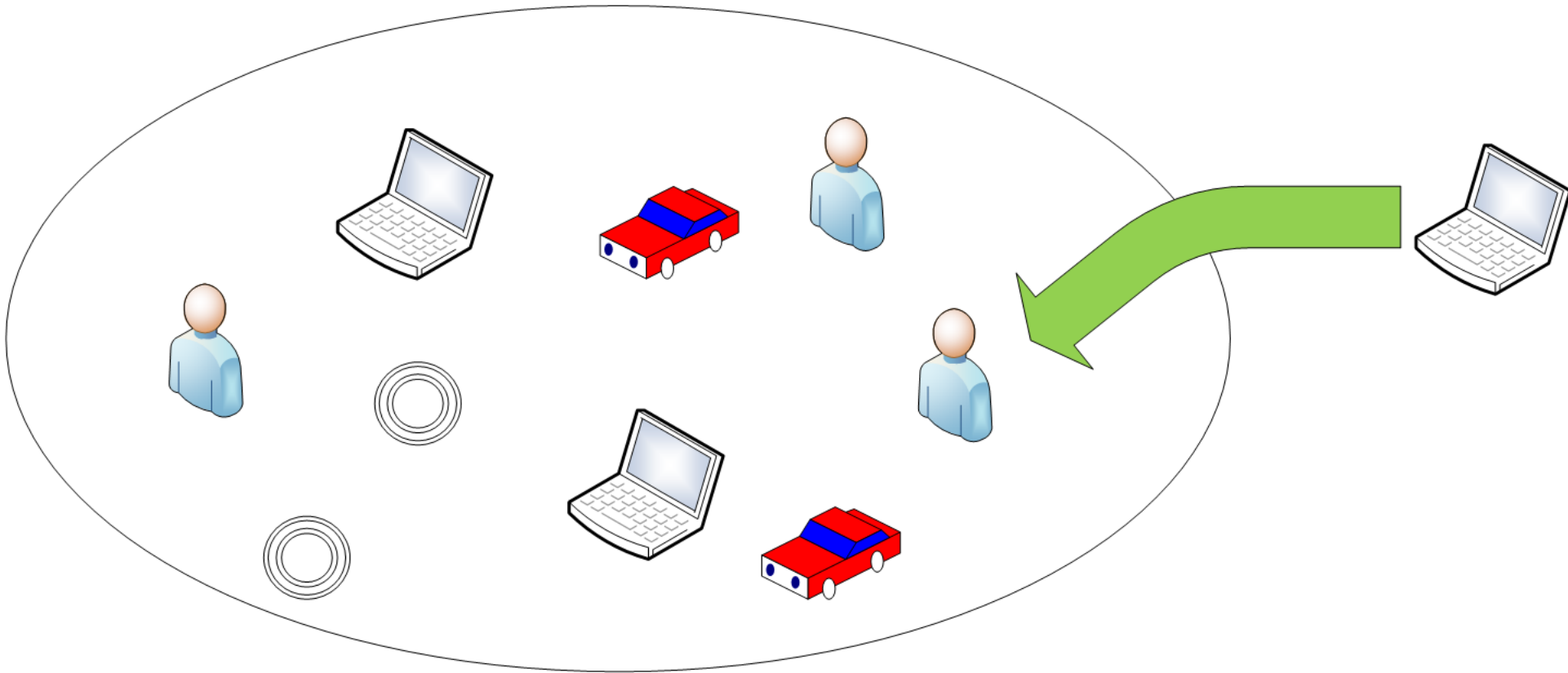
Suggested solution

- There is nothing in the scenario that decide that the network technology must have either a centralized or a decentralized architecture.
- **Centralized architecture:**
 - Sensors and lamps communicate with a base station / access point, acting as a gateway. The gateway is connected to the back-end server system (over the Internet if needed).
- **Decentralized architecture:**
 - Sensors and lamps send data directly to each other until the data reaches a sink that is connected to the back-end server system (over the Internet if needed).
 - Potentially, the lamps can act as mesh nodes since they have good access to electricity. In this case, one of the lamps can act as a sink or we have a another sink node.

Node association / Initial access

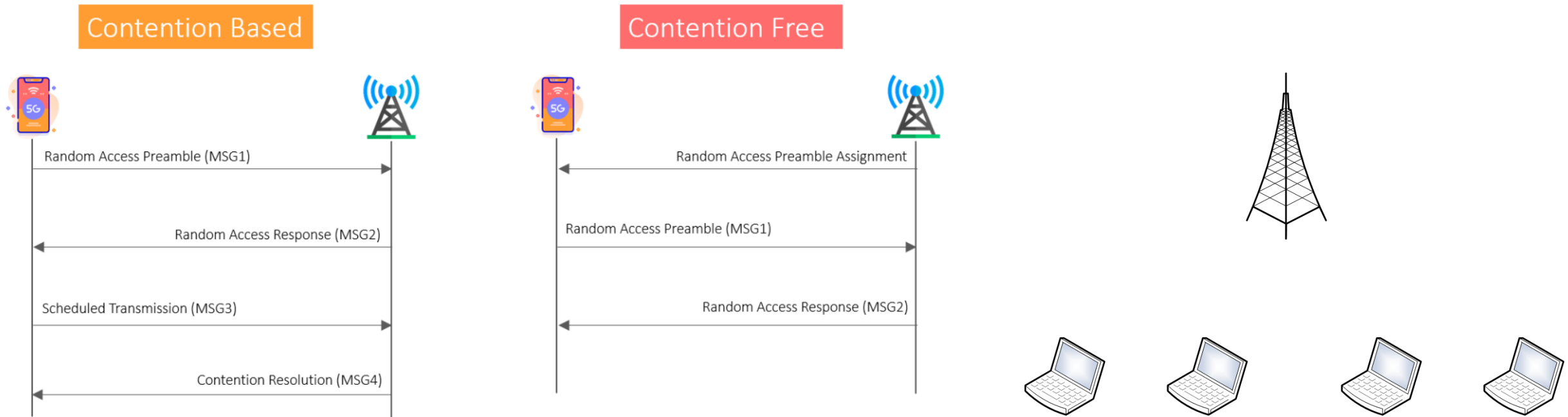
Node association / Initial access

Within a wireless network, a **node association process** is performed every time a new node wants to join the network.



Centralized network architectures

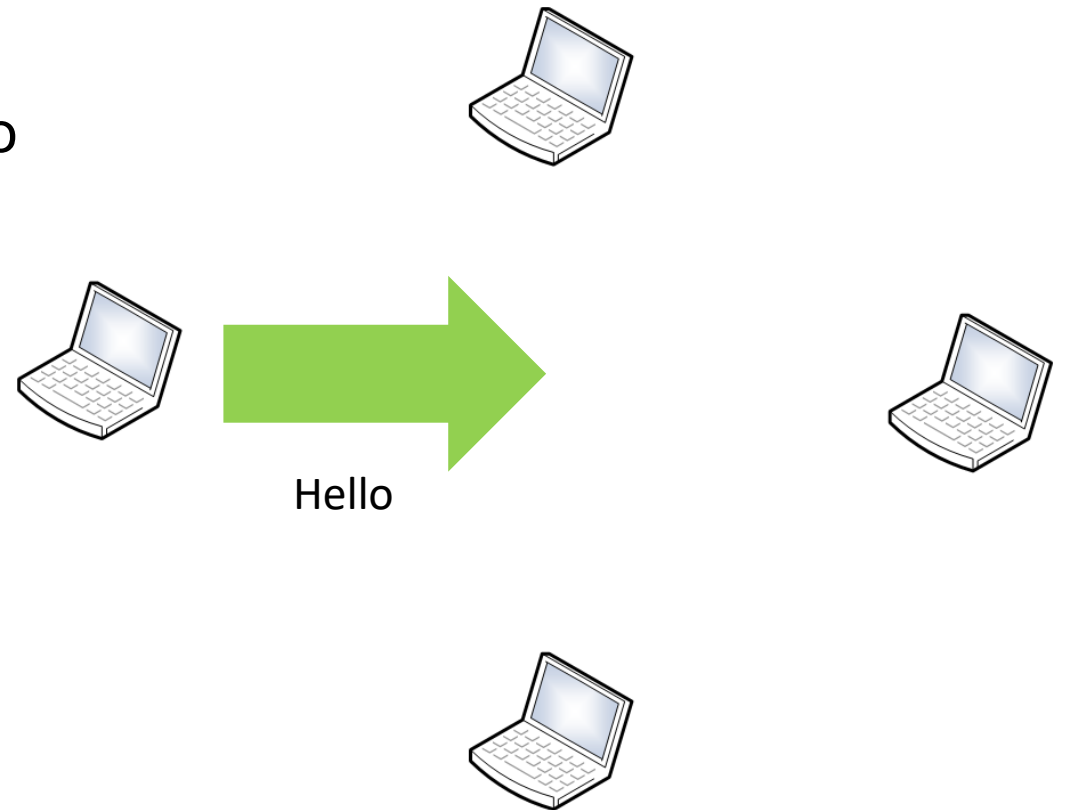
- In centralized network architectures, there is a base station / access point that controls the network operations.
- When joining such a network, a node needs to make contact with this base station / access point.
 - In Cellular networks: RACH process



Decentralized network architectures

Decentralized networks are self-organized.

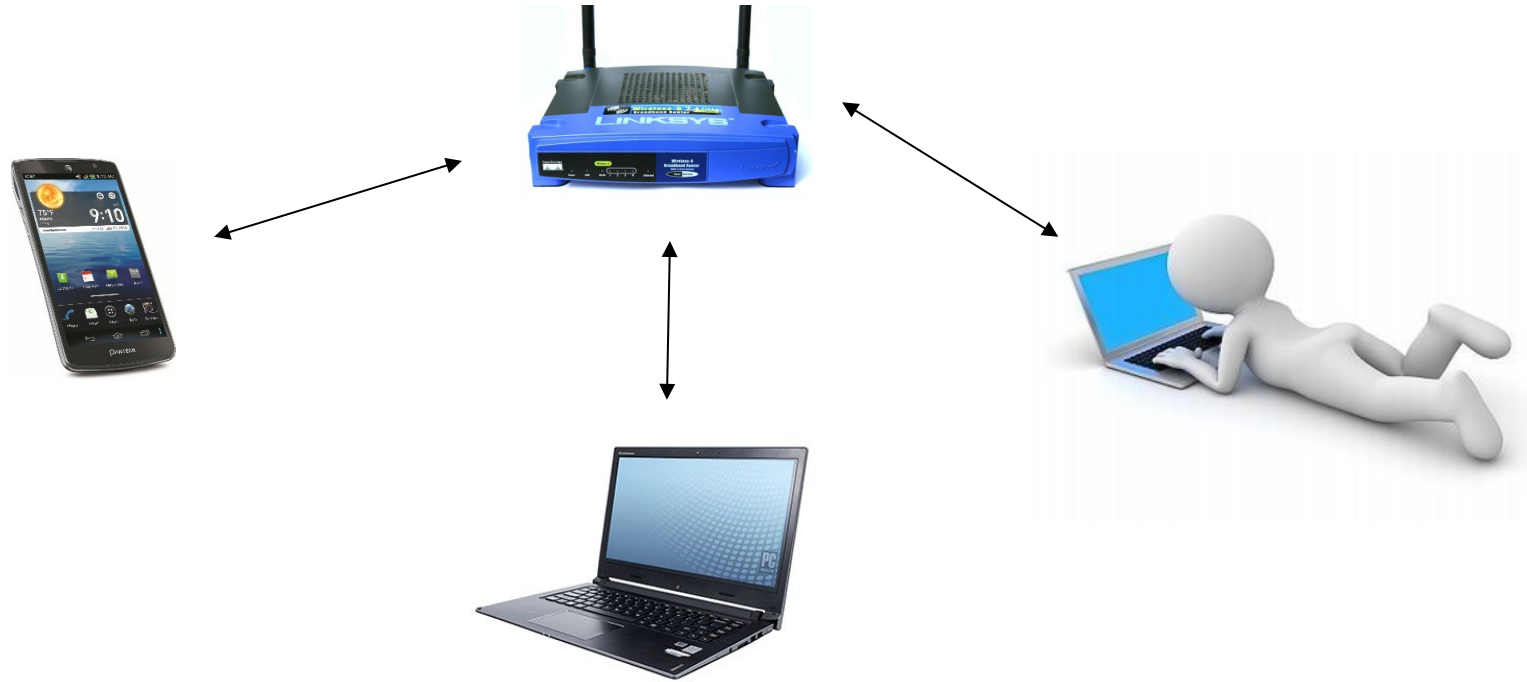
- **Node discovery** is an important part of a decentralized network.
- Decentralized networks with mobile nodes also need a mechanism to continuously test **link connectivity**.
- **Hello messages (heart-beat)** can be used.
 - Each node periodically broadcasts a Hello message with information about itself.
 - All nodes that hear the Hello message are within radio range and therefore have link connectivity with the sender.



Medium Access Control (MAC) protocols

The wireless physical media is shared

A wireless link (medium, channel) is always shared with others within the network.



Medium access

- When multiple terminals can send data on the same wireless communication channel, the terminals need to agree on how they get access to the medium.
- This is called a **medium access control (MAC)** method or a multiple access method.
- The protocol that handles the medium access control is called a MAC protocol.

The MAC protocol in a wireless network is very important for the system design!

Functions

Responsibilities of a MAC protocol include:

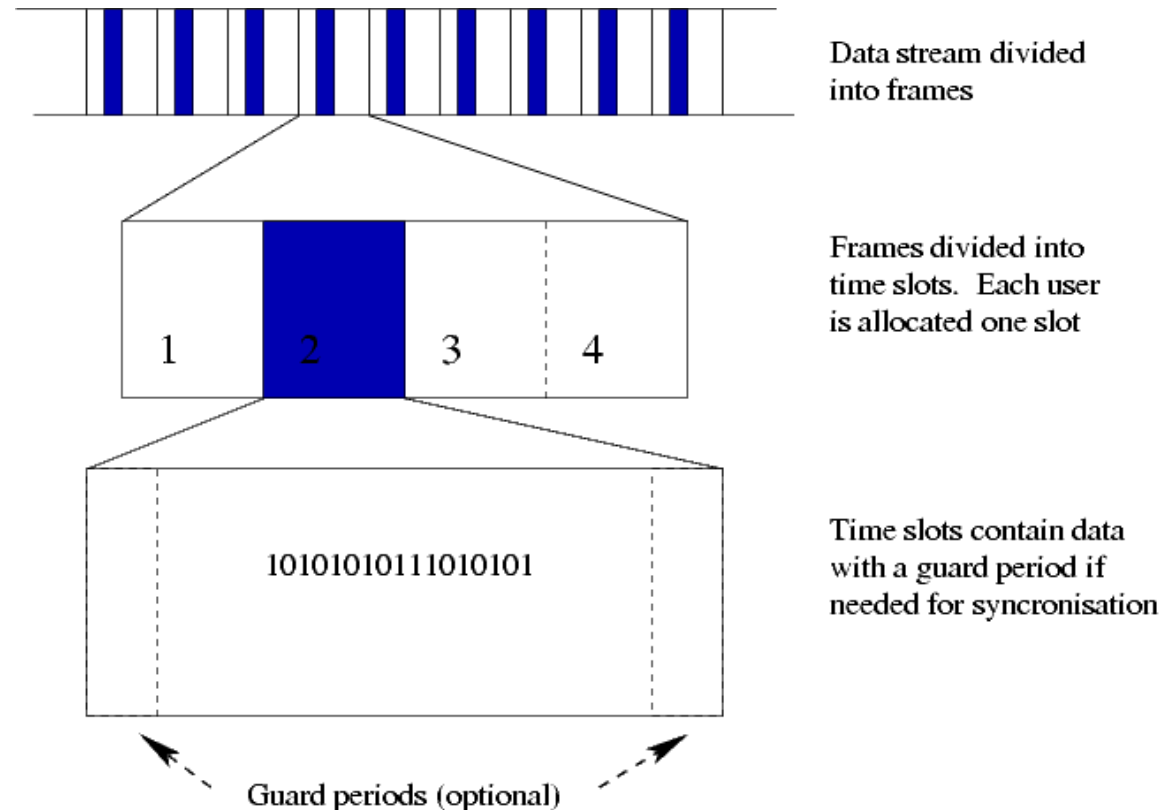
- decide when a node can access a shared medium.
- resolve any potential conflicts between competing nodes.
- perform other activities such as framing, addressing, and flow control.

Medium access control – general categories

- In a **contention-free MAC protocol**, collisions can be avoided by ensuring that each node can use its allocated resources exclusively.
 - Fixed assignment strategies: TDMA, FDMA, CDMA.
 - Dynamic assignment strategies: Polling, Reservation-based, Token passing.
- In a **contention-based MAC protocol**, nodes may initiate transmissions at the same time, which requires mechanisms to reduce the number of collisions and to recover from collisions.
 - ALOHA, CSMA/CD, CSMA/CA

Time-Division Multiple Access (TDMA)

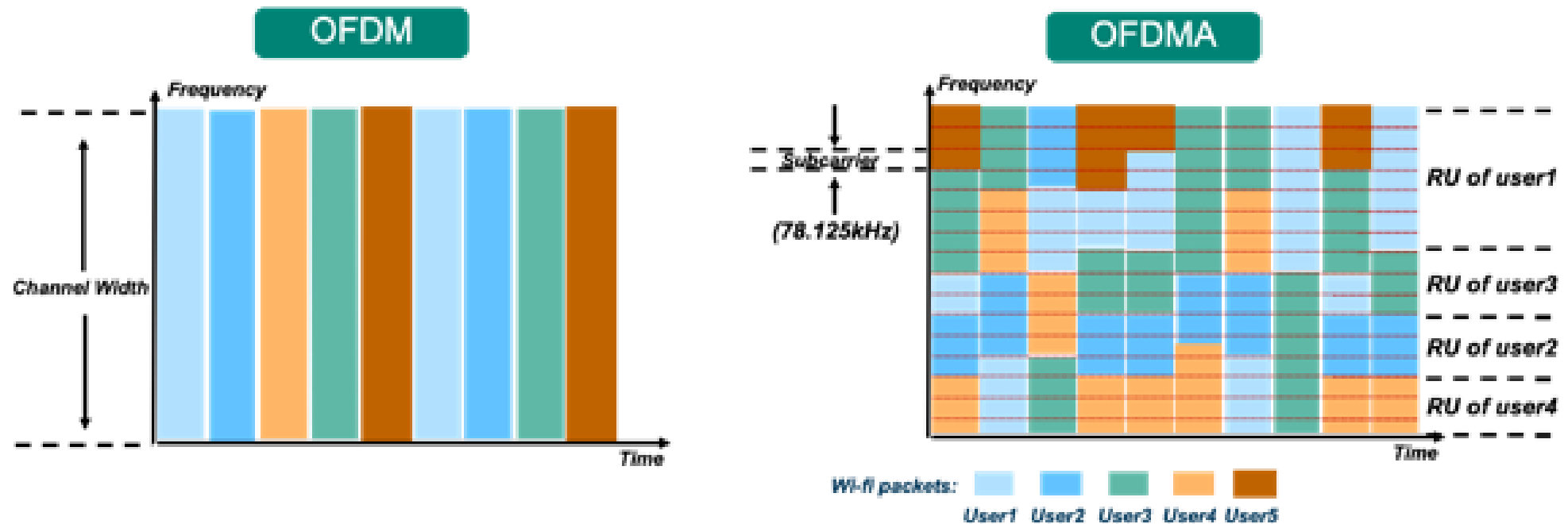
TDMA allows several users to share the same frequency channel by dividing the signal into different time slots. Some variants of TDMA can allow for reservation of several slots.



Orthogonal Frequency-Division Multiple Access (OFDMA)

Fast-speed wireless networks often use a technique called Orthogonal Frequency-Division Multiple Access (OFDMA).

OFDMA combines FDMA (Frequency-Division) with TDMA (Time-Division). A user gets time slots on several (narrow) frequency bands and data is transmitted in an intelligent way to mitigate disturbances.

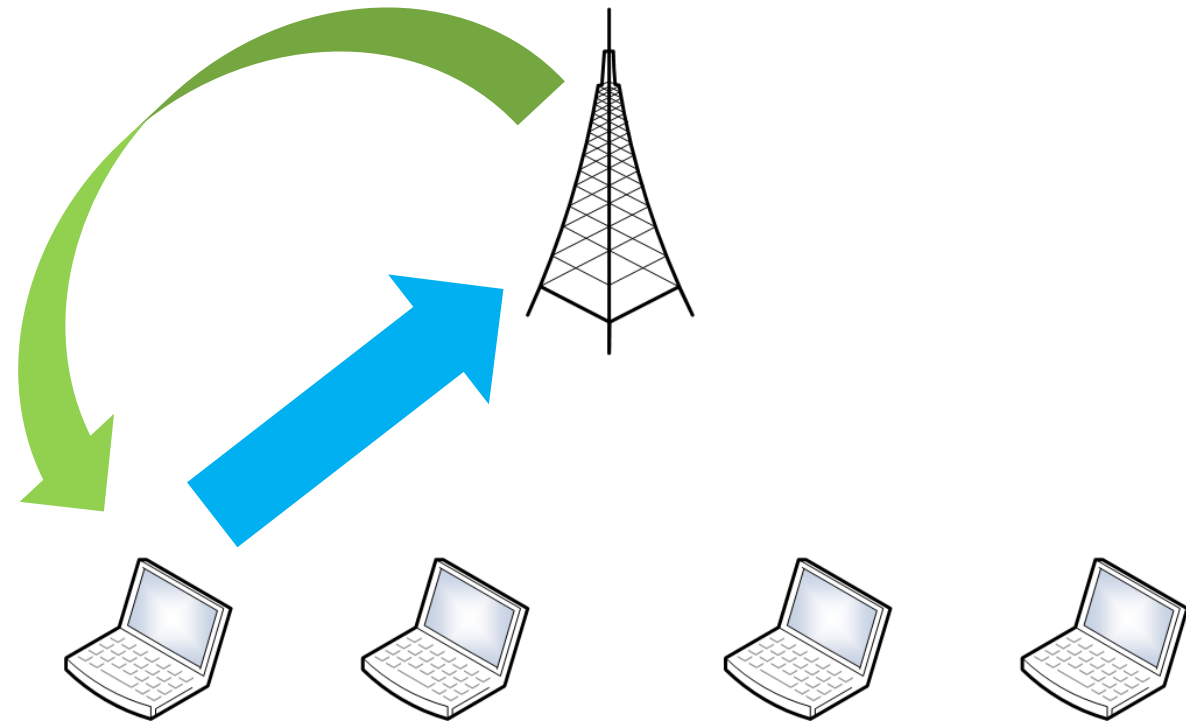


ALOHA (for centralized architectures)

- ALOHA is the simplest contention-based protocol for wireless networks. It was developed for ALOHANET in 1970.
- ALOHA (or modified versions of ALOHA) can be found in several network technologies for different purposes.

Procedure for centralized architectures:

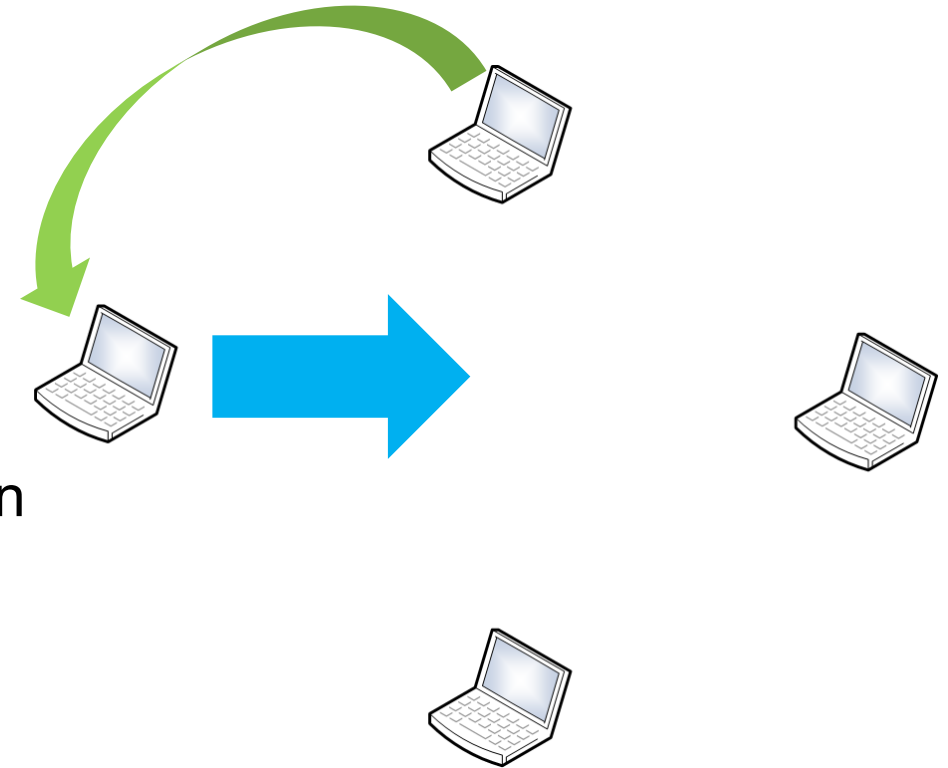
1. A device that has data to send, **initiate a data transmission at any time.**
2. If the data is received correctly at the base station, the base station sends an **ACK on another communication channel.**
3. If the sender has not received an ACK within a certain time period, it initiates a retransmission.



ALOHA in Decentralized network architectures

ALOHA also works for decentralized network architectures.

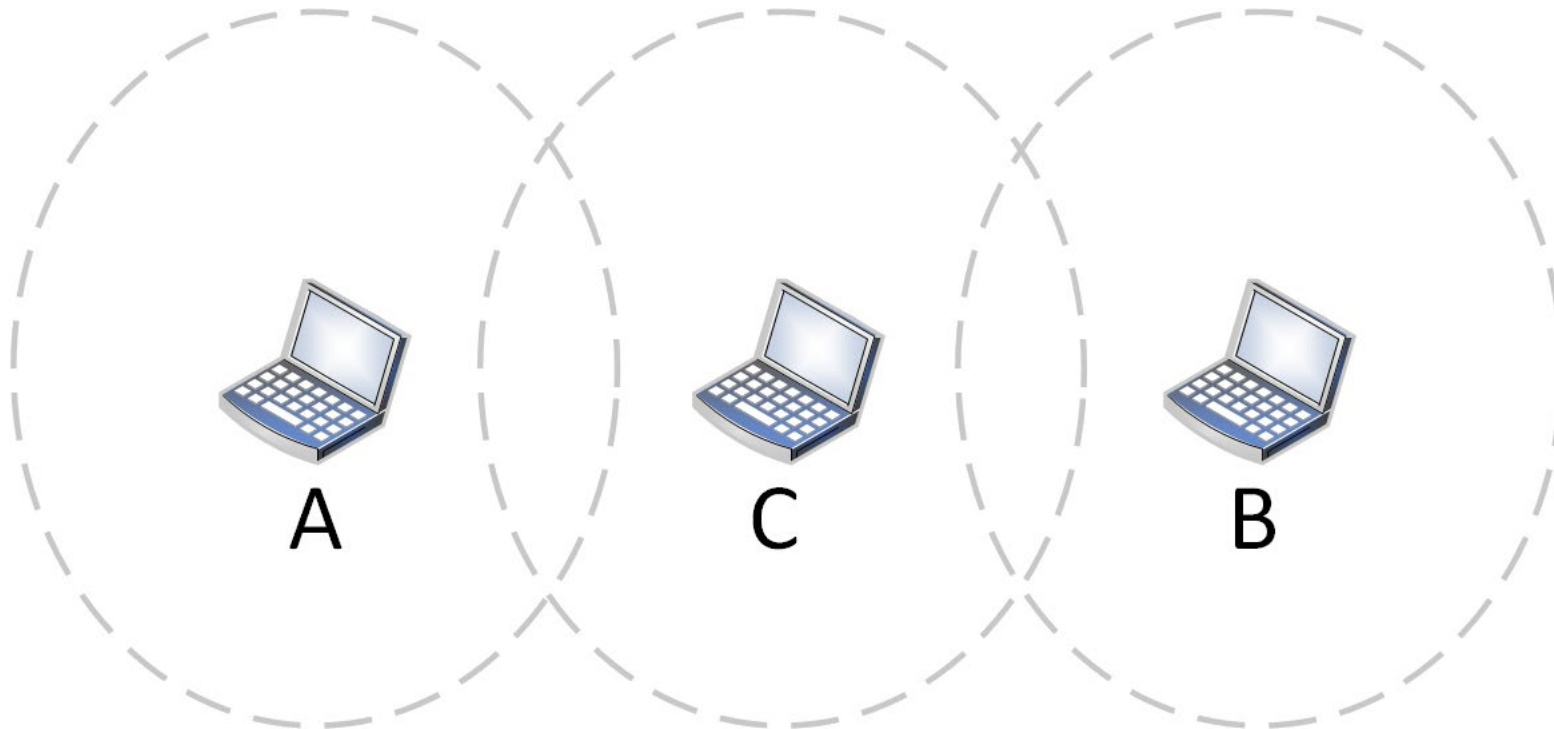
- The nodes have two communication channels, one for data and one for ACKs.
 - These channels could be on the same frequency band, but separated in time. For example, there can be an agreed time slot for ACKs after a data packet has been sent.
- A node that has data to send, initiates a data transmission at any time. This data must include an address to the receiver.
- The receiver answers with an ACK.
 - If the receiver has not received an ACK within a certain time period, it initiates a retransmission.



Hidden terminal problem

In all wireless networks, the hidden terminal problem is a technical challenge that must be solved.

- Main challenge: Two terminals A and B may both be in range for C, but cannot hear each other.



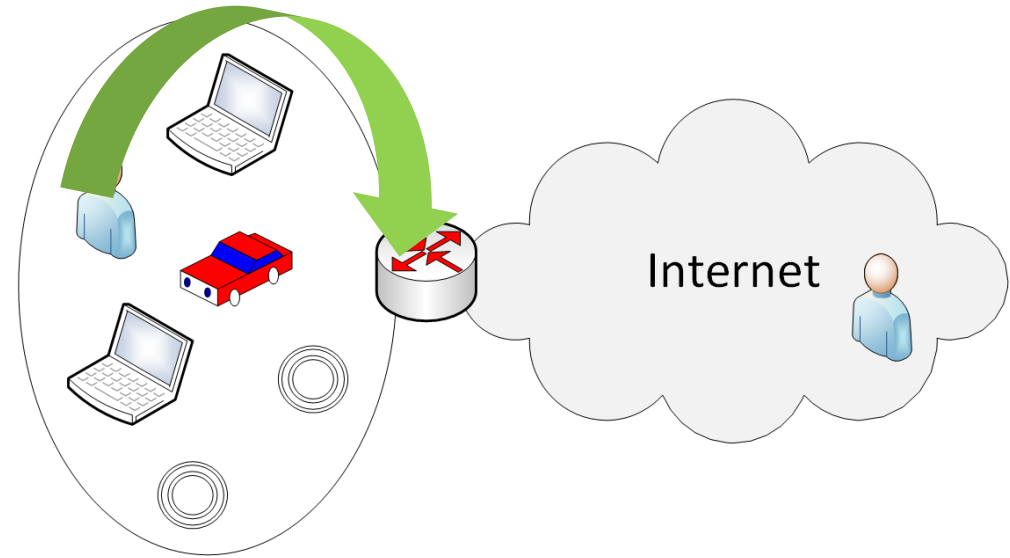
Common technical solutions to the Hidden terminal problem

- Use a **contention-free MAC** protocol, for example, a base station determines when hosts can send data.
 - For example in cellular networks, NB-IoT and WiFi 6/7.
- Use a **contention-based MAC protocol in combination with a Request-to-send / Clear-to-send (RTS/CTS) procedure**. A node must receive a CTS from the receiver/base station before it can send its data. All hosts hear this CTS, and knows that the link will be occupied for some (pre-specified) time
 - For example in WiFi (CSMA/CA with DCF)
- Use a **contention-based MAC protocol (usually various types of ALOHA) in combination with an ACK procedure**.
 - For example in LoRa.
- **Do not care** about it
 - For example in Argos

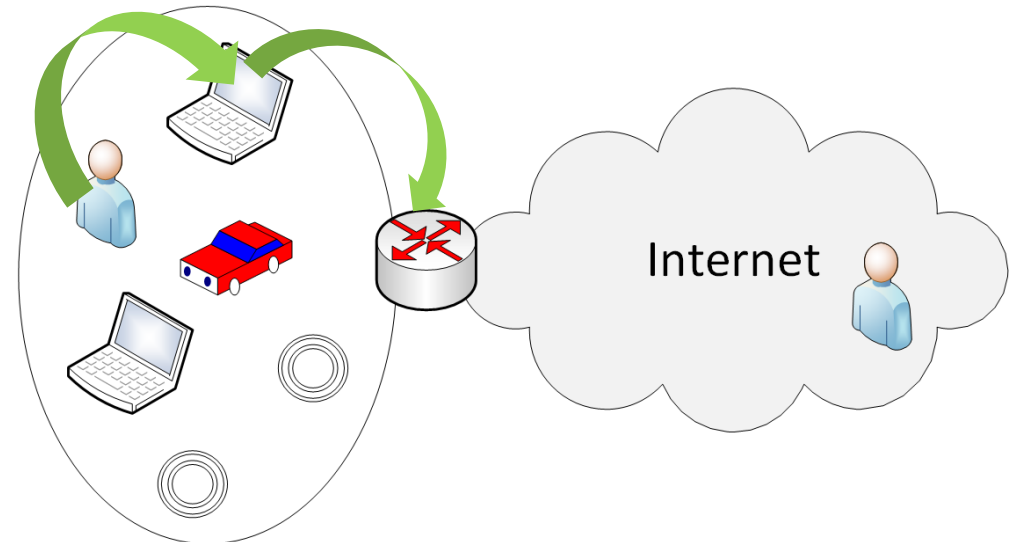
Data forwarding

Data forwarding (routing) schemes

- **Single-hop (Direct) data forwarding**
 - A host can reach the gateway in one hop.

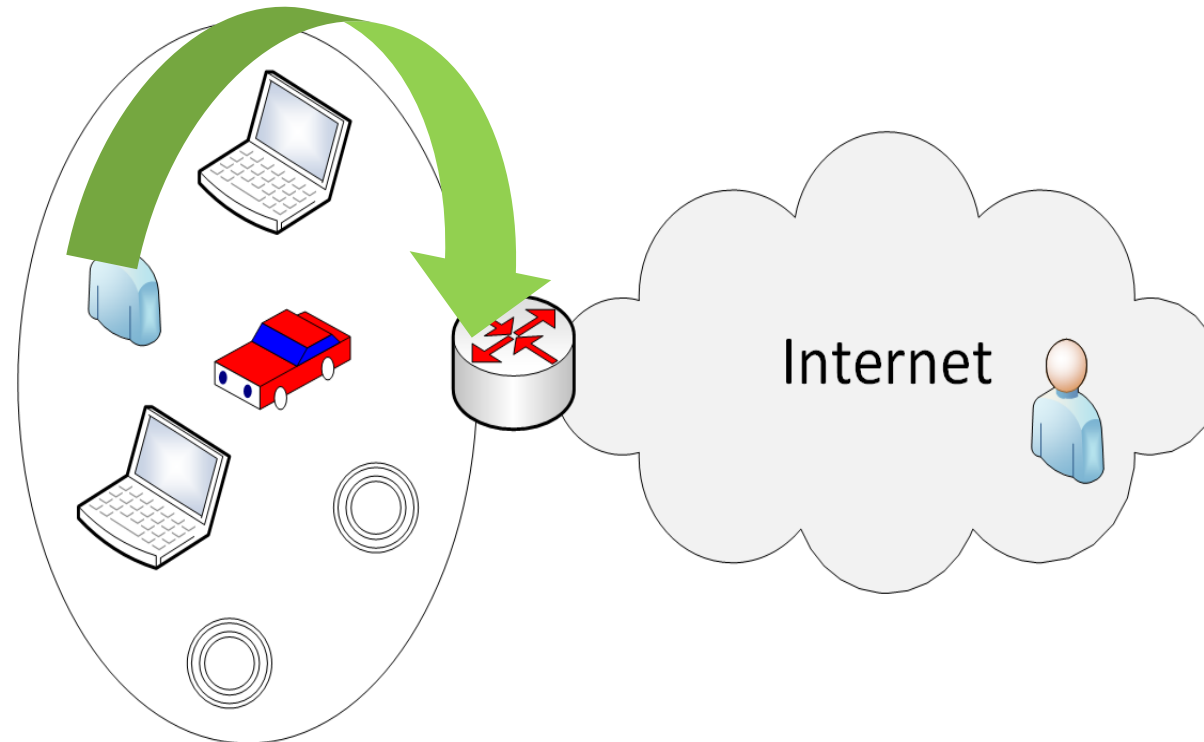


- **Multi-hop data forwarding**
 - To reach the gateway, a host can use other hosts as relays.



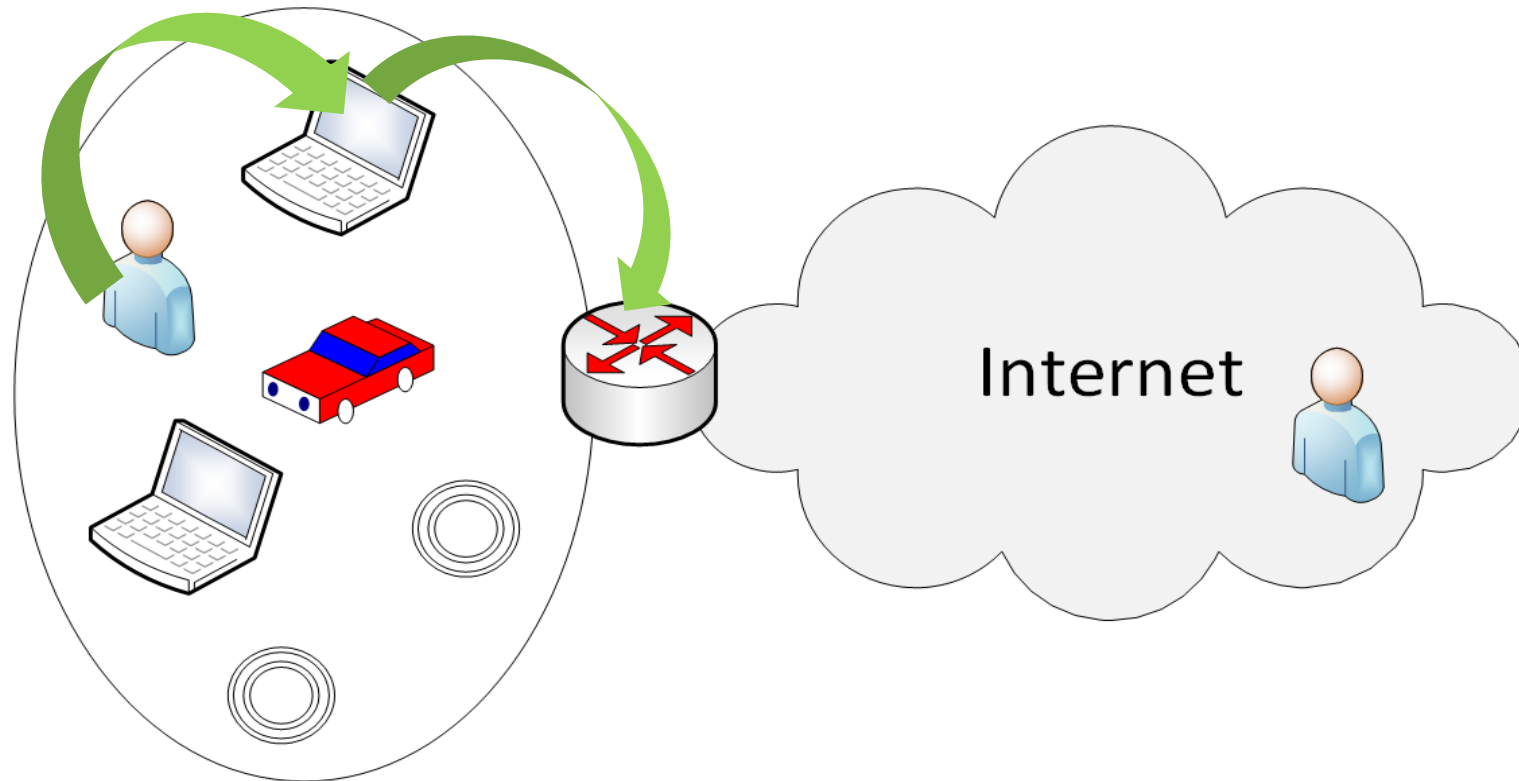
Single-hop (Direct) data forwarding

- All centralized network architectures are based on single-hop data forwarding.
- Decentralized network architectures may be based on single-hop data forwarding. In this case, the communication is based on single peer-to-peer connections.



Multi-hop data forwarding

- Most decentralized network architectures are based on multi-hop data forwarding.
- **A routing protocol** is used to decide the best path for the data forwarding.



Single-hop or multi-hop data forwarding?

You have been given the task to help a friend that wants to install a smart lighting system for their greenhouse. The system includes about 10 sensors distributed in the greenhouse. Also, the system includes smart lamps that can be controlled via the Internet. The sensors collect and send data to a back-end server system.

The back-end server system includes an AI system that processes the data and then adjusts the lamps in the greenhouse so that the plants always have optimal light.

Your task is to suggest a solution for the complete networked system.



Suggested solutions

The solution can be based on either single-hop or multi-hop data forwarding.

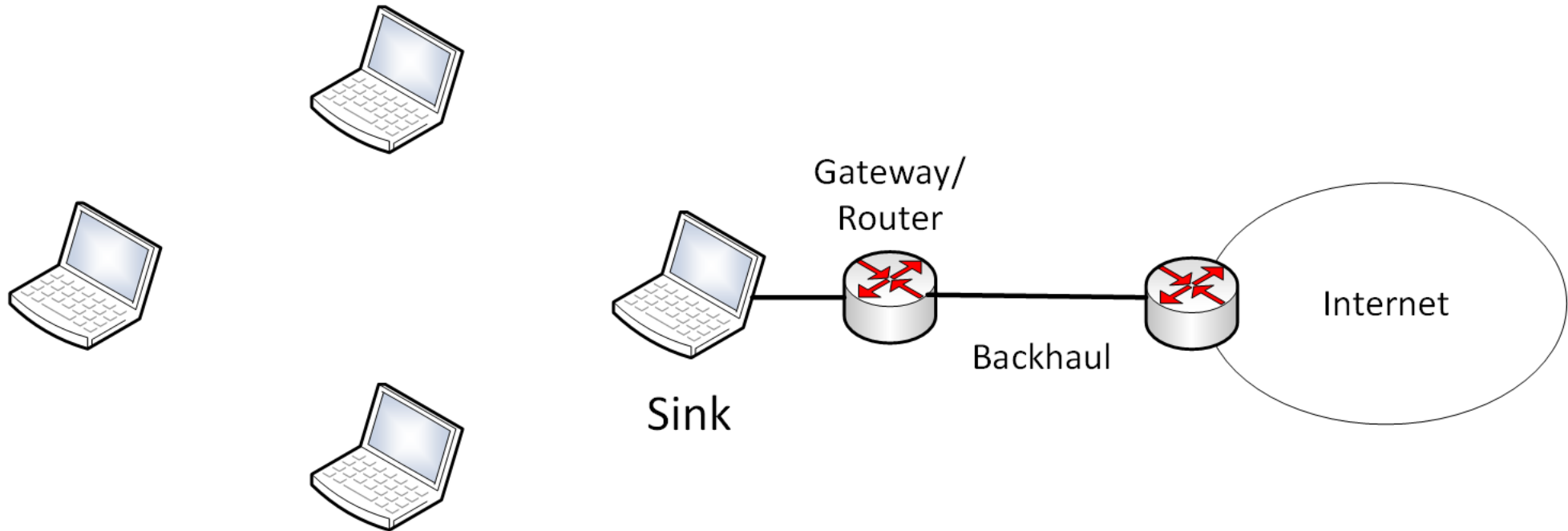
- **Single-hop data forwarding:**
 - There is an access point / base station placed in the greenhouse or close to the greenhouse. The base station is connected with the back-end server system (over the Internet if needed).
 - Each sensor send its data to the base station.
 - The base station sends control signals to the lamps.
- **Multi-hop data forwarding:**
 - The sensors and lamps send data directly to each other using a routing protocol. One or more of the sensors or lamps act as a sink and is connected to the back-end server (over the Internet if needed).
- **Comment:** Multi-hop data forwarding will result in a higher energy consumption for the sensors and lamps.

Multi-hop routing in decentralized network architectures (ad-hoc networks)

Routing objective: Find the best path!

Two main routing principles:

- Find the best path between a sender and the intended receivers for a message (one or more receivers).
- Find the best path to the sink.



Data transmission methods

- **Unicast**

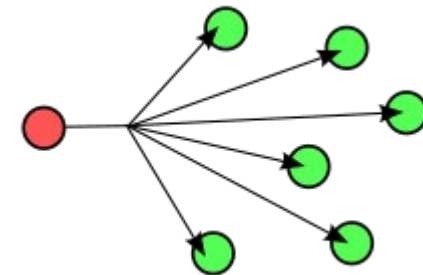
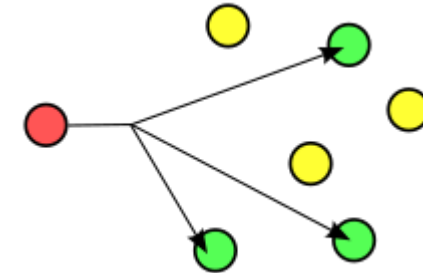
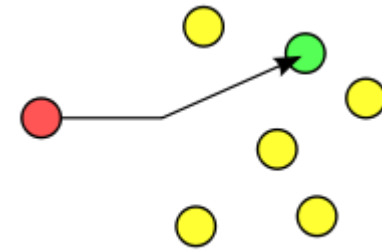
- Data transmission from one point in the network to another point; that is, one sender and one receiver.

- **Multicast**

- Data transmission from one point in the network to a group of destinations simultaneously.

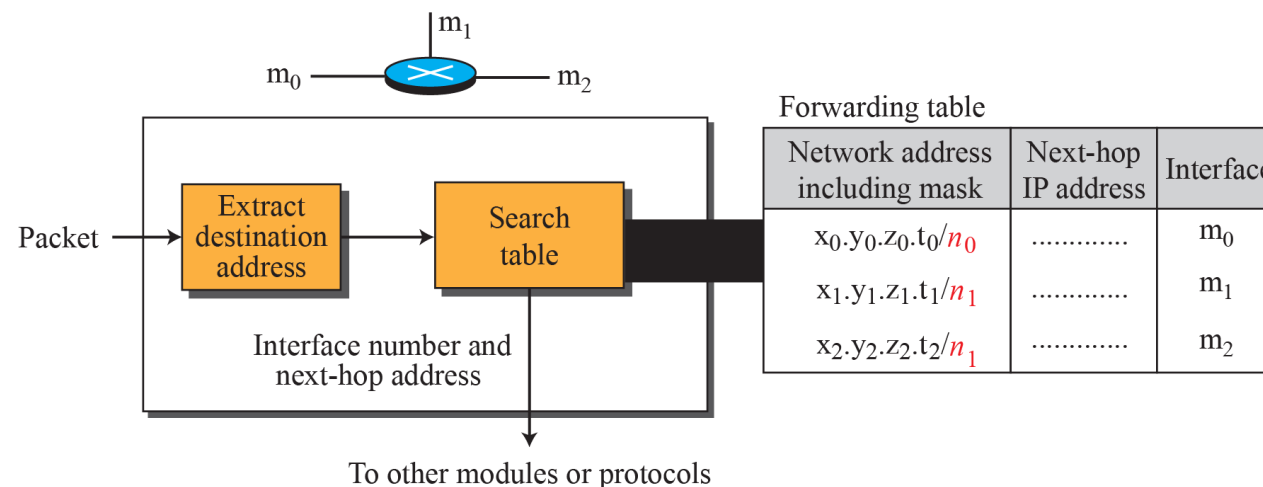
- **Broadcast**

- Data transmission from one point in the network to all destinations in the network simultaneously.



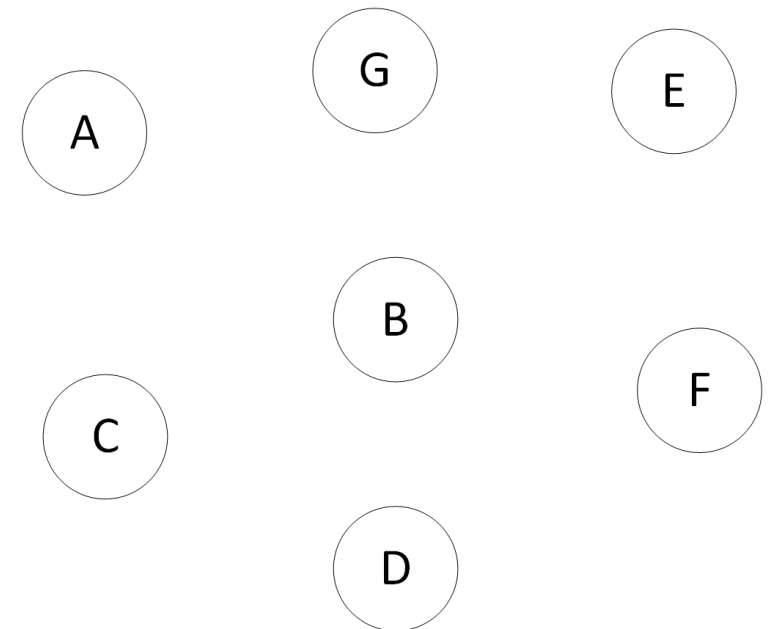
Traditional Internet routing

- Internet routing is performed in the Network layer.
- Each router has a routing table with information about the next hop for packets with a specific network destination.
- Routers exchange routing information with each other and calculate best paths based on this information.
 - Best paths can be based on, for example, link costs or hop count.



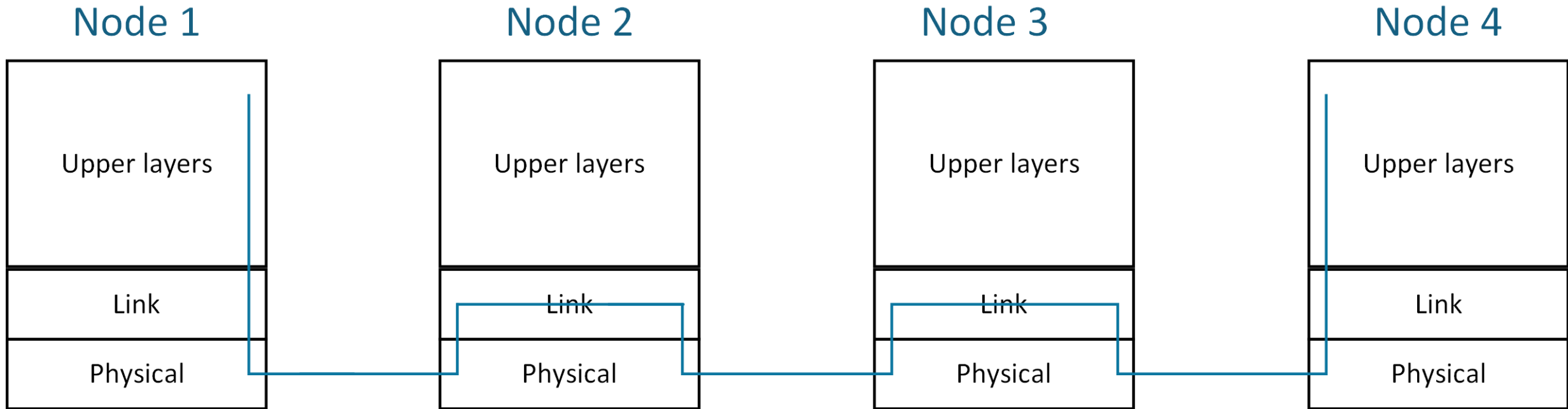
Multi-hop routing in ad-hoc networks

- Multi-hop routing on the **Link layer**
 - The link layer protocols includes routing functions.
 - The routing protocol is incorporated into the network standard.
- Multi-hop routing above **link layer (but still within the same network)**
 - The data dissemination is **performed by the application**, which may include data aggregation and data analysis.
 - **Allows for multi-hop data dissemination with ad-hoc connections.**



Multi-hop routing on link layer

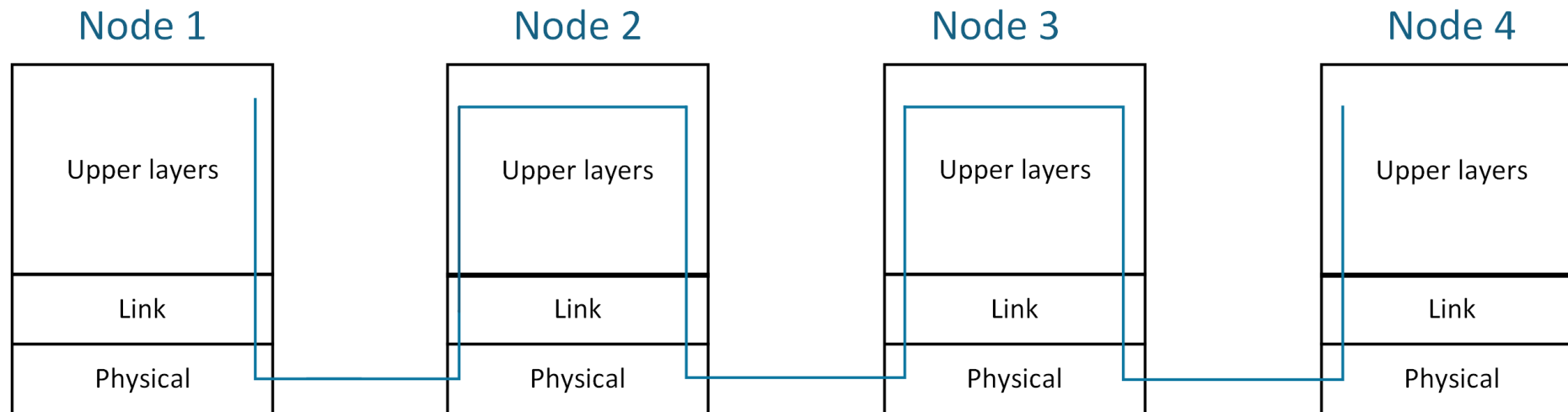
When the multi-hop routing is implemented on the link layer, the link layer protocol must include forwarding and routing mechanisms.



Multi-hop above link layer (application)

When the multi-hop routing is implemented above the link layer, the forwarding and routing mechanisms are implemented as part of the application.

- In this case, there can also be mechanisms for data aggregation, that is, an application can collect data from several nodes, analyse the data, and then forward only an aggregated result.
- The link layer protocol does only need to provide single-hop forwarding (i.e ad-hoc connections).



Routing in multi-hop ad-hoc networks

- Two main approaches:
 - **Proactive**: the collection of route information happens in a scheduled manner, independently of the transmission needs. In a proactive protocol, routers are constantly exchanging information.
 - **Reactive**: Path discovery mechanisms are activated only when necessary. Nodes will have to wait until the information is gathered, what means a somehow delayed beginning of the transmission.
- Some **hybrid protocols** exist as well, which combine proactive and reactive approaches in different ways.

Ad-hoc on demand Distance Vector (AODV)

- Ad-hoc On demand Distance Vector (AODV) is a routing algorithm that was developed in 1999. AODV uses a **reactive approach**.
- AODV is developed for **unicast**.
- Each node has its own sequence number that grows monotonically over time and ensures that there are no loops in the paths used.
- In addition, each node assigned to routing functionality stores its own path index, which contains the address of the next node in the direction of the destination (next hop), its sequence number, and the total distance given in hops, or possibly other metrics designed to measure link quality.

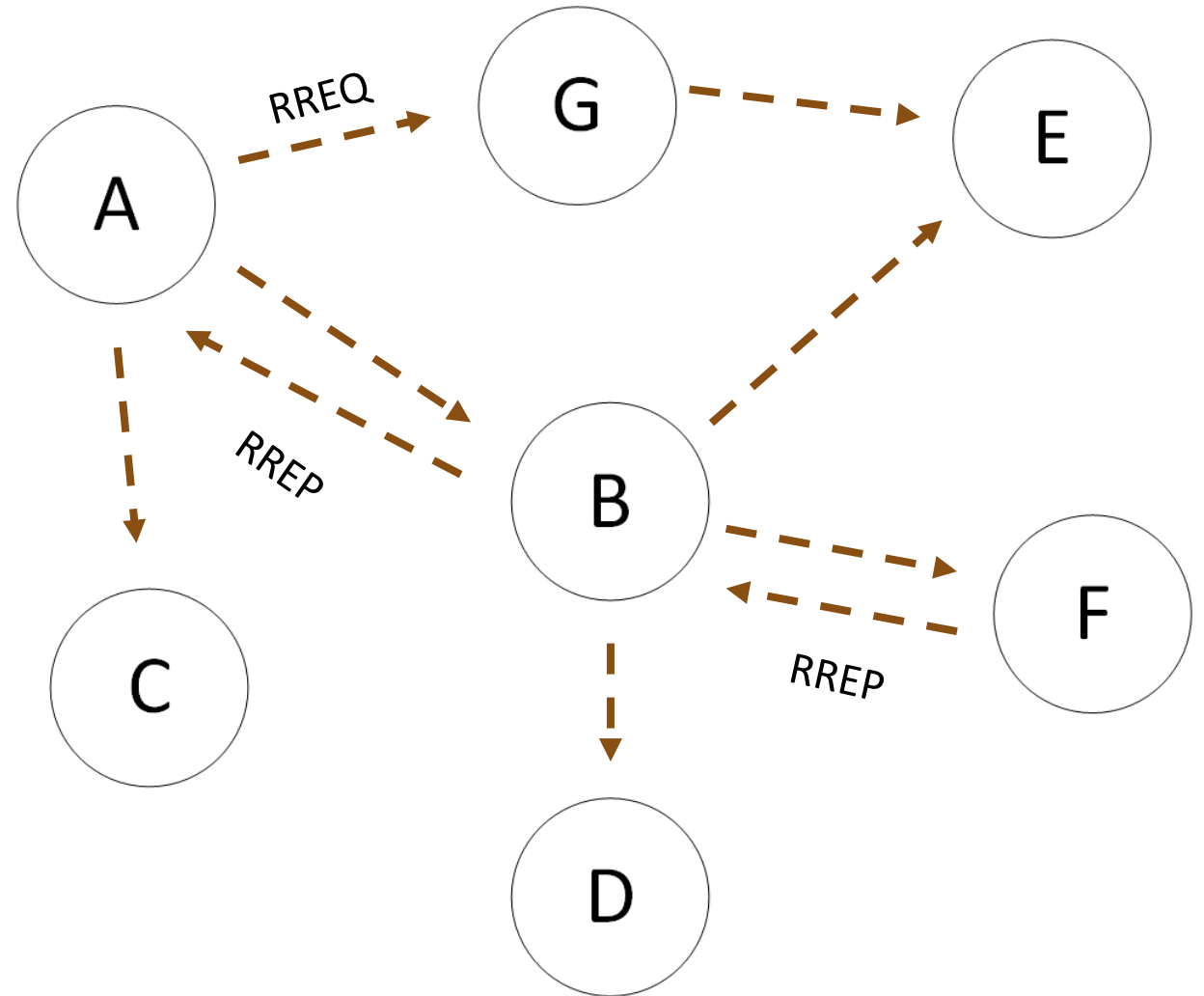
Ad-hoc on demand Distance Vector (AODV)

The network remains completely silent until a connection is required to forward a data packet. If S = Sender node and D = Destination node:

- S broadcasts a RREQ frame to all its neighbors with the address of D.
- When a node receives an RREQ message but does not have a route to the requested destination, it in turn broadcasts the RREQ message. Also, it remembers a reverse-route to the requesting node which can be used to forward subsequent responses to this RREQ.
- This process repeats until the RREQ reaches a node that has a valid route to the destination. This node (which can be the destination itself) responds with an RREP message that is sent in unicast along the reverse-route.
- When a node loses connectivity to its next hop, the node invalidates its route by sending an RERR to all nodes that potentially received its RREP.

AODV, illustration

- A wants to find the route to F.
- A broadcasts a RREQ to all nodes within radio range (called neighbors).
- Nodes that do not know the route to F, forwards the RREQ to their neighbors.
- Finally, one node knows the route to F (can be F itself).
- This node sends back a RREP in unicast on the reverse path.
- All nodes on the way back stores all RREQ and RREP information in their routing tables.

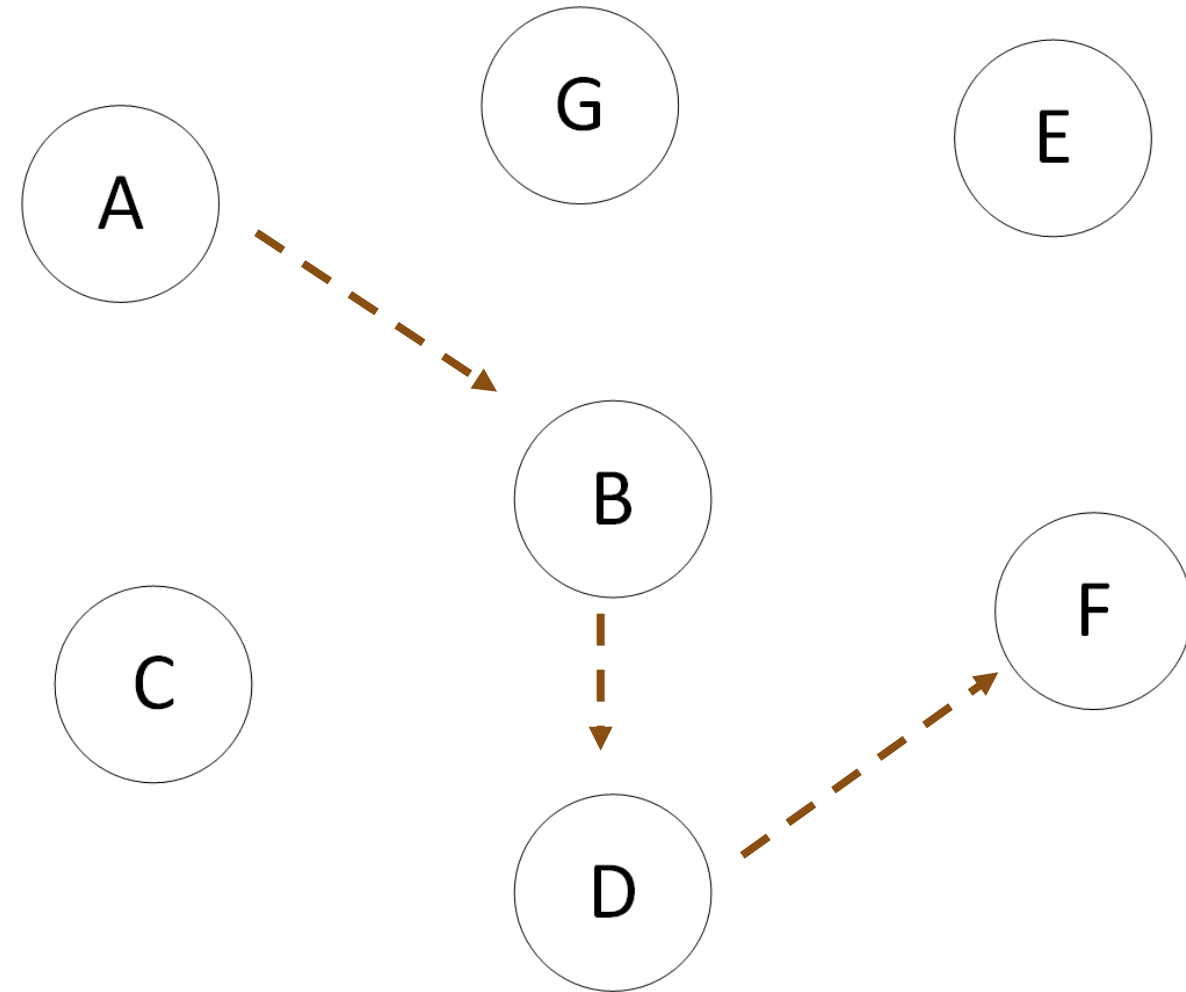


Position-based routing

In position-based routing, the routing-table includes the position of neighbor nodes.

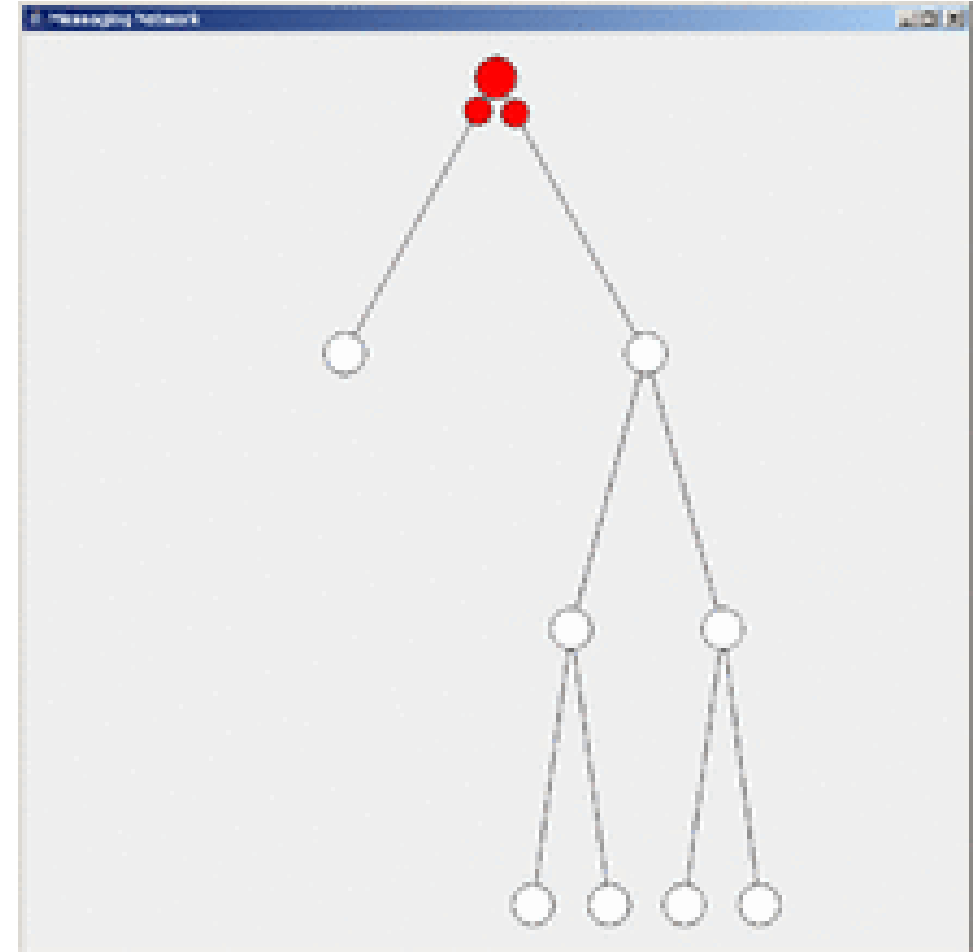
A message must include the position of the receiver.

- A wants to send a data packet to F.
- A looks in its routing table, and sends the data packet to the neighbor node that is the closest to F.
- This node (B in the figure) forwards the data packet to its most closest neighbor within range (D in the figure).
- Finally, the data packet reaches F.



Broadcast based routing

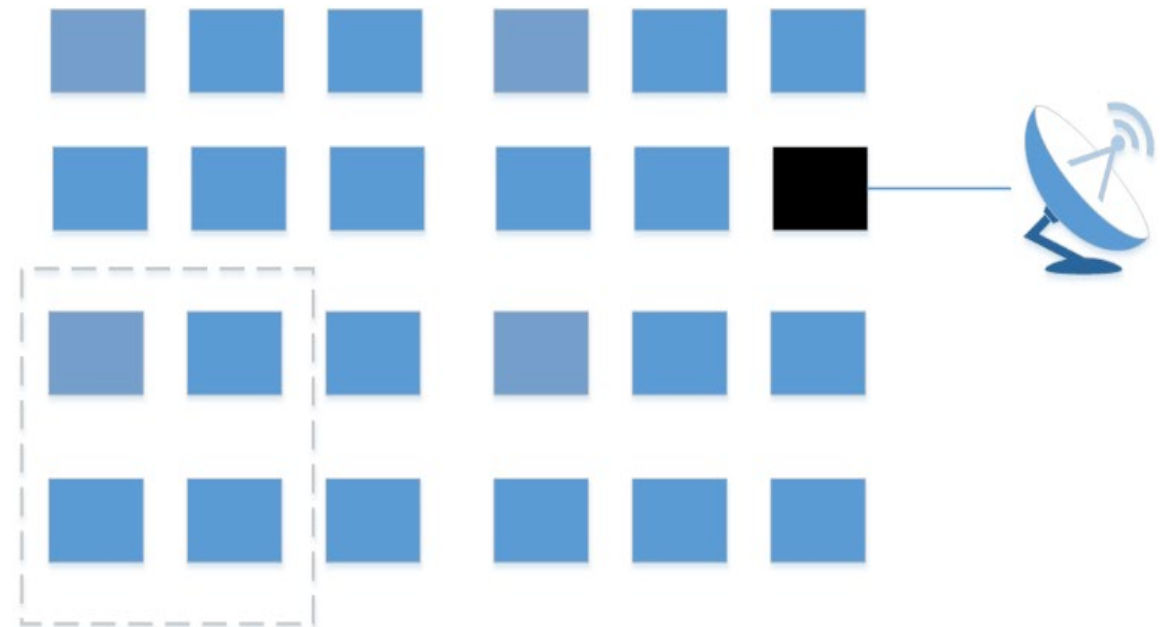
- Controlled flooding, where a node forwards data to its neighbor nodes.
- There can be rules for what data to forward, and to which nodes the data should be forwarded.



Exercise: Routing in Ad-hoc networks (ETSN10 230316)

The image shows a sensor network with the sink marked in black. All sensors are stationary, and their positions are known. The sensors can communicate multi-hop, but only to neighboring sensors. There is a message coming from the back-end that should be distributed to **all** nodes in the marked square (with dashed lines). Since each data transmission cost energy, it is important to minimize the number of data transmissions.

Describe a suitable routing protocol for this system and data transmission method. Also, use this routing protocol and calculate the minimum number of data transmissions required to transmit the message to all the nodes within the marked square. You need to include a good motivation to your answer.



Suggested solutions

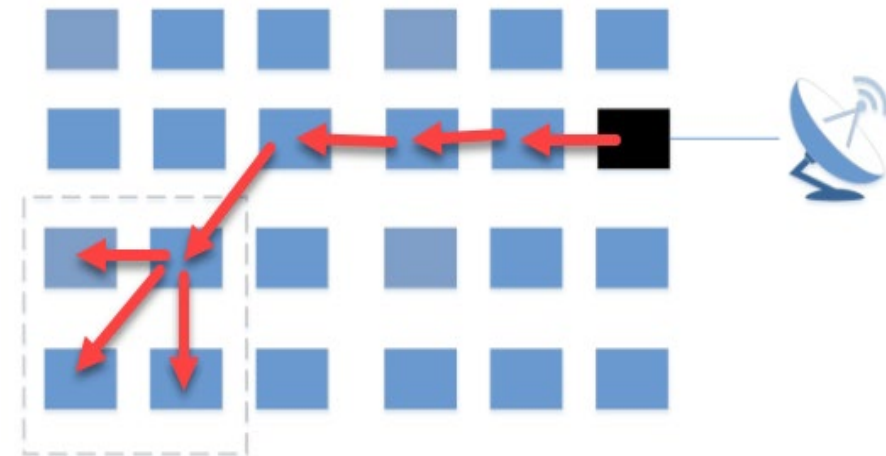
This problem did not have one single solution. For full points, you should describe a routing protocol that is suitable for this particular network system. It does not have to be a standardized protocol, you can design a good protocol yourself. The sensors are stationary, and their positions are known.

Here are three examples of solutions that were given full points on the exam.

Student solution 1

Since the sensors are stationary and the positions are known, this means that each node can store the routes with the least cost metric for each of the available nodes through geographically based routing. Upon receiving a packet with its node id, the node will look at the network layer location address and forward the packet to the neighboring node that is geographically closest to the destination. A node can also broadcast the data if it exists within the destination target area.

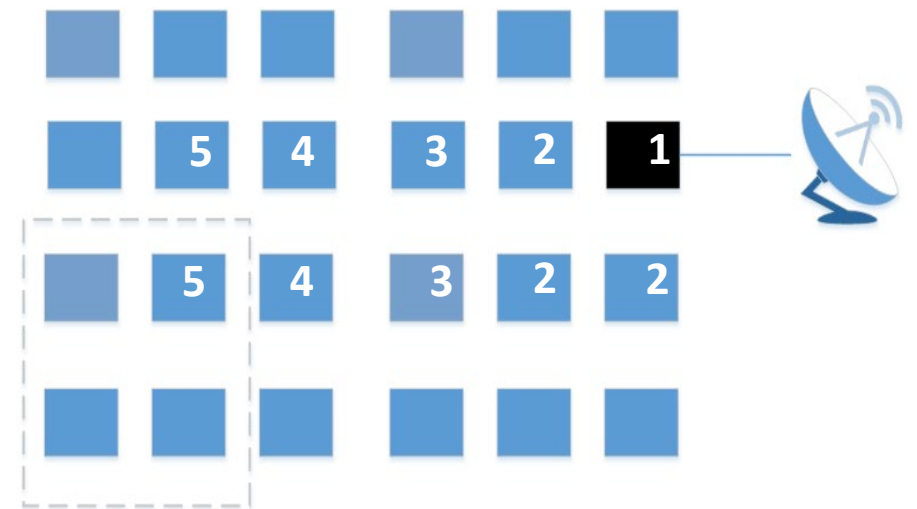
For example, the minimum data transfer needed for this method is 5, where 4 transmission is a hop by hop transmission to reach the node in the target area that is closest to the sink. This node then broadcasts the received data to its neighbor which minimizes the amount of needed transmission.



Student solution 2

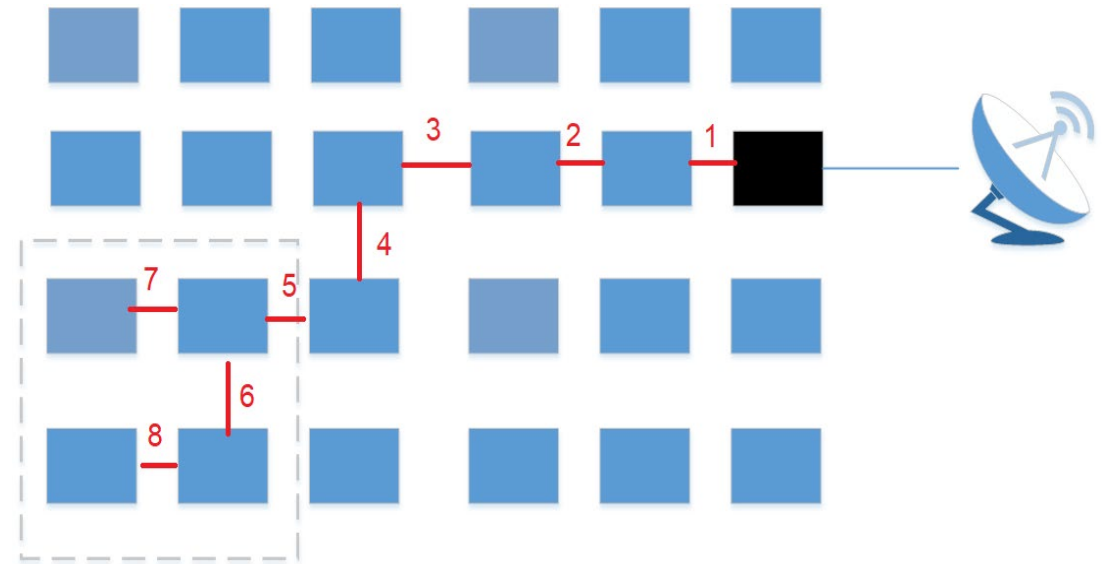
A suitable routing protocol would be a broadcast-based routing protocol. This protocol is simple, easy to implement, and guarantees message delivery to all nodes within the market square. The sensors are also stationary, which means that the network topology does not change frequently, which further proves that the broadcast-based flooding protocol is more suitable.

To minimize the amount of data transmissions required, we could implement a rule that states only the middle two rows of nodes broadcast to all of their neighbours. This would make the minimum number of data transmissions to be 10. This includes the sink to its neighbours, then the middle two row nodes to their neighbours (x9). This will allow all of the nodes in the square to have the message.



Student solution 3

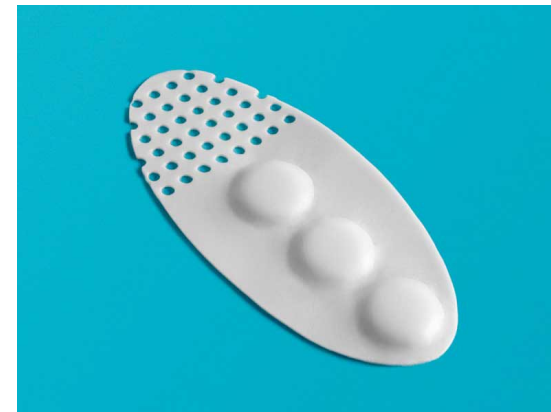
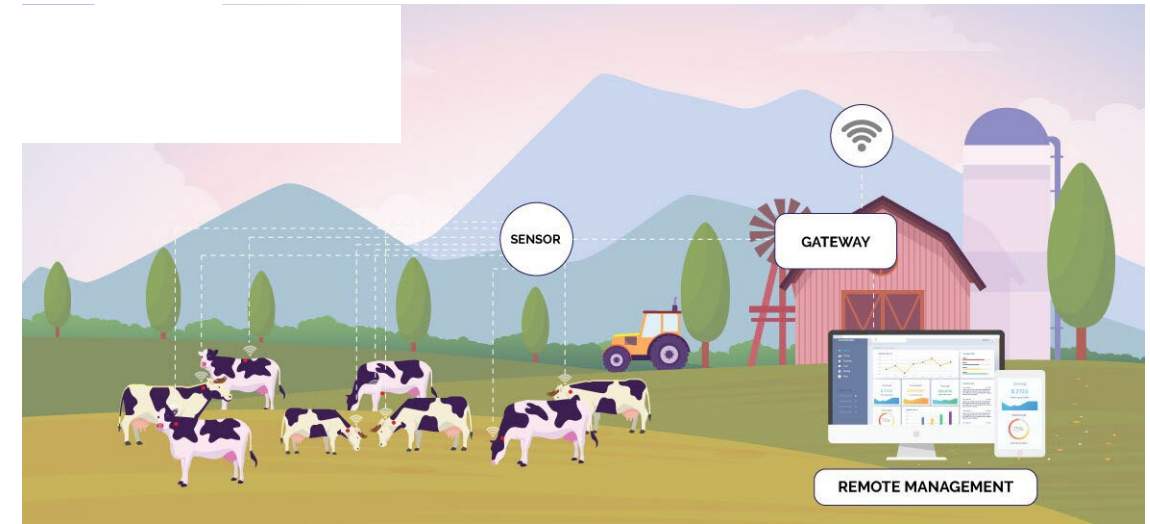
Since all nodes are stationary with known positions, a position-based routing system with a known (i.e. hardcoded) routing table is highly suitable. This avoids the overhead inherent in discovering routes (either regularly or on-demand). In addition to this, multicast support is desired, as we wish to send the data to multiple (but not all) devices. A route that achieves the goal in 8 hops may look as follows (though the exact route may differ assuming the real-world locations don't follow a perfect grid).



Resource-constrained networking

Resource-constrained networking

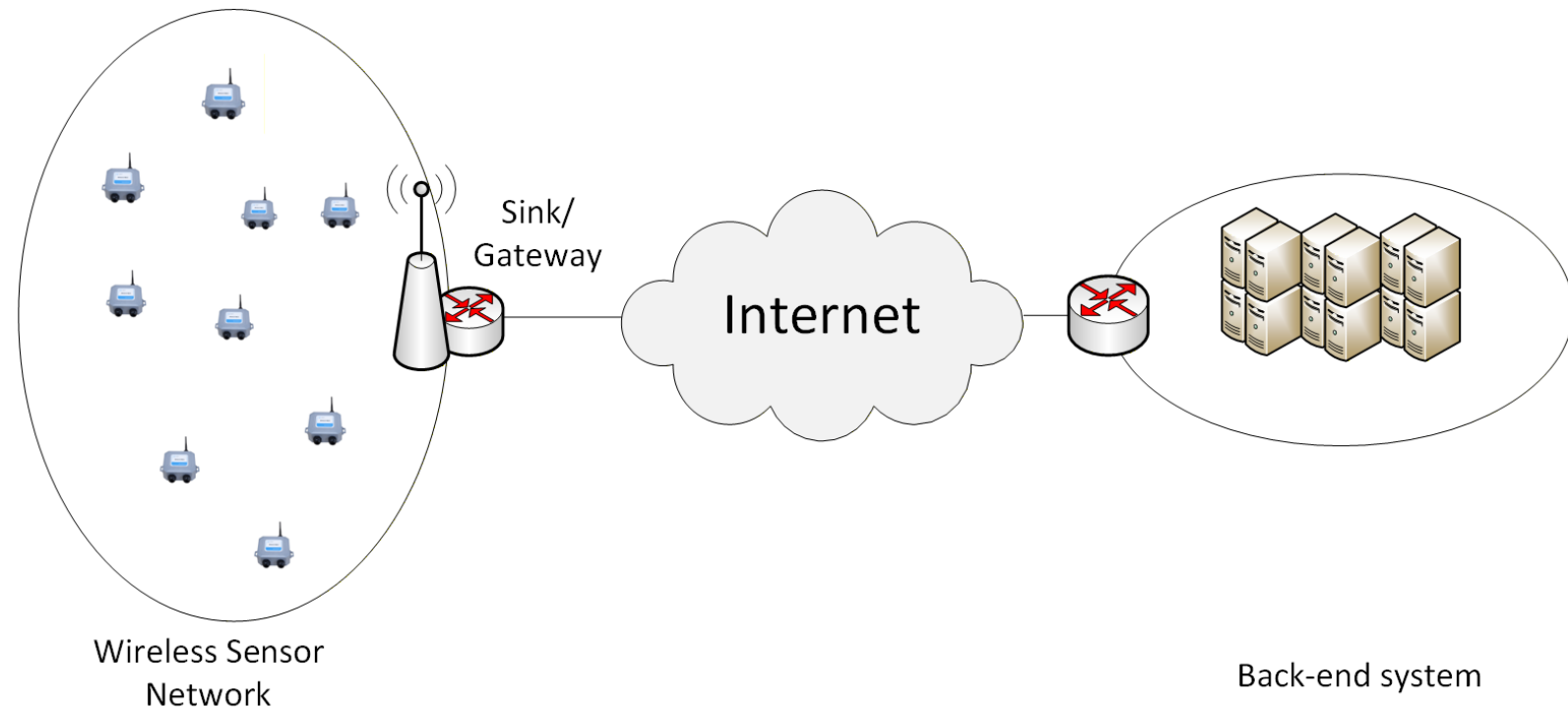
Resource-constrained networking includes all types of network technologies where **low energy consumption** is important.



Sources: <https://www.hudsonmedicalinnovations.com/body-sensors>
<https://psiborg.in/livestock-monitoring-using-iot/>
<https://www.tern.org.au/news-standards-assist-conservation-decision-making/>

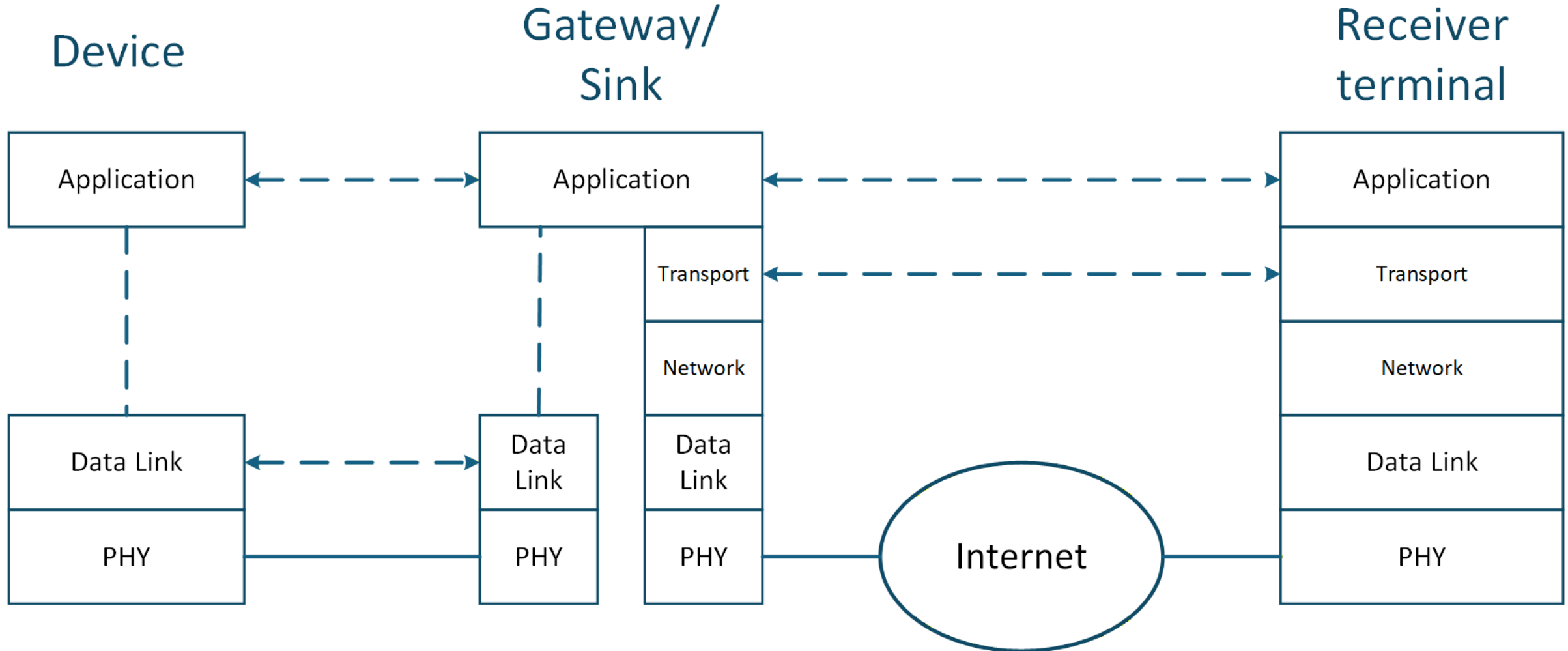
Wireless sensor networks

- **Wireless sensor networks (WSNs)** refer to networks of sensors that monitor and record the physical conditions of the environment and forward the collected data to a central location.
- The main objective of a WSN is usually to **send data about the environment to a sink/gateway with as low energy consumption as possible**, for further transport to a back-end server (user application).



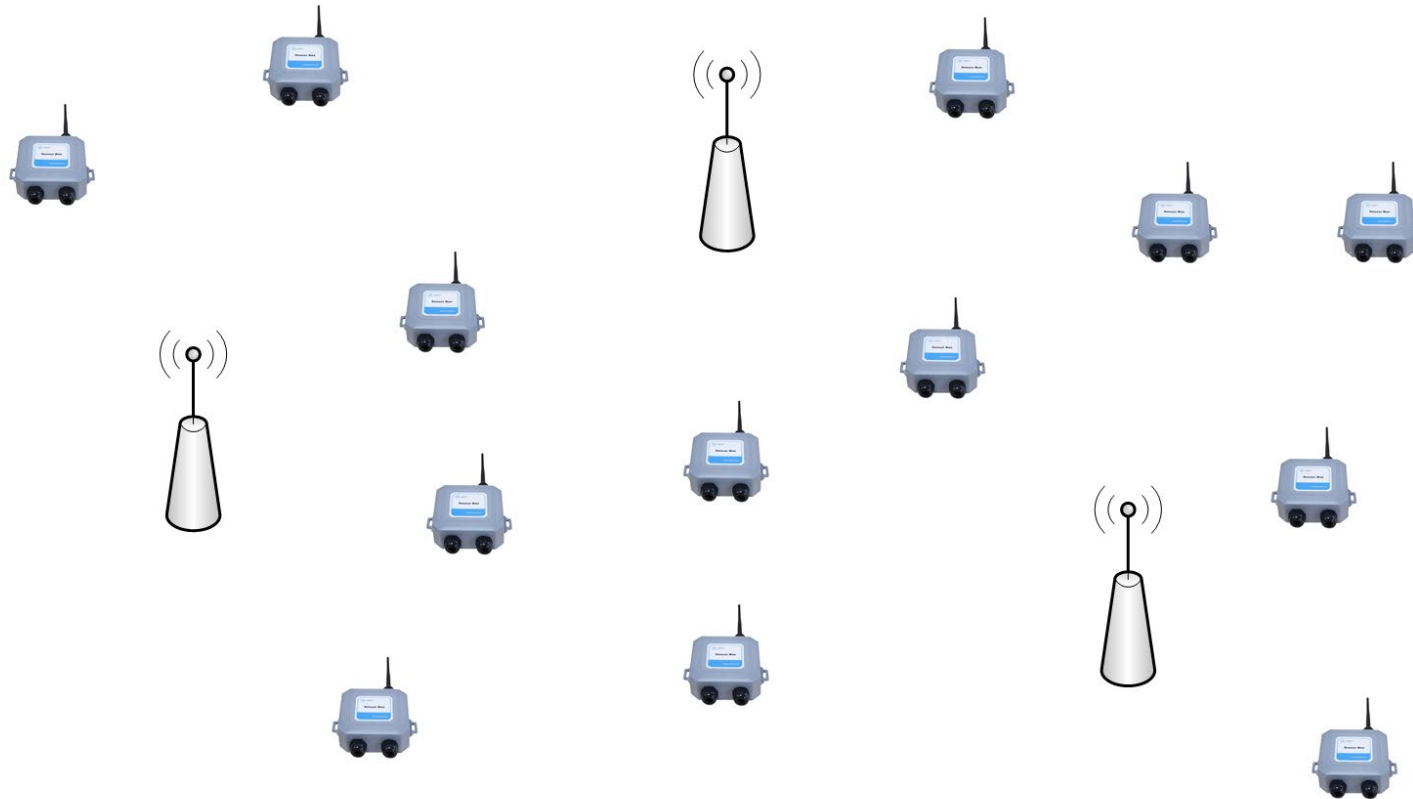
Typical protocol stack for sensor networks

Not a definition, but the common practice.



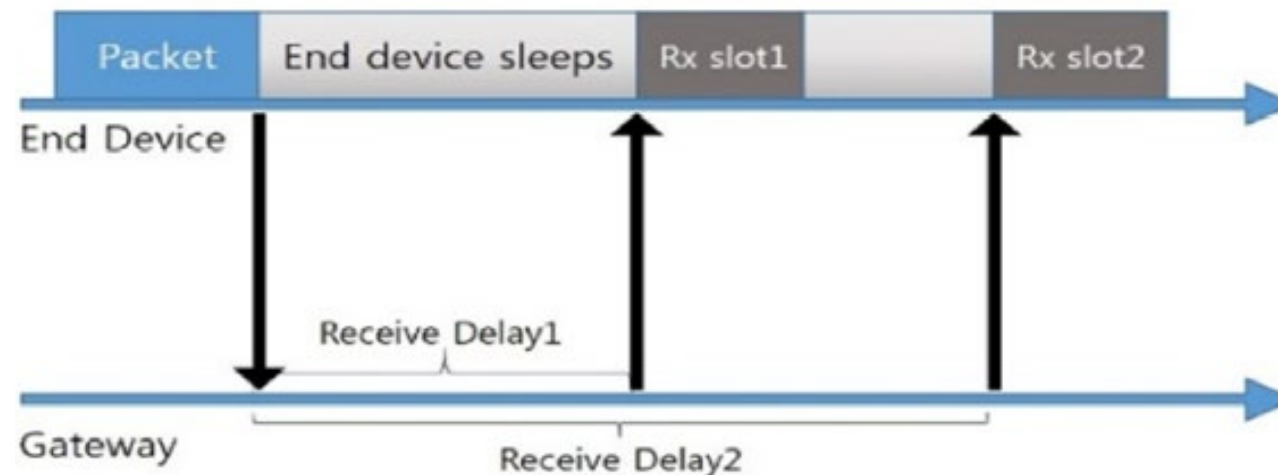
Wireless sensor network, basic scenario

- A large number of sensors with very limited power.
- One or more sinks/gateways/access points (with better access to power).



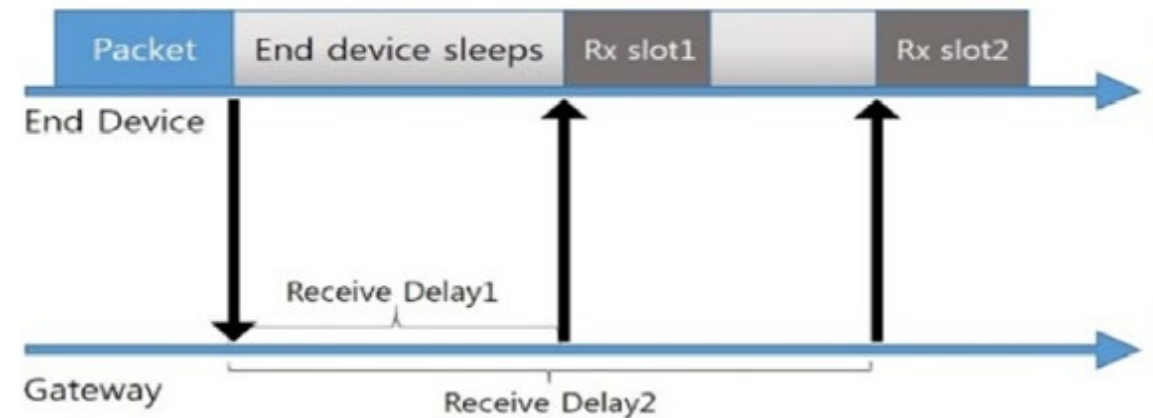
Resource-constrained data communication

- The basic idea for resource-constrained data communication is that the devices must be allowed to go into **sleep-mode** when they do not send or receive data.
- Therefore, the data communication is often **half-duplex**, that is, a device either sends or receives data, never both at the same time.
- Also, **data communication is often predefined or even scheduled**, so that the devices know when they can enter sleep-mode.



Resource-constrained data communication – Main characteristics

- Resource-constrained data communication requires **non-critical applications**.
- For low energy consumption, the **data rate must be (very) limited**.
- MAC protocols for resource-constrained data communication usually allow for the device/sensor to use a **sleep mode** when not transmitting or receiving data.
- The communication protocols may use **predefined or scheduled data transmissions** so that the device/sensor know when it can go to sleep mode.
- Also, the data communication can be in **half-duplex**, that is, a device either sends or receives data, never both at the same time.



Resource-constrained networking?

You have been given the task to help a friend that wants to install a smart lighting system for their greenhouse. The system includes about 10 sensors distributed in the greenhouse. Also, the system includes smart lamps that can be controlled via the Internet. The sensors collect and send data to a back-end server system.

The back-end server system includes an AI system that processes the data and then adjusts the lamps in the greenhouse so that the plants always have optimal light.

Your task is to suggest a solution for the complete networked system.

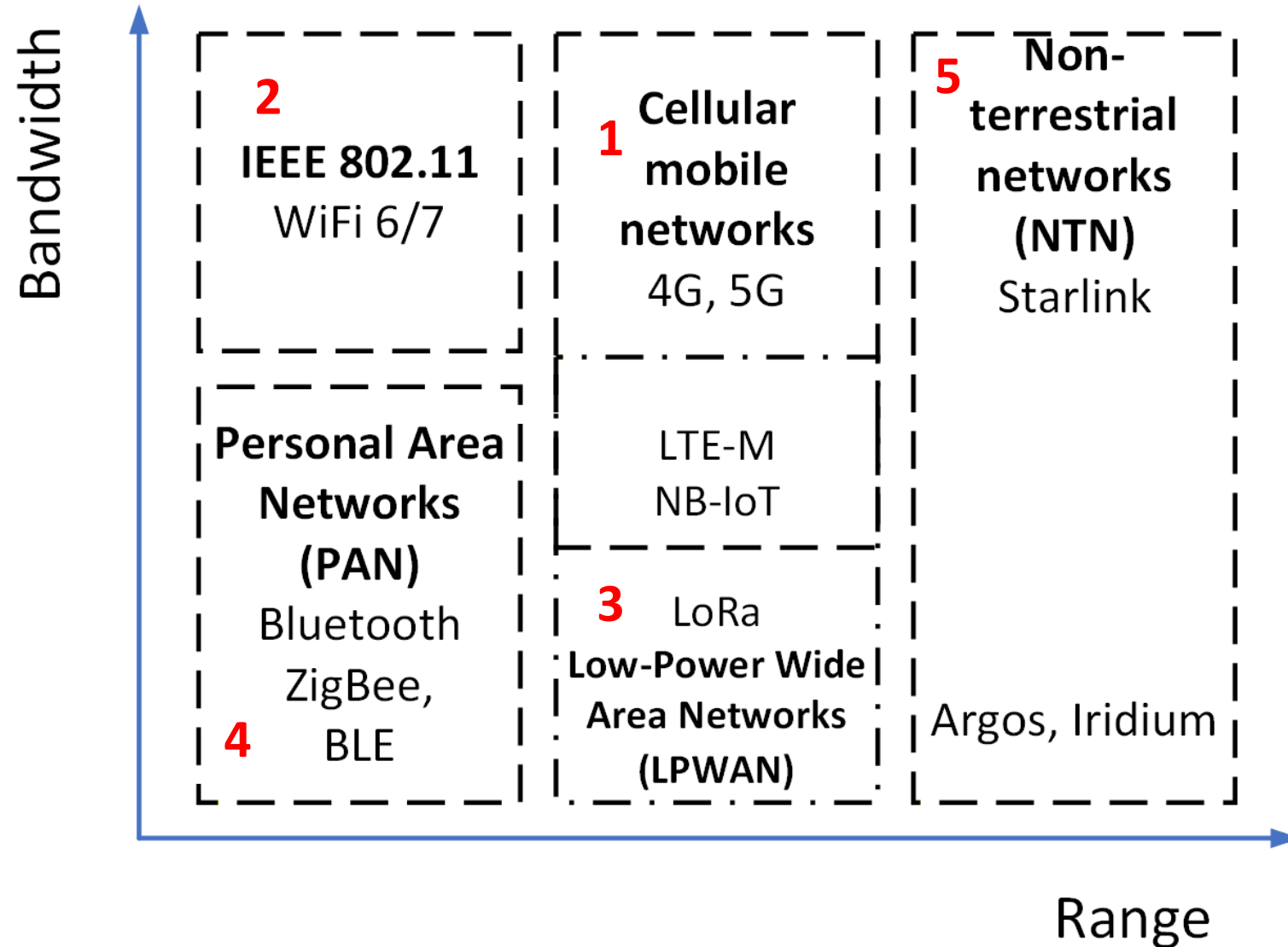


Suggested solution

- The lamps are not resource-constrained.
 - If the sensors use batteries, the solution depends on how easy it is to re-charge or change the batteries.
- 1. Easy to re-charge or change batteries:** The solution does not require resource-constrained networking.
 - 2. The batteries cannot easily be re-charged or changed:** The solution requires resource-constrained networking.

Note: Since the greenhouse must have good access to electricity, there is no real need to use resource-constrained batteries for the sensors.

Coming lectures



- 6. Delay-tolerant networking
- 7. Interplanetary networks
- 8. Underwater networks



LUND
UNIVERSITY