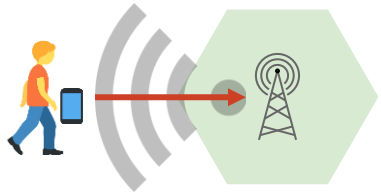


Lecture 25 (Wireless 2)

Cellular

Lecture 25, Spring 2026

Slides credit: CS168@UC Berkeley

Brief History of Cellular Networks

Lecture 25, Spring 2026

Why is Cellular Different?

- **Brief History**
- Standards
- Challenge: Mobility

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

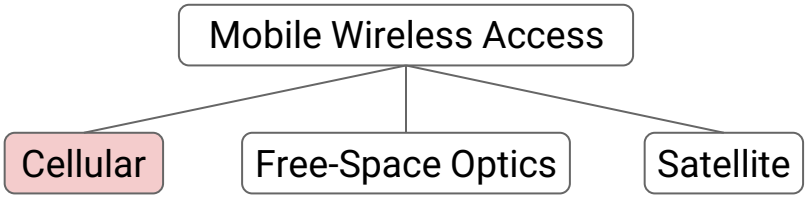
Why Study Cellular?

Goal: Wireless mobile connectivity, e.g. watching video in a moving car.

- Cellular is the dominant approach today.
  - Over 50% of web traffic originates from a cellular device!
- Other technologies (e.g. satellite) also exist.

Active area of research!

- New bandwidth-intensive mobile apps, e.g. virtual reality, self-driving cars.
- Cellular network is facing severe scaling challenges.
  - Deploying towers and buying spectrum is expensive.
  - Traditional operators (AT&T, Verizon) don't have a reputation for rapid innovation.



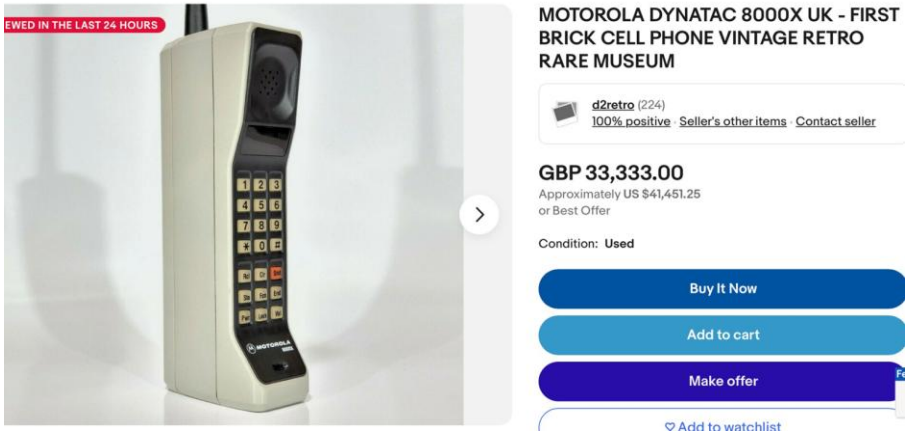
Brief History of Cellular Networks

Cellular networks are derived from the old telephone network.

- Original purpose: Make phone calls wirelessly.

Martin Cooper made the first mobile call on this Motorola phone.

Sold for $4,000 in 1983 (over $12,000 today).



Apparently worth over $40,000 today as an antique.

Brief History of Cellular Networks

Roots in the telephone network led to design choices that differ from the Internet.

Cellular networks:

- Resource reservations.
- Per-user state in the network.
- Emphasis on accountability.

The Internet:

- Best-effort.
- Per-flow or per-packet state.
- Doesn't really track usage per user.

In recent years, cellular networks evolved to be more compatible with the Internet.

- Today, can think of cellular networks as Layer 2 networks within the Internet.

Cellular Network Standards

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- **Standards**
- Challenge: Mobility

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

Cellular Standards Evolution

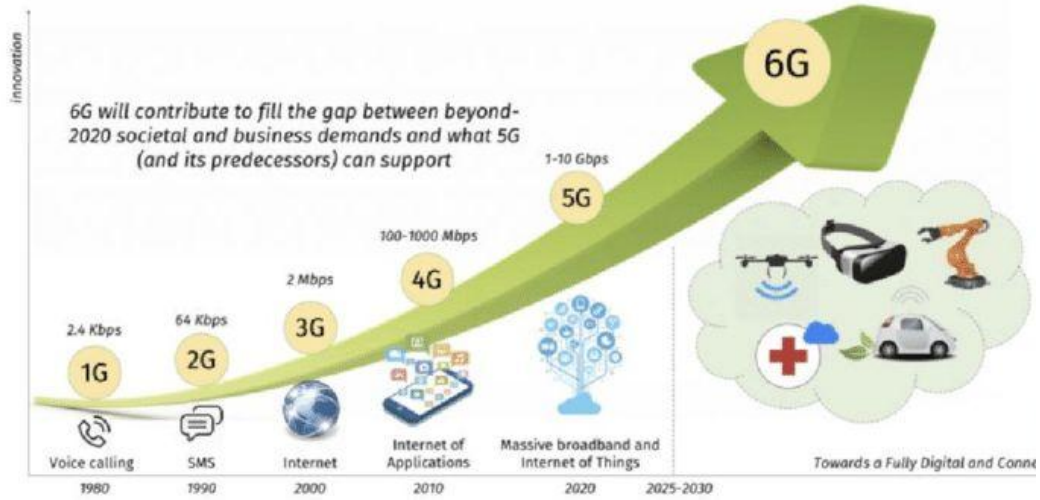
3GPP (*3rd Generation Partnership Project*) consortium oversees standardization efforts.

- Includes equipment vendors and telecommunications companies.
- Everyone must agree on protocols to achieve interoperability.

Standards ratified by ITU (*International Telecom Union*), part of the United Nations.

New generation every 10 years: 1G, 2G, 3G, 4G, 5G.

- 5G introduced in 2019, still being deployed.
- 6G coming in 2030.



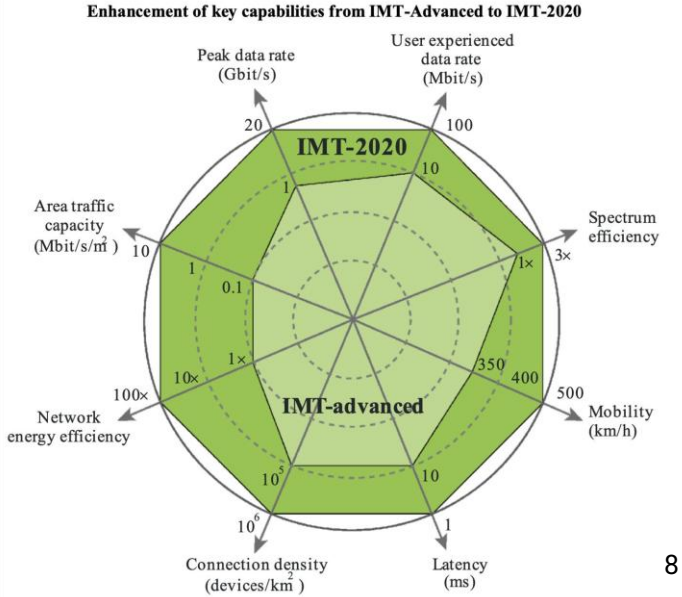
Cellular Standards Evolution

Each generation aims for a ~10x improvement along a few different dimensions:

- Peak theoretical data rate.
- Average data rate experienced by users.
- Mobility: Connection while user travels at high speed.
- Connection density: Number of devices in a specific era.

Light green = 4G quality along 8 different dimensions.

Dark green = 5G quality along those same dimensions.



Cellular Standards Evolution

In addition to performance evolution, there's also been an *architectural* evolution:

- 1G:
  - Analog.
  - Designed for voice calls.
- 2G/3G:
  - Mostly circuit-switched.
  - Focused on voice traffic. Some texting. Barely any Internet access.
- LTE/4G onwards:
  - Packet-switched.
  - Voice just one of many different applications.

Cellular specifications are long and complicated.

- Components/protocols are renamed in every generation!
  - "Base station" → "NodeB" → "evolved Node B (eNodeB)“ → next-gen Node B (gNB)

In this class, we’ll use terminology loosely based on the LTE architecture.

Challenge: Mobility

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- **Challenge: Mobility**

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

Key Challenge: Mobility

What fundamental new requirements does mobility introduce?

- **Discovery**: What cell tower should a mobile device connect to?
- **Authentication**: Should the tower provide service to this device?
- **Seamless** communication: No disruption to new/ongoing application sessions.
- **Accountability**: Enforcing resource limits based on the user's service plan.

Cellular Infrastructure

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

Cellular Networks

- **Infrastructure**
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

Infrastructure Components (1/5): Radio Towers

Inside a radio tower:

- **Radio transceiver**: Converts data to signals sent over the *air interface*.
- **Radio controller**: Decides how to allocate radio resources.
  - Traditionally near the tower, but sometimes in the cloud now.

Range of tower

Antenna

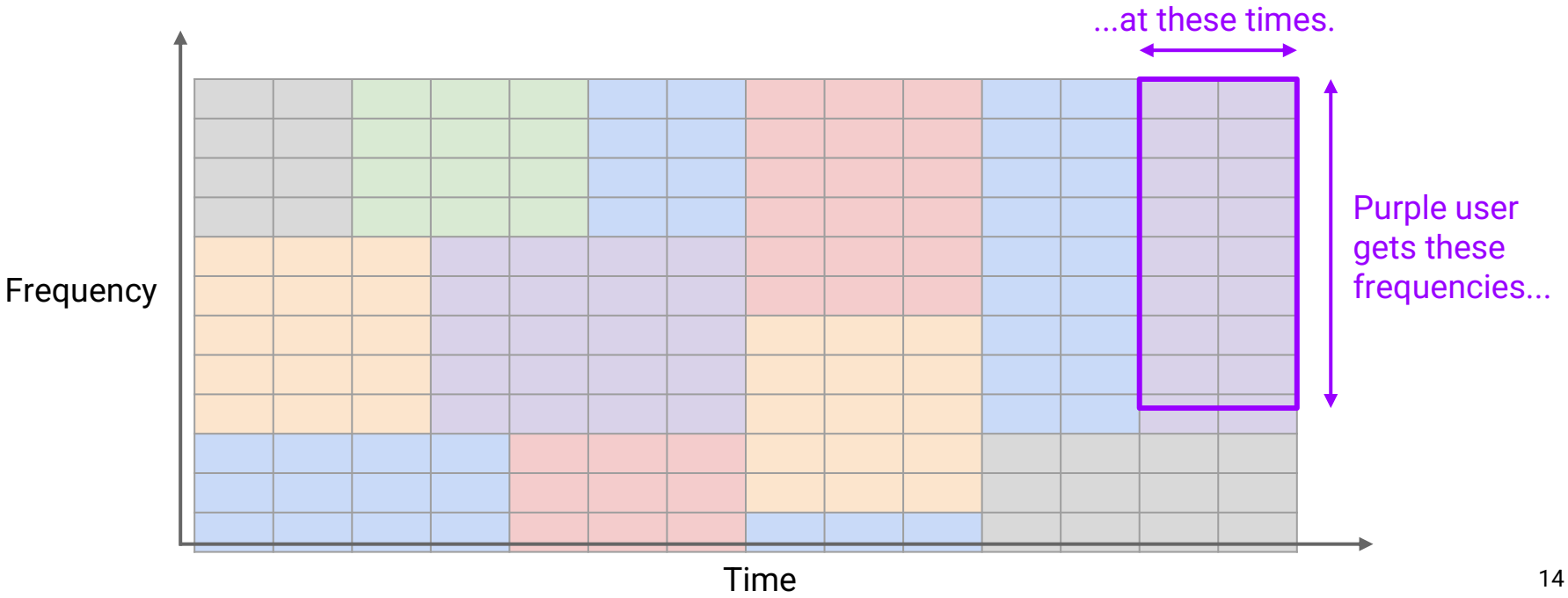
Transceiver

Controller

Infrastructure Components (1/5): Radio Towers

Simplified model: Radio controller is like a CPU running a scheduler.

- Decide who gets to transmit when, and on what frequency.
- Each block represents one part of the spectrum at one time slot.

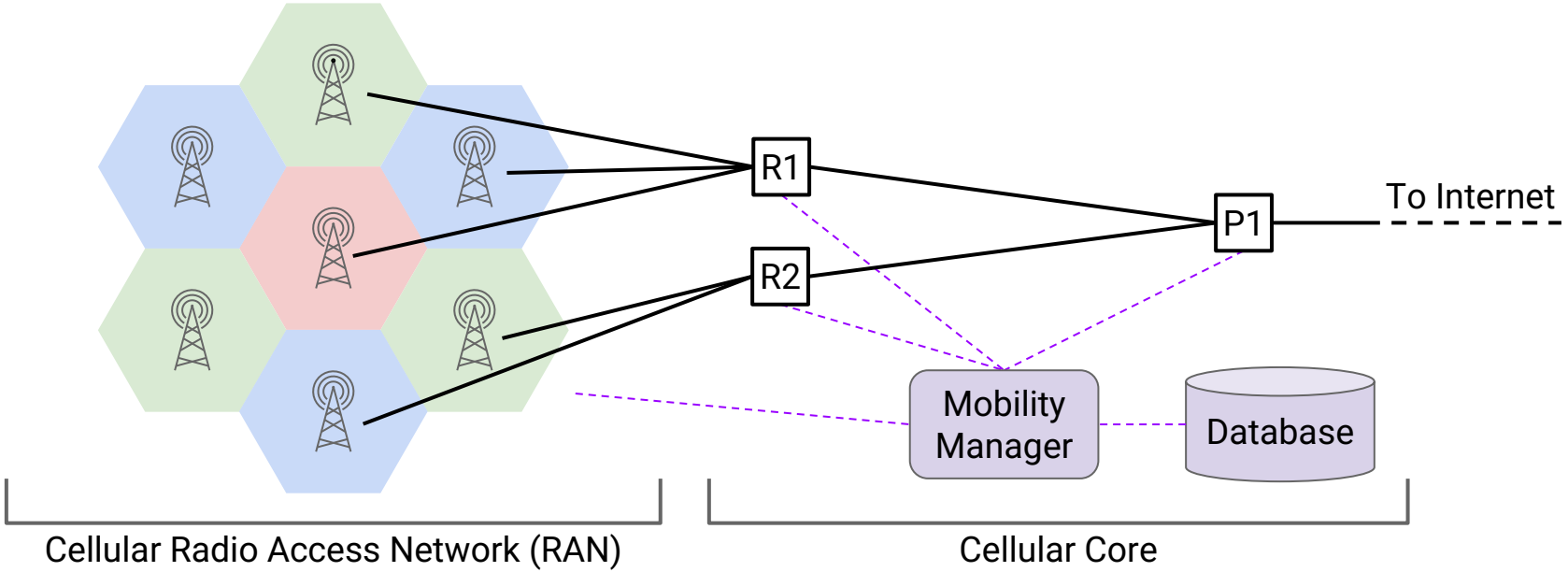


Infrastructure Components: Cellular Core

Each operator has a **radio access network** of many towers.

- Neighboring towers are assigned non-overlapping frequency ranges.
- Towers in more populated areas can get allocated more frequencies.

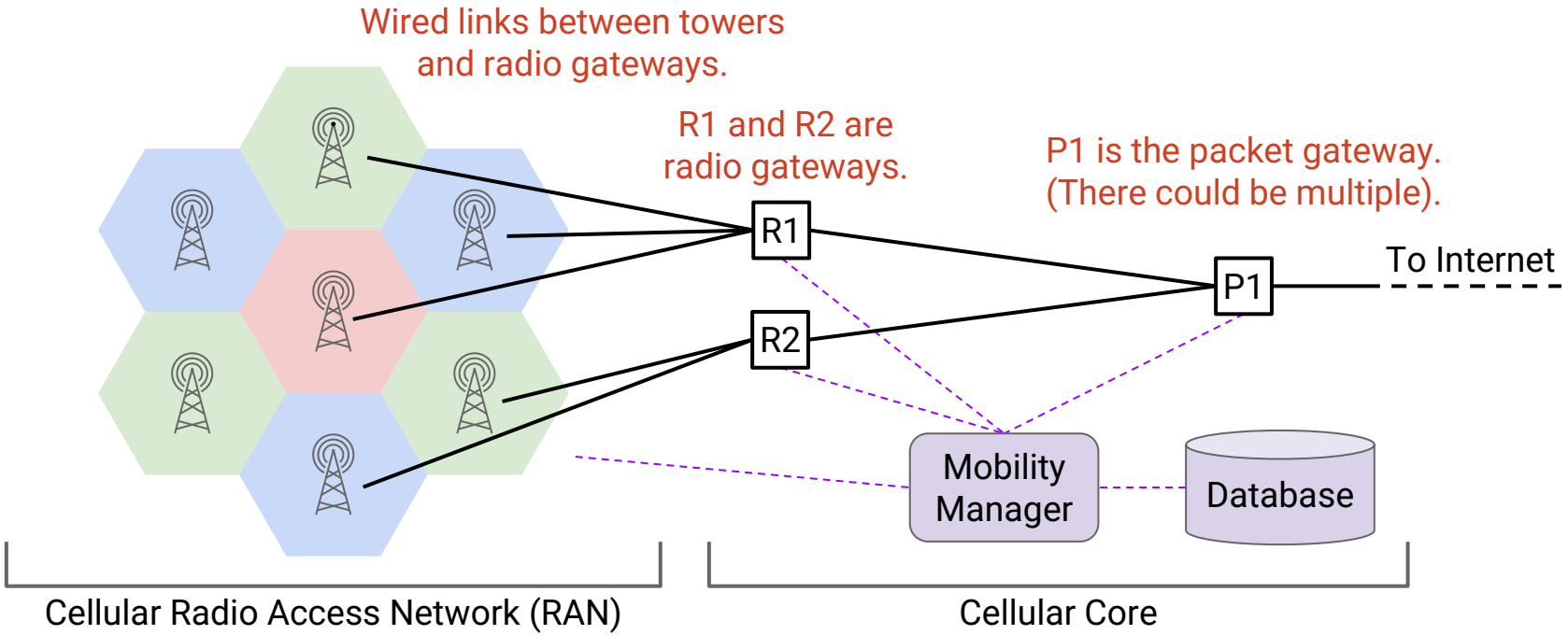
The **cellular core** is the "backend" of the cellular network.



Infrastructure Components (2/5 and 3/5): Radio Gateway, Packet Gateway

Data-plane components (routers):

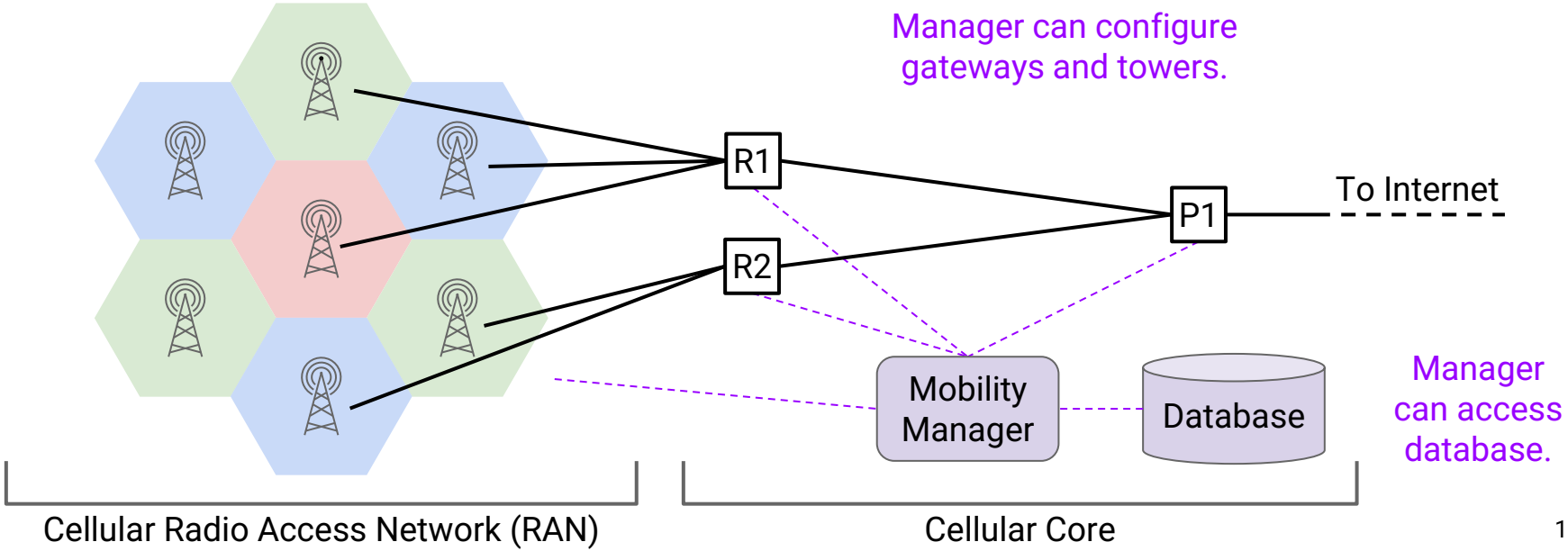
- **Radio gateway**: Boundary between RAN and core.
- **Packet gateway**: Boundary between cellular network and rest of Internet.



Infrastructure Components (4/5 and 5/5): Mobility Manager, Database

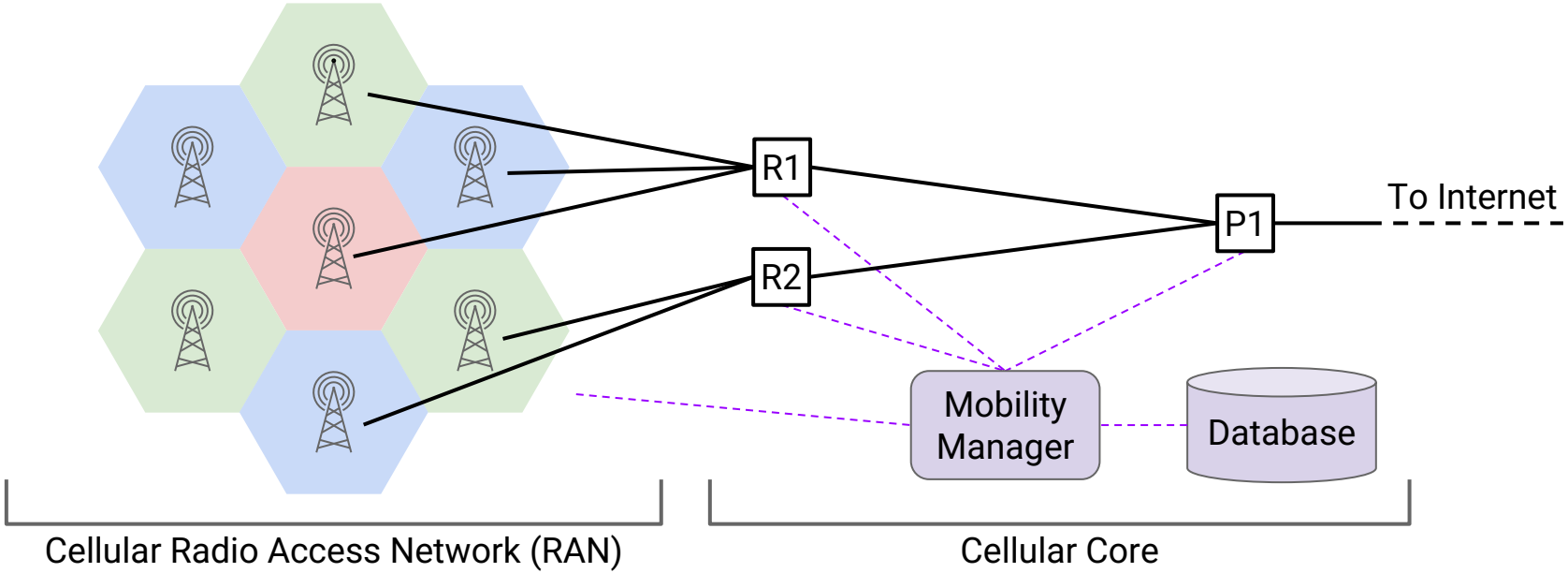
Control-plane components:

- **Mobility manager**: Handles authentication, mobility, location tracking, etc.
- **Database**: Stores information about customers.



Infrastructure Components: Summary

- Cell towers (arranged in a RAN).
- Data plane: Radio gateways, packet gateways.
- Control plane: Mobility manager, database.



High-Level View

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

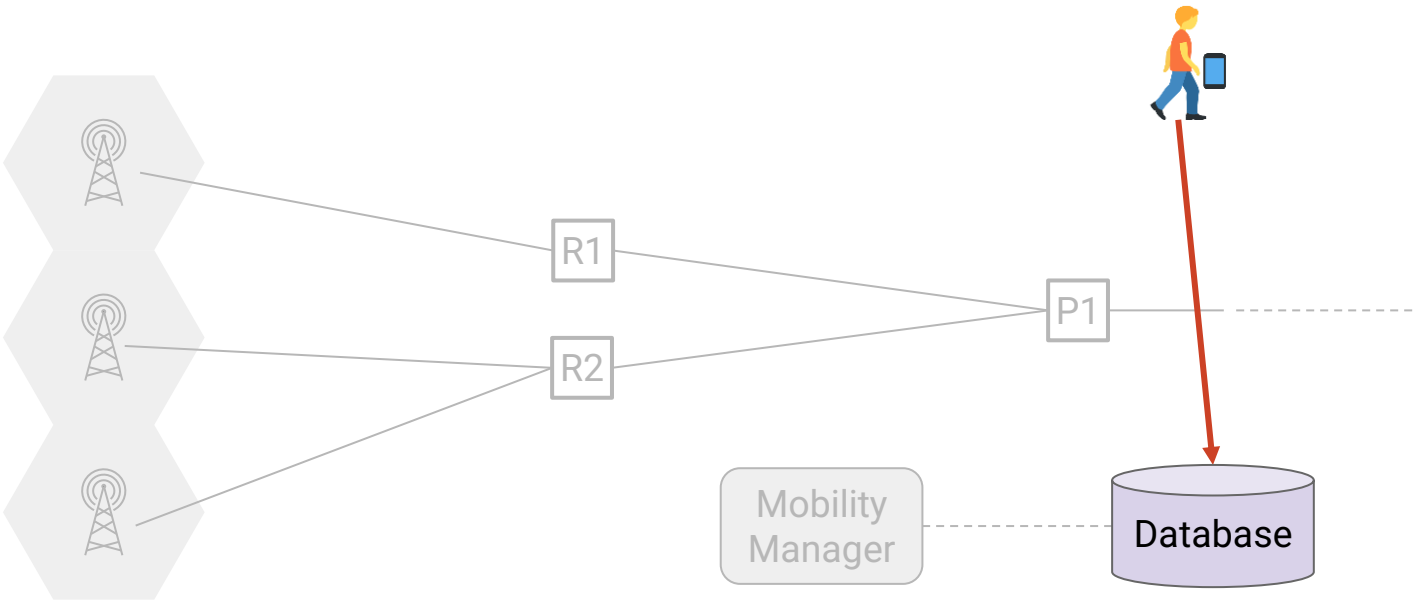
Cellular Networks

- Infrastructure
- **High-Level View**
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

High-Level View (0/4) – Registration

Step 0: **Registration**.

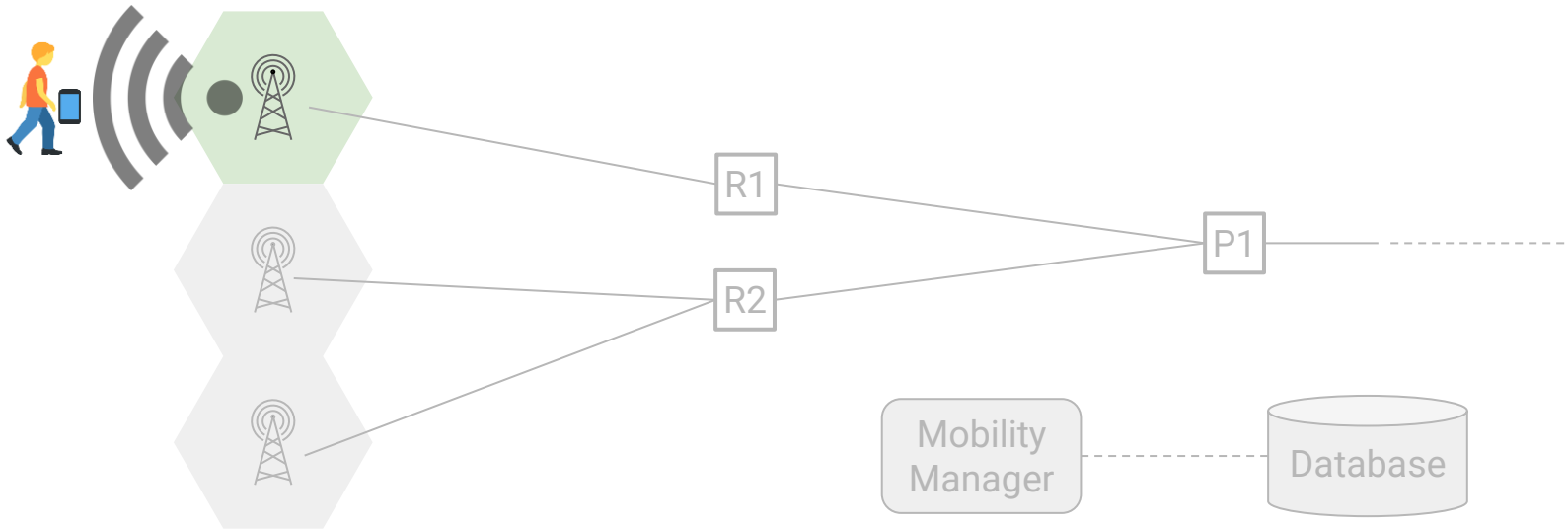
- User registers for the service. Database is updated.



High-Level View (1/4) – Discovery

Step 1: **Discovery**.

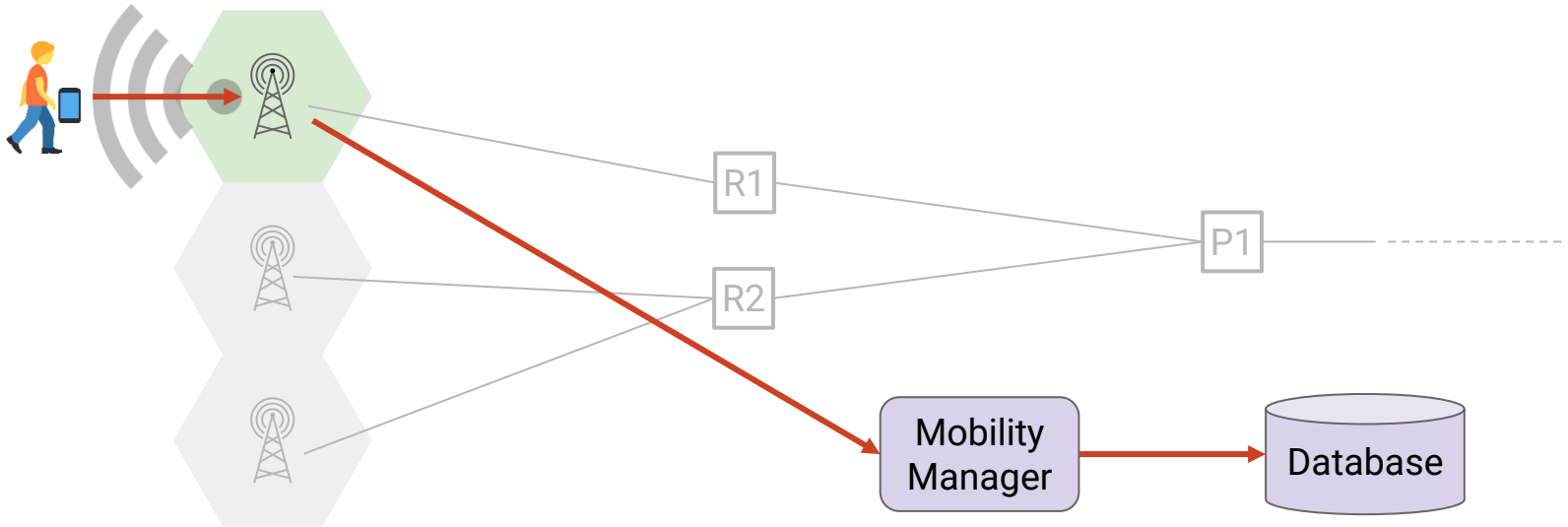
- User wants to connect.
- User device discovers available towers and picks one.



High-Level View (2/4) – Attachment

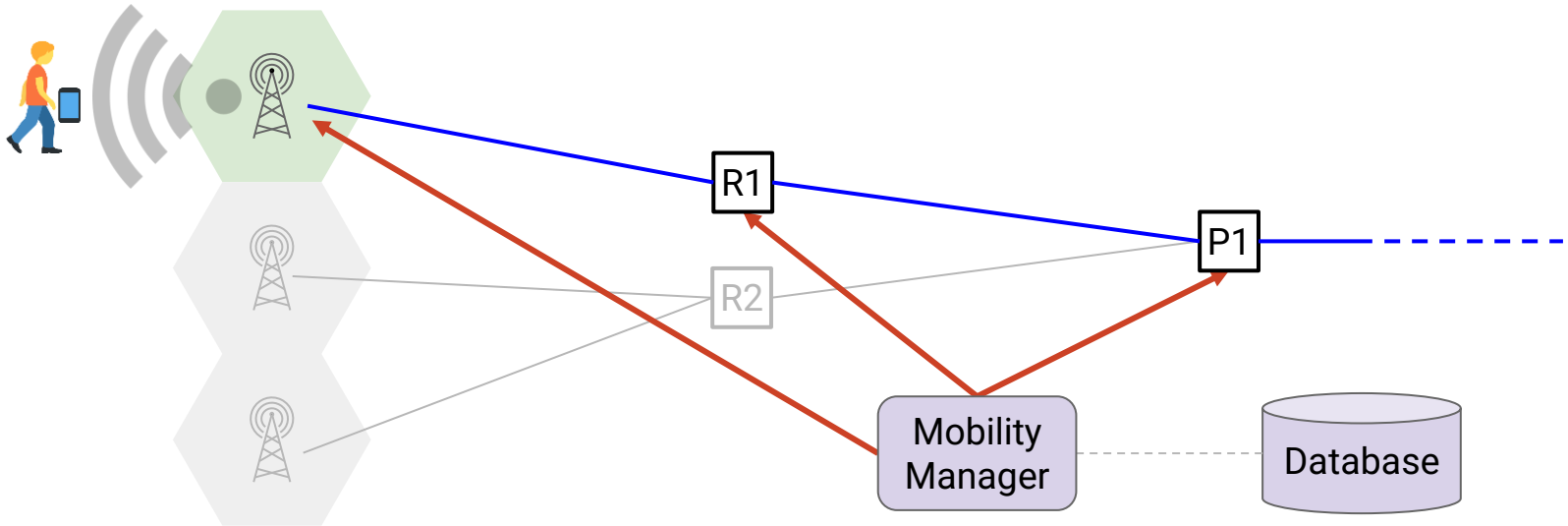
Step 2: **Attachment**.

- Device asks the tower to connect.
- Tower checks with mobility manager if connection is allowed.



Step 2: **Attachment**.

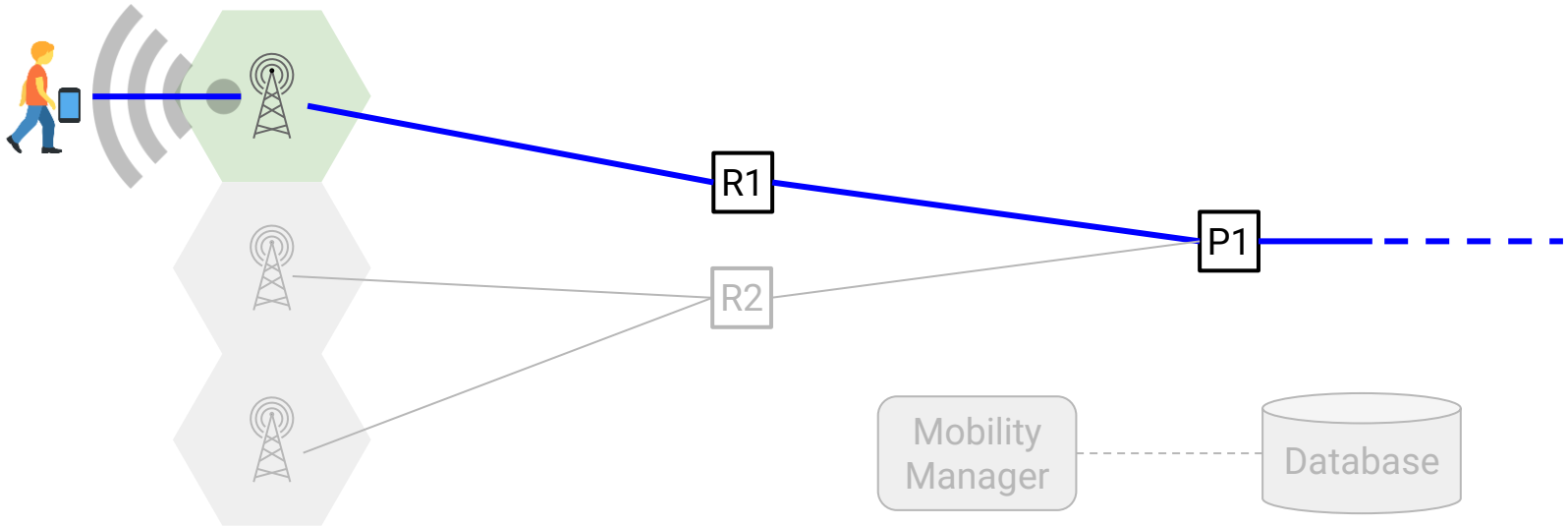
- If manager approves request, it configures a path between user and Internet.



High-Level View (3/4) – Data Exchange

Step 3: **Data exchange**.

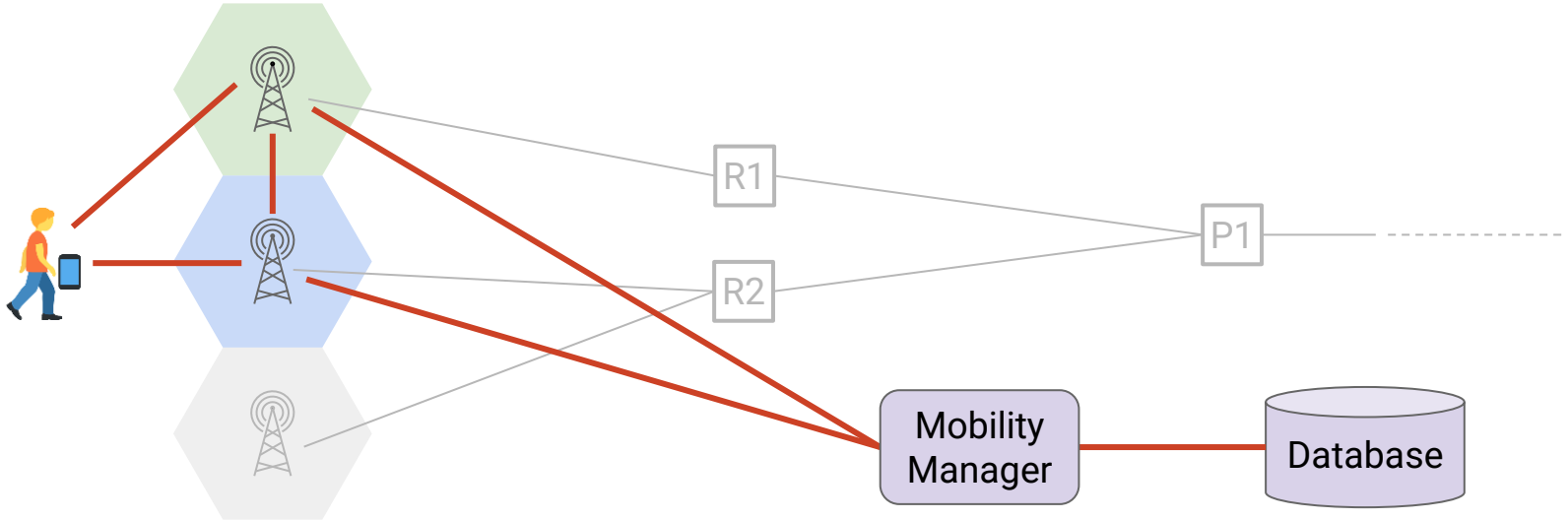
- User can now send and receive data!
- Packets travel along the path configured in previous step.



High-Level View (4/4) – Handover

Step 4: **Handover**.

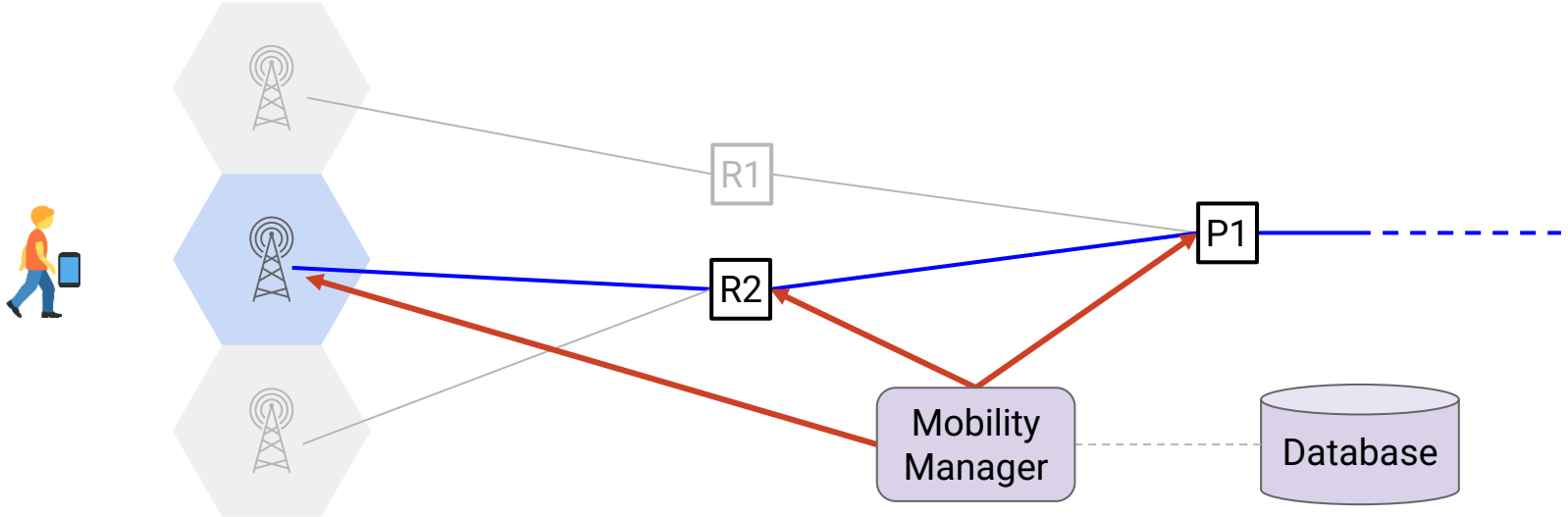
- Device might move away from old tower, closer to a new tower.
- Device, old tower, new tower, and manager work together to switch towers.



High-Level View (4/4) – Handover

Step 4: **Handover**.

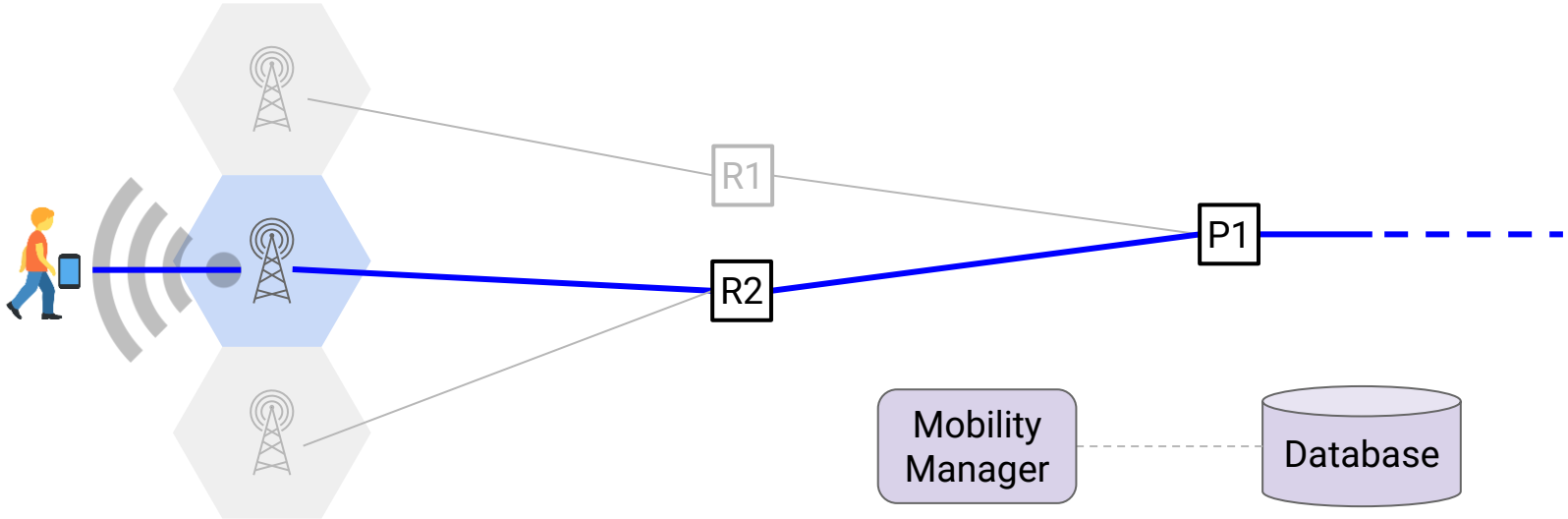
- Manager configures a new path through the network for the user.
- Handover must be seamless. We can't interrupt the user's connection!
  - User's IP address should stay the same.



High-Level View (4/4) – Handover

After handover, user has a new path through the network.

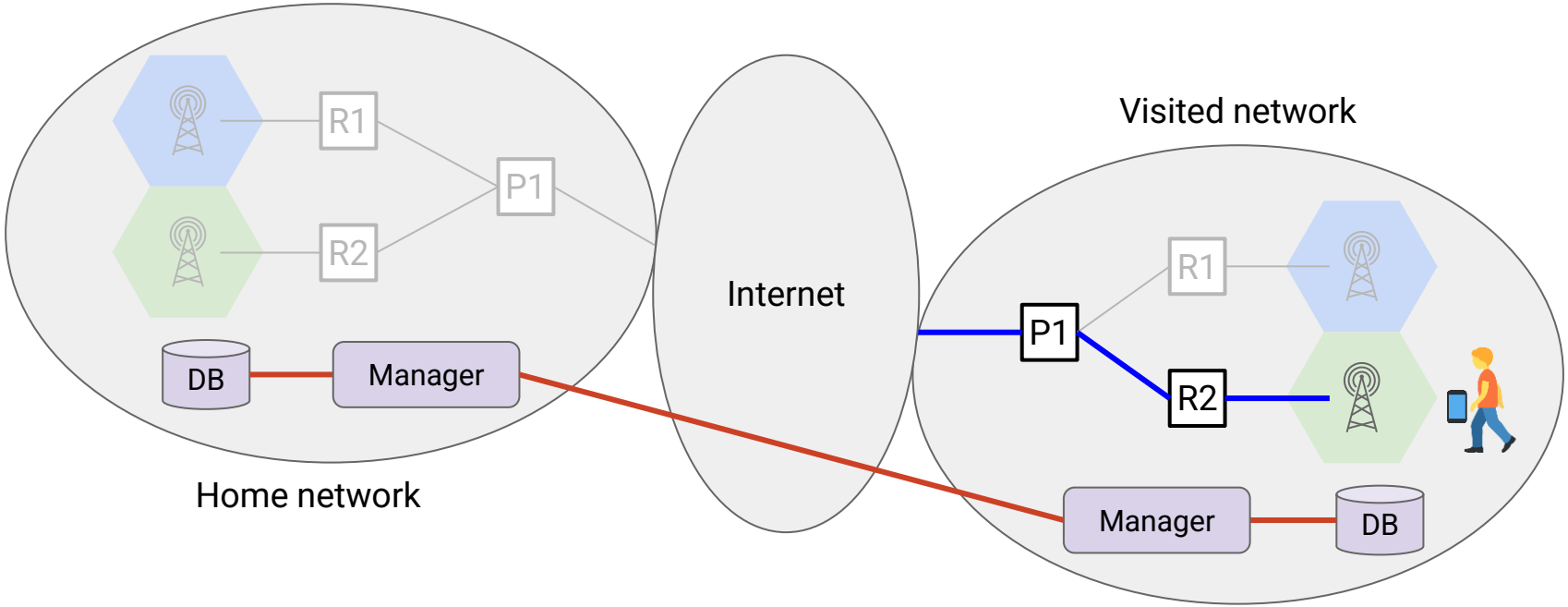
Step 3 (Data Exchange) and Step 4 (Handover) repeat as the user moves around.



High-Level View – Roaming

One last feature is **roaming**: User connecting to a different network.

- Example: User visiting a different country.
- Mostly works the same as what we've seen.
- Main difference: Managers in the visited and home networks must coordinate.



Step 0: Registration

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

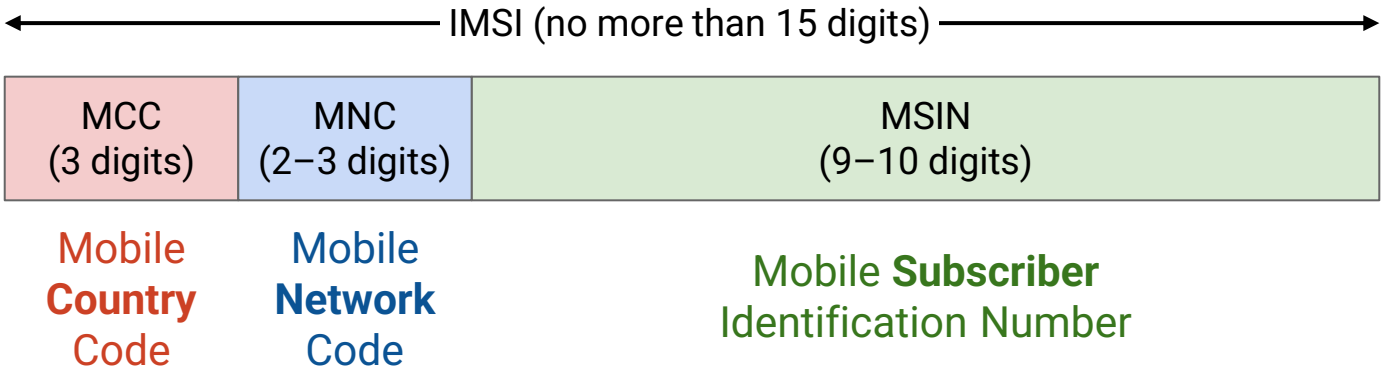
Cellular Networks

- Infrastructure
- High-Level View
- **Step 0: Registration**
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

Identifying User Devices: IMSI

When you register for a service, you receive an IMSI (*International Mobile Subscriber Identity*).

- Uniquely identifies a user's subscription.
- Securely stored in hardware (SIM) card.
- IMSI stays the same if you switch phones, but keep the same service plan.



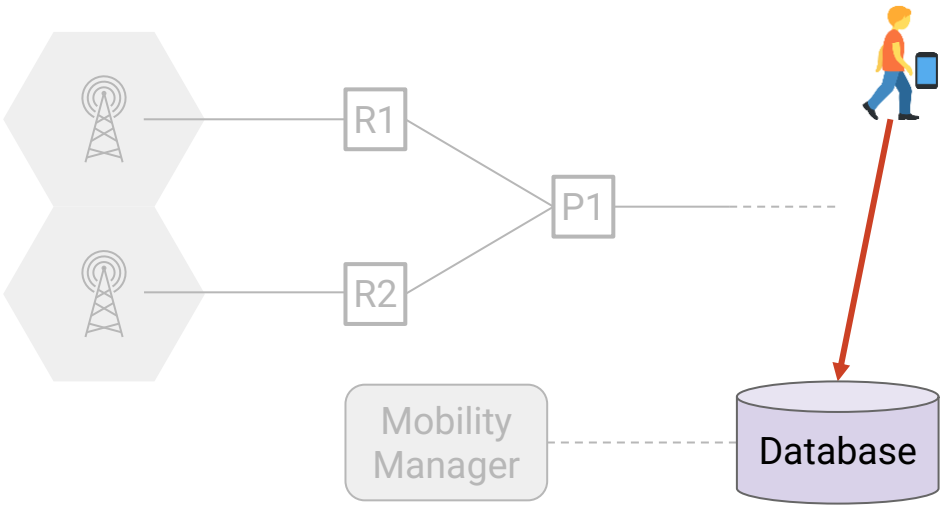
Identifying User Devices: IMSI, IMEI, IP, MSISDN

Different ways to identify a user device:

- **IMSI**: Identifies a user subscription.
- **IP address**: Assigned on attachment, typically retained across handovers.
  - Can change each time you attach to the network.
- **IMEI** (*International Mobile Equipment Identity*): Identifies a physical device.
  - Identifies device manufacturer and model.
  - Burned into hardware. Stays the same even if you switch plans.
- **MSISDN**: Your phone number.
  - Operator maps your phone number to your IMSI.

Step 0: Registration

- User registers for the service.
- Operator stores user's IMSI and plan information in the database.
- Establishes a shared key known only by the user and operator.
  - User: Stored in SIM card.
  - Operator: Stored in database.



Step 1: Discovery

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- **Step 1: Discovery**
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

Step 1: Discovery

Towers transmit periodic *beacons* to announce their presence.

- Beacons transmitted on a dedicated control channel.
  - Avoids interfering with data.
  - Each frequency range has its own control channel.
    Avoids beacons interfering with each other.
- Beacons identify the network operator.
  - User compares beacon against the network ID (in the user's IMSI).

User measures signal strength to different towers,
and picks the tower (belonging to its operator)
with the best signal.

Discovery: Finding Control Channel

Bootstrapping problem: How does the user know which control channel to listen to?

- Scan all frequencies.
  - Slow, but sometimes unavoidable.
- At registration, pre-configure device with a list of frequency channels.
- Cache previously-used channels.

Note: During handovers, the old tower tells the user the channel on the new tower.

- No need to scan! Handovers take 0.01s–0.1s.
- Contrast with attachment, which takes 10s–100s.

Step 2: Attachment

Lecture 25, Spring 2026

Why is Cellular Different?

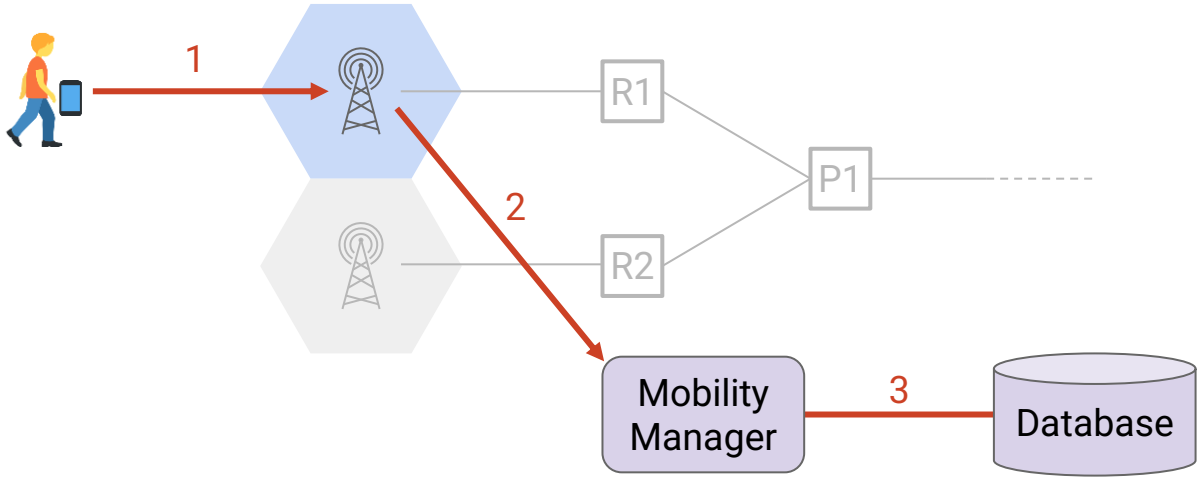
- Brief History
- Standards
- Challenge: Mobility

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- **Step 2: Attachment**
- Step 3: Data Exchange
- Step 4: Handover
- Roaming and Other Features

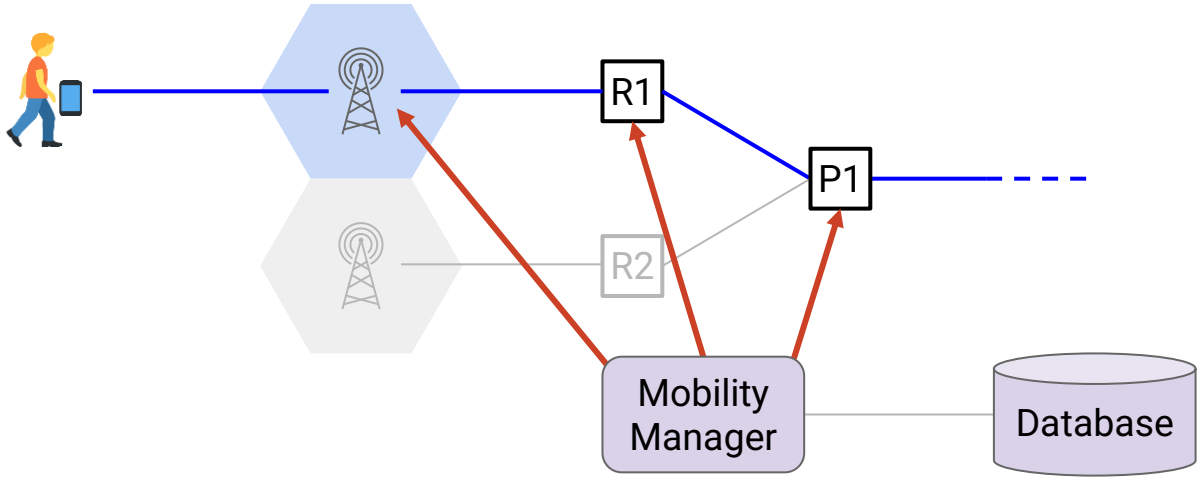
Step 2: Attachment

1. User sends attach request to tower, containing user's IMSI.
2. Tower forwards request to mobility manager.
3. Mobility manager processes the request, by looking up the IMSI in database.
   - Use secret key to authenticate: Is the user who they claim to be?
   - Use database to check service parameters: Did user pay their bills?



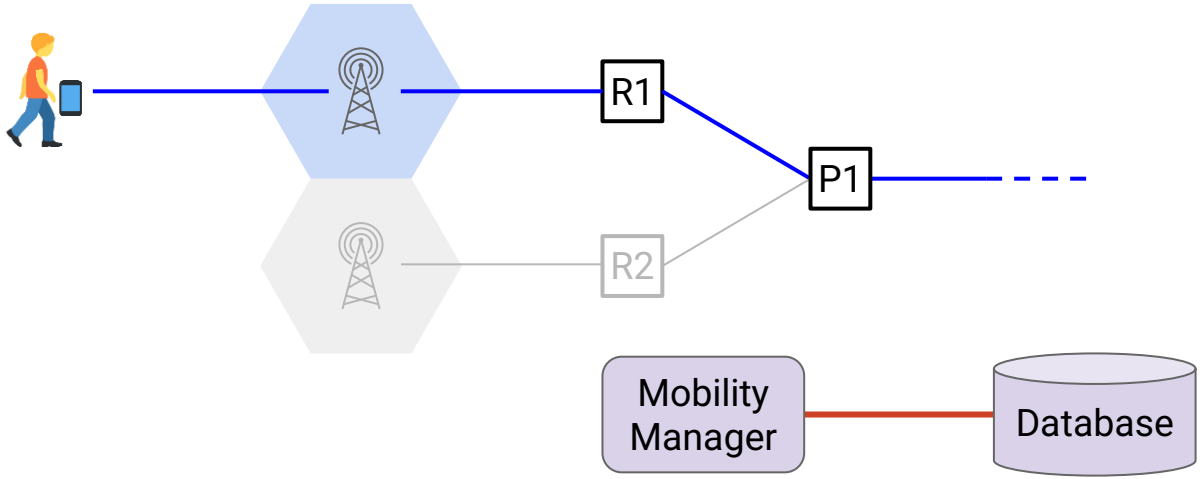
4. If request is approved, mobility manager configures the data plane.

- Assign an IP address to the user.
- Tell the tower how many resources to allocate for this user.
- Configure tower and routers to create a path from user to Internet.
- Initialize counters to track the device's usage.



5. If request is approved, mobility manager records information in the database, mapping the user's IMSI to their current:

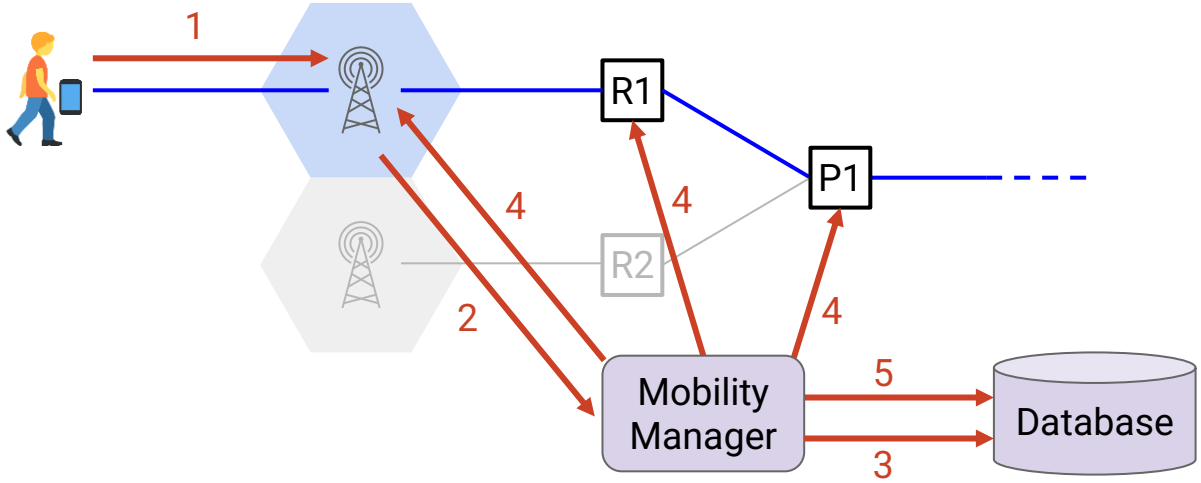
- Location (tower).
- Path to the Internet (radio gateway, packet gateway).
- IP address.



Step 2: Attachment

1. User sends attach request to tower, containing user's IMSI.
2. Tower forwards request to mobility manager.
3. Mobility manager processes the request, by looking up the IMSI in database.
4. If request is approved, mobility manager configures the data plane.
5. If request is approved, mobility manager records information in the database.

Note: All communication so far is over dedicated control channels.



Step 3: Data Exchange

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

Cellular Networks

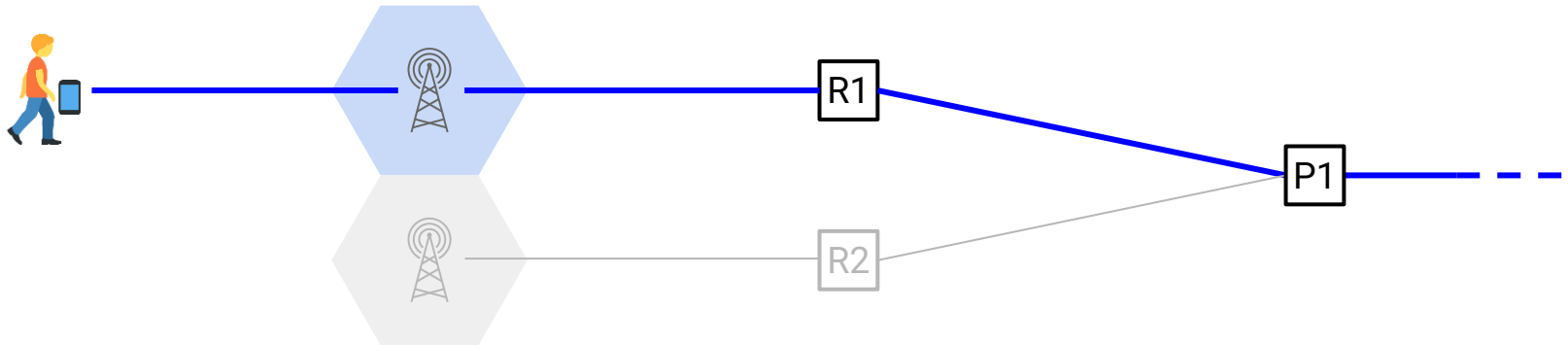
- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- **Step 3: Data Exchange**
- Step 4: Handover
- Roaming and Other Features

Step 3: Data Exchange

Device can now send and receive packets with its IP address!

How does the network know how to forward packets?

- Users are constantly moving.
- Traditional routing algorithms (Distance Vector, Link State) won't converge.

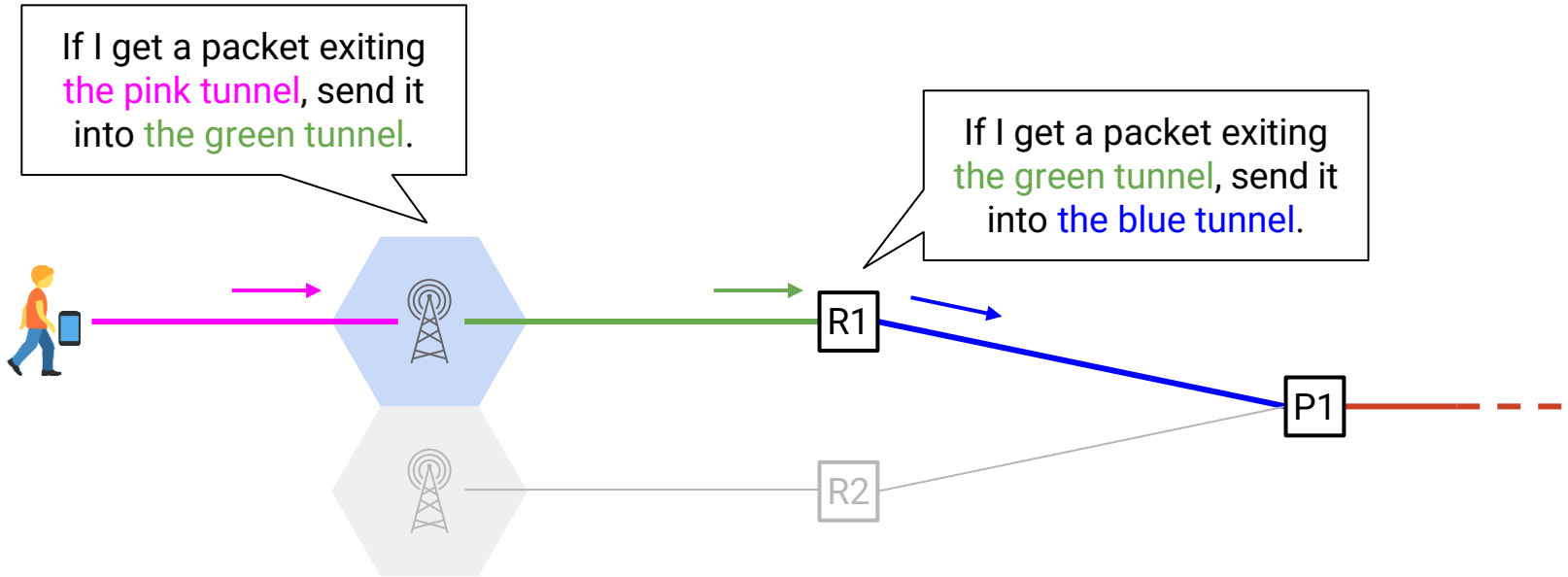


Step 3: Data Exchange with Tunnels

Solution: Mobility manager configures a path from user to Internet using **tunnels**.

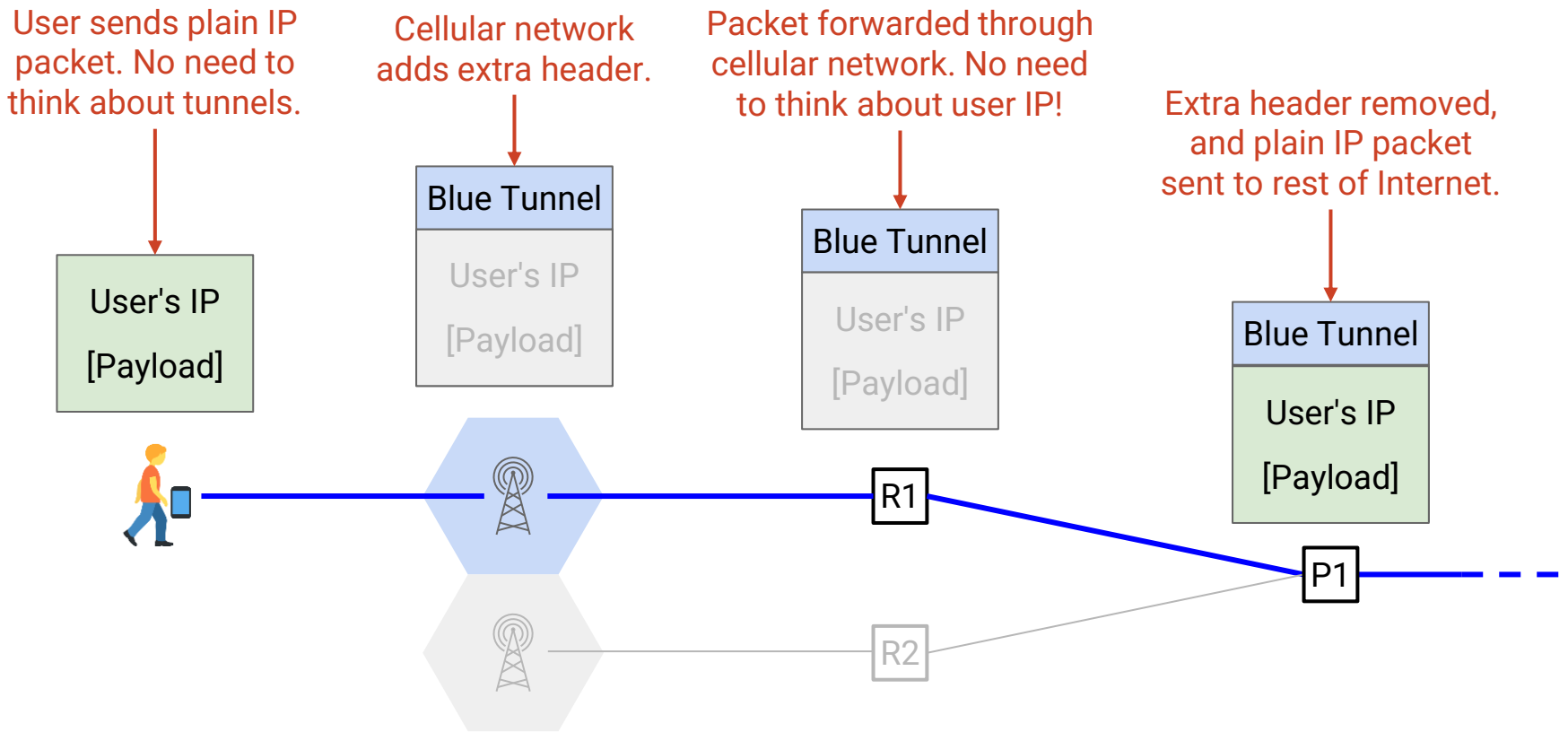
Different from traditional IP networks:

- No direct forwarding on the user's IP address!
- Requires installing per-user state in the network.



Step 3: Data Exchange with Tunnels

How do we tell if a packet is traveling through a tunnel? Use **encapsulation**.



Step 4: Handover

Lecture 25, Spring 2026

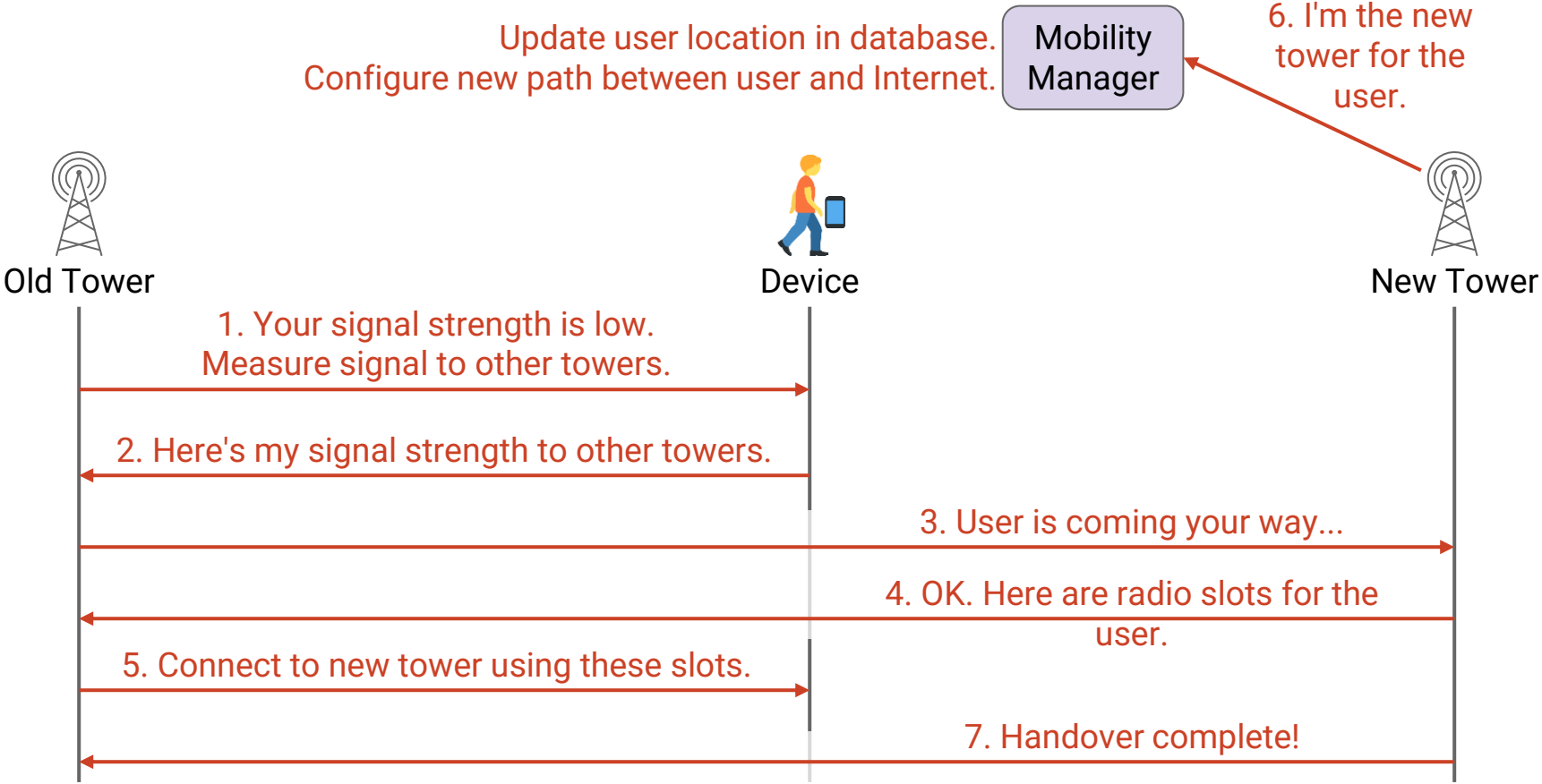
Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- **Step 4: Handover**
- Roaming and Other Features

Step 4: Handover



Step 4: Handover

Handover is complicated.

- Cooperative process between user, towers, manager, and gateways.
- More involved when we have to change the radio or packet gateways being used.

Handover must be seamless.

- User's IP address cannot change.
- User is still sending/receiving data during handover.
- Old tower can buffer data it receives during handover.
- After handover, old tower transfers buffer to new tower.

Decisions are made by the operator.

- Device reports signal strength, but old tower chooses the new tower.
- Benefit: Operator has more control, e.g. for load-balancing.
- Drawback: Slower, requires extra round-trips.

Roaming and Other Features

Lecture 25, Spring 2026

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

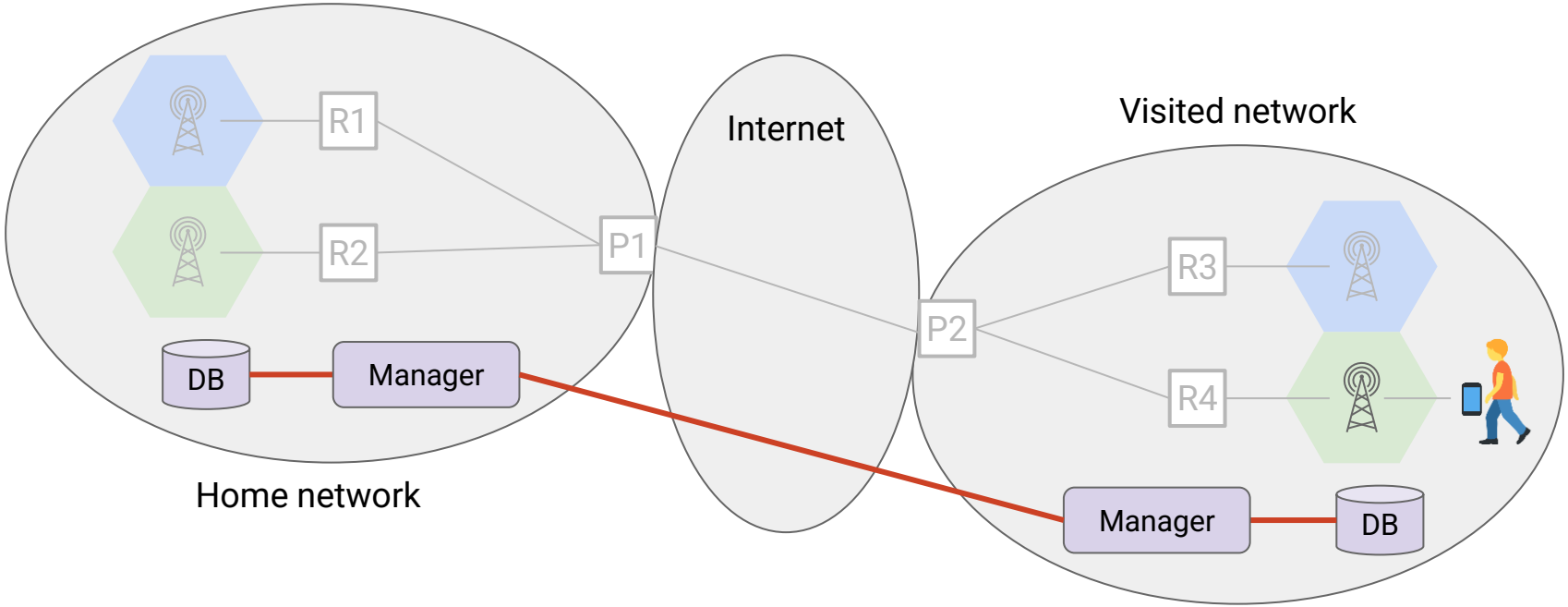
Cellular Networks

- Infrastructure
- High-Level View
- Step 0: Registration
- Step 1: Discovery
- Step 2: Attachment
- Step 3: Data Exchange
- Step 4: Handover
- **Roaming and Other Features**

Roaming

Visitor and home networks must establish a roaming agreement.

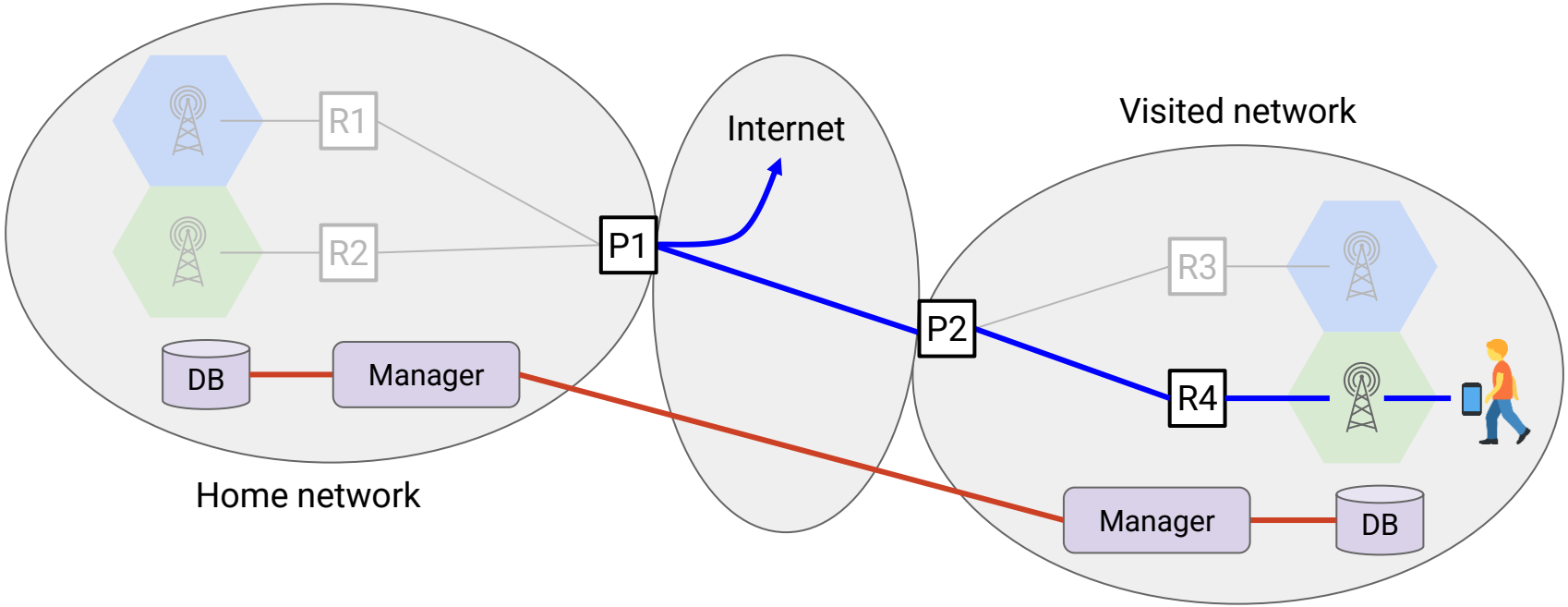
- Visited network uses device's network code (in IMSI) to learn the home network.
- Need home network's help to authenticate user.
- Need to update home network's database with user's location.



Roaming

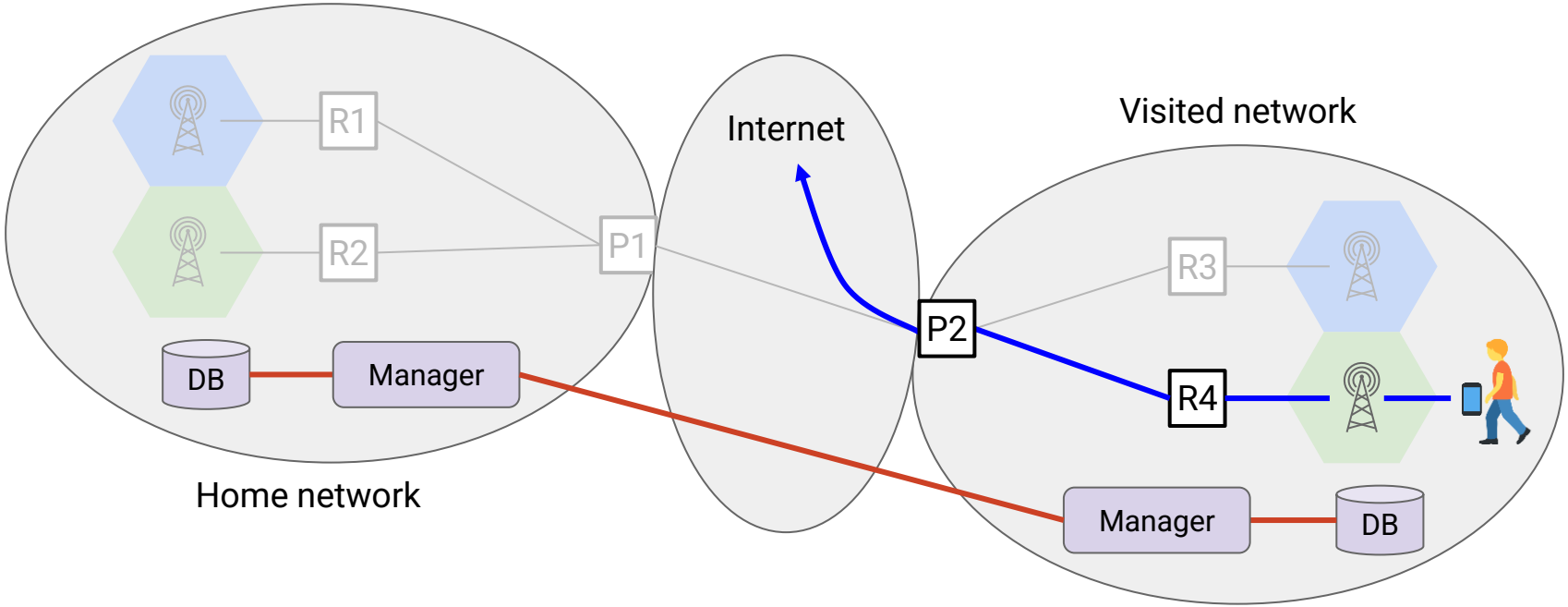
Two common ways to configure path from user to Internet.

- **Home routing**: Tunnel traffic through the **home** network's packet gateway.
- Benefit: Home network can track user.
- Drawback: Packets takes longer path to Internet.



Two common ways to configure path from user to Internet.

- **Local breakout**: Tunnel traffic through the **visitor** network's packet gateway.
- Drawback: Harder for home network to track user.
- Benefit: Packets takes shorter path to Internet.



Additional Operations

Other operations in cellular networks:

- **Lawful intercept**:
  - Allows law enforcement to wiretap specific subscribers.
  - Operators must be able to fulfill wiretap requests.
- **Stolen phone registries**:
  - Users can report their phone stolen.
  - If someone connects stolen phone to network, the phone can be tracked.
  - Use IMEI (burned into phone) to identify the stolen phone.

These operations are possible because of centralized control.

Design Reflections

Stateful networks are complex and challenging!

- Must store per-user state in the network.
- Must reconfigure tunnels each time the user moves.
- Requires extreme optimization to scale well.

Alternate designs:

- Tunnels.
  - Drawback: Must store per-user state for routing.
  - Benefit: Can use standard routing protocols.
- Change IPs on handover:
  - Benefit: Can use standard routing protocols.
  - Drawback: TCP connections break when IPs change.

Possible solution: QUIC is an alternate Layer 4 protocol that allows changing IPs.

Summary: Cellular

Cellular networks are based on a very different design philosophy:

- Authentication and accountability are primary goals.
- Allocation of radio bandwidth is based on reservations.
- Lots of in-network state that is dynamic and per-user.
- Generality was not an early goal.
- Mobility is the central challenge.

Cellular networks have evolved from a standalone voice network, to being an integral part of the Internet.

- We've been able to seamlessly integrate cellular networks into the Internet.
- Cellular architecture continues to evolve toward the Internet architecture.