Lecture 27

Cellular Networks

CS 168, Fall 2024 @ UC Berkeley

Why Study Cellular?

- **The de facto access technology for <u>mobile</u> users/devices**
  - 5B+ users
  - Over 50% of web traffic originates from a cellular device!

Why Study Cellular?

- **The de facto access technology for <u>mobile</u> users/devices**
  - 5B+ users
  - Over 50% of web traffic originates from a cellular device!
- **Little doubt that mobile wireless access is the future**
  - Cellular currently the dominant technology, though other options exist (WiFi, satellite)

Why Study Cellular?

- **The de facto access technology for <u>mobile</u> users/devices**
  - 5B+ users
  - Over 50% of web traffic originates from a cellular device!
- **Little doubt that mobile wireless access is the future**
  - Cellular currently the dominant technology, though other options exist (WiFi, satellite)
- **Cellular operators now facing severe scaling challenges!**
  - New bandwidth-intensive mobile apps: AR/VR, self-driving cars, IoT, *etc.*
  - Deploying towers and buying spectrum is an expensive undertaking
  - Traditional telcos (at&t, verizon) don't have a reputation for rapid innovation
  - General consensus that this is an area ripe for disruption

Outline

- **Why is cellular different?**
  - Brief history
  - Standards
  - Challenge: mobility
- **How cellular networks work**
  - Infrastructure
  - Overview
  - Operation in detail

Brief History of Cellular Networks

Why is Cellular Different?

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

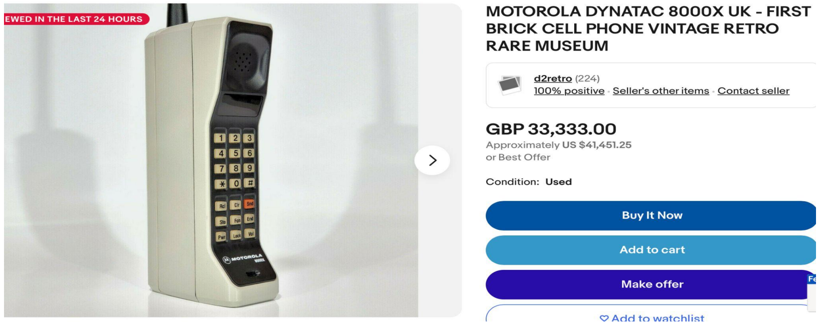
Cellular Networks

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

History

- **Derived from the old telephone network**
  - NTT in 1979 supports voice calls for users in Tokyo (1G)
  - In 1983, Motorola sells first mobile phone in US for ~$4k ($12k today)

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



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

History

- **Derived from the old telephone network**

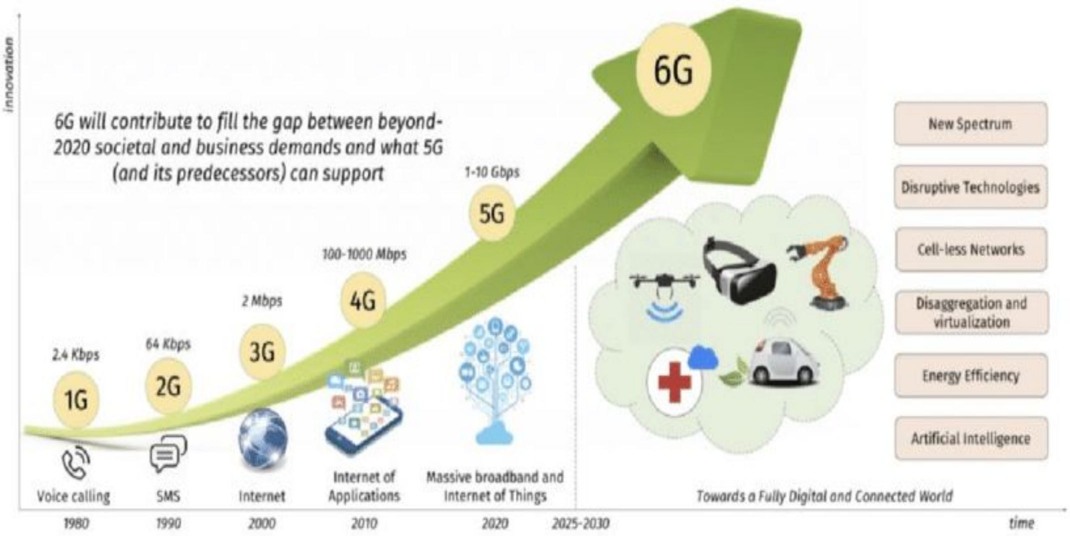
- These roots lead to architectural choices that differ from the Internet
  - Billing and authentication are central goals, voice calls as target app, *etc.*

- Early cellular networks did not rely on Internet technologies
  - Didn't use IP addresses, routing protocols, BGP peering, *etc.*

- Today, can think of cellular networks as L2 networks within the Internet
  - Internals of cellular networks are evolving to embrace (TCP/IP) Internet concepts

Standards

- The 3GPP (3rd Generation Partnership Project) consortium oversees standardization efforts
- 3GPP standard ratified by the ITU (International Telecom Union), part of the United Nations!
- Typically, a new technology generation ("G") introduced every 10 years

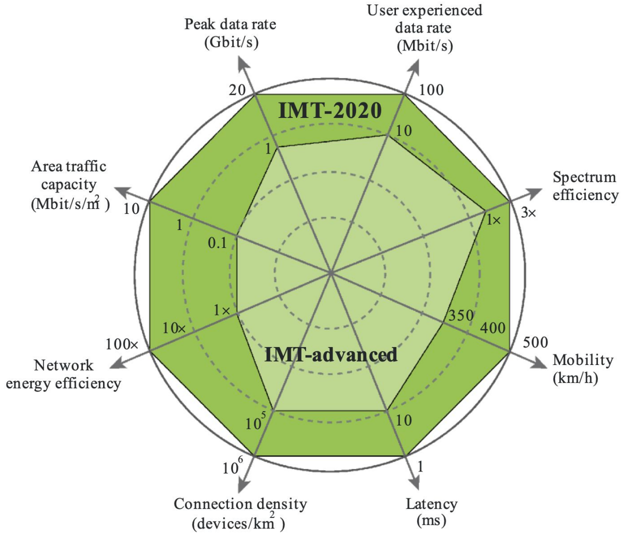


Marketing view

Standards

- The 3GPP (3rd Generation Partnership Project) consortium oversees standardization efforts
- 3GPP standard ratified by the ITU (International Telecom Union), part of the United Nations!
- Typically, a new technology generation ("G") introduced every 10 years

Enhancement of key capabilities from IMT-Advanced to IMT-2020



[ITU view]

Light green = 4G quality along 8 different dimensions.

Dark green = 5G quality along those same dimensions.

Standards

- The 3GPP (3rd Generation Partnership Project) consortium oversees standardization efforts
- 3GPP standard ratified by the ITU (International Telecom Union), part of the United Nations!
- Typically, a new technology generation ("G") introduced every 10 years

- Each generation achieves better performance and efficiency

Standards

- The 3GPP (3rd Generation Partnership Project) consortium oversees standardization efforts
- 3GPP standard ratified by the ITU (International Telecom Union), part of the United Nations!
- Typically, a new technology generation ("G") introduced every 10 years

- Each generation achieves better performance and efficiency

- Also significant architectural evolution, from a voice to data network
    - 1G: analog phones
    - 2G/3G: mostly circuit switched; focus still on voice traffic (i.e., still not a *data* network)
    - LTE/4G onwards: packet switched; voice just another app

Note

- Reading a cellular specification is not for the faint of heart!
    - 100s of documents, 1000s of pages, obscure naming conventions, and endless acronyms
    - To make matters worse, components/protocols are renamed in every generation!
    - E.g., Base station → NodeB → evolved Node B (eNodeB) → next-gen Node B (gNB)

- In this class, we will exercise poetic license and invent our own terminology
    - Loosely based on the LTE architecture

- Conceptually correct but not a 1:1 match to textbooks, standards, *etc.*

Challenge: Mobility

Mobility

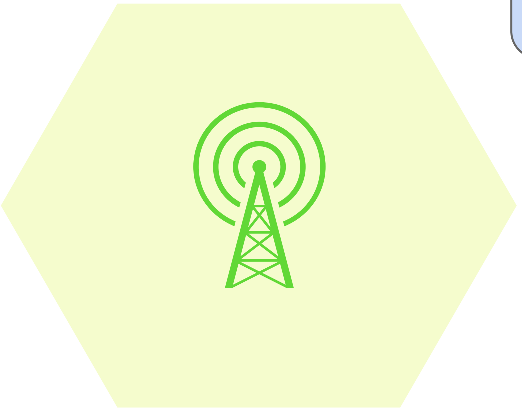
- **What fundamental new requirements does mobility introduce?**

Mobility

- **What fundamental new requirements does mobility introduce?**
  1. Discovery: what cell tower should a mobile device connect to?
  2. Authentication: should the tower provide service to this device?
  3. *Seamless* communication: no disruption to new/ongoing app sessions
  4. Accountability: enforcing resource limits based on the user's service plan

Cellular Infrastructure

Infrastructure Components (1/5): Radio Towers



Radio Tower
(*a.k.a Base Station, eNodeB, gNB, …*)

Converts between data and signals sent over the *air interface*

Decides how to allocate radio resources

Radio Transceiver

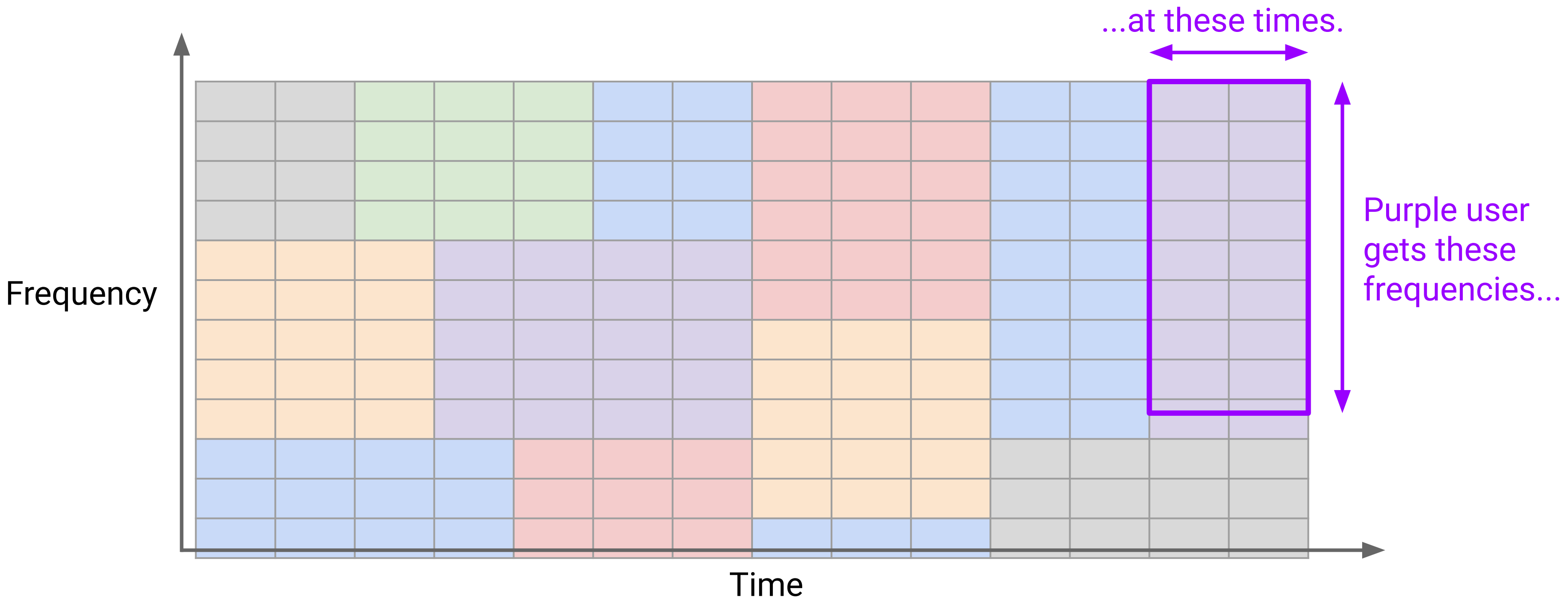
Radio Controller

Key internal components

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 (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.

Different from the media access protocols we discussed in the last lecture!

- CSMA/MACA/MACAW/etc - devices cooperatively figuring out when to send
- Cellular: all decisions made by the radio controller

A Note on Radio Frequencies in Cellular vs. WiFi Networks

- Frequency *spectrum:* range of frequencies over which a technology operates

- Cellular typically operates on licensed spectrum
  - Regulatory authorities (e.g., FCC in the US) controls use of these frequencies
  - Operators must pay for the right to use these frequencies

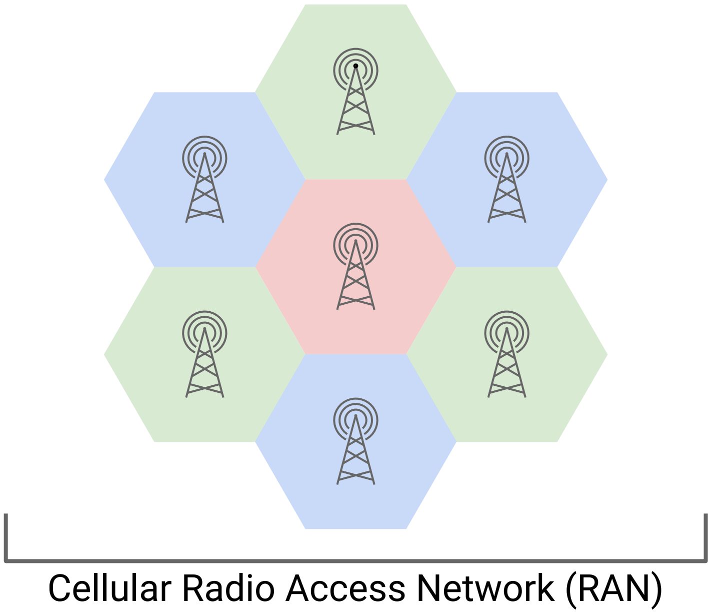
- WiFi operates on unlicensed spectrum

- One of the reasons cellular technology is typically more expensive than WiFi

Infrastructure Components: Radio Access Network

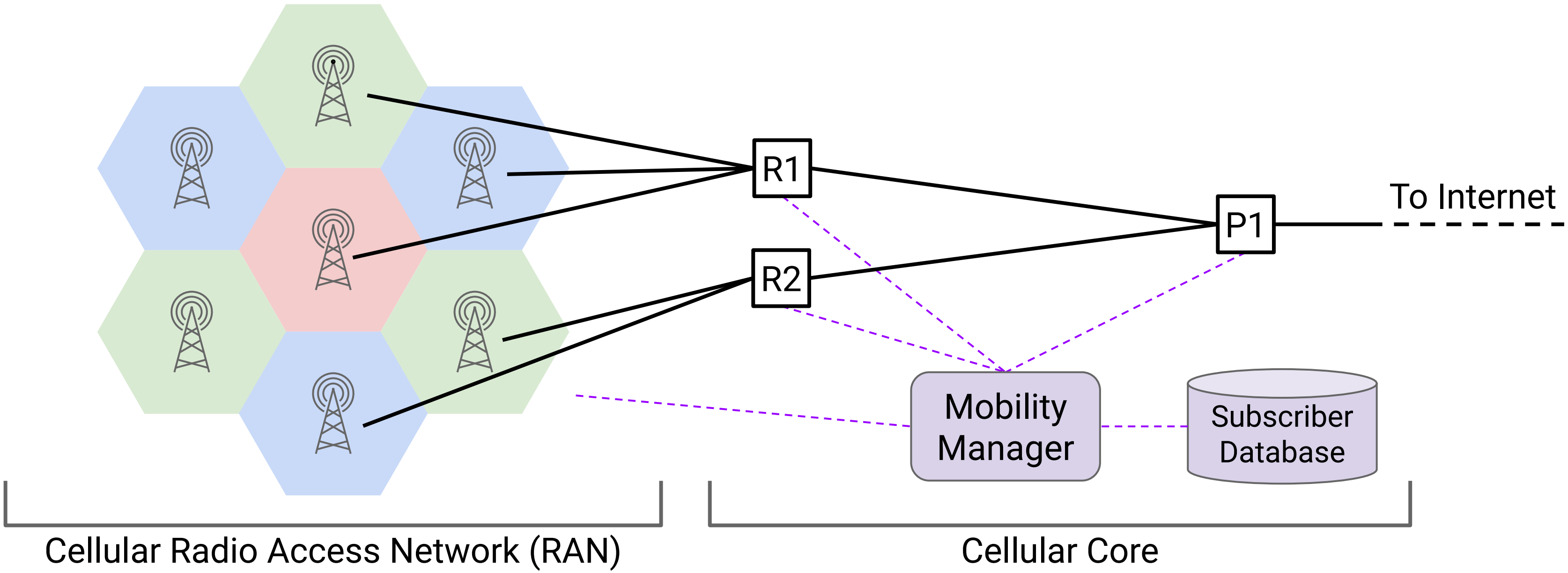
Each operator has a **radio access network (RAN)** of many towers.

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



Infrastructure Components: Cellular Core

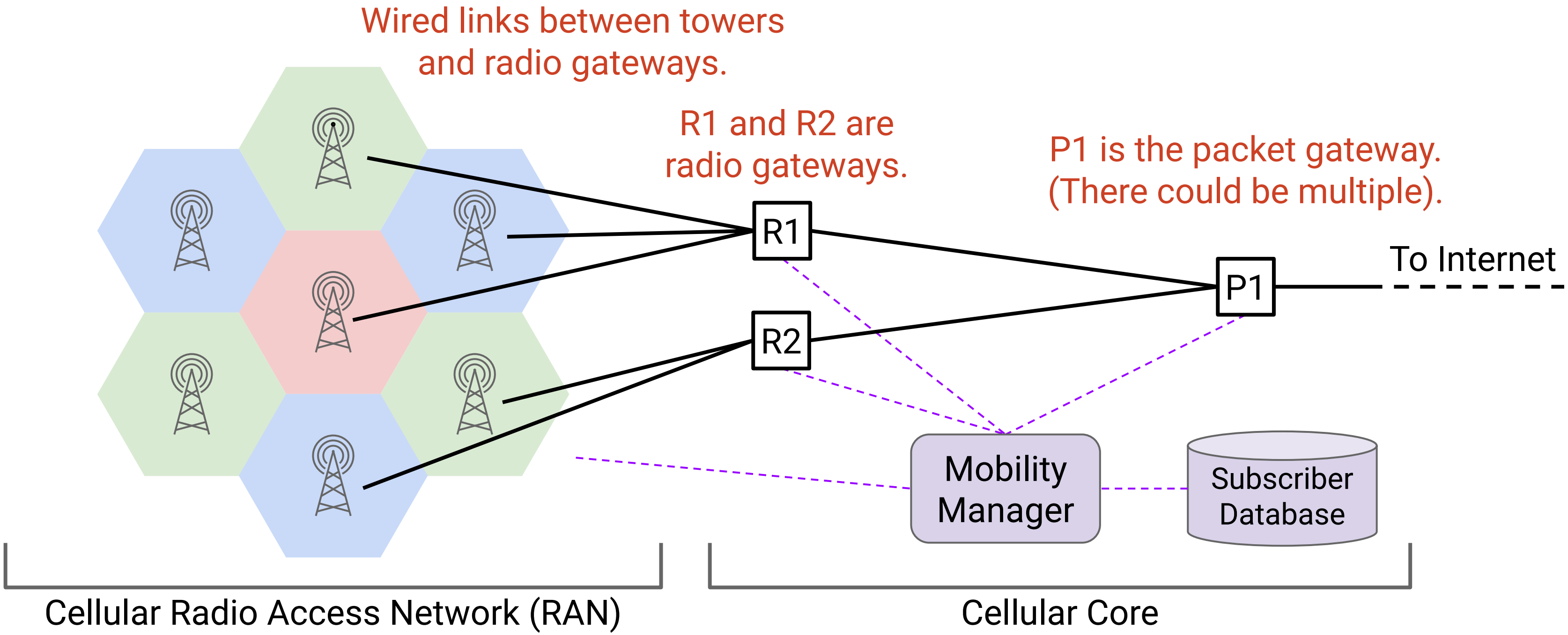
The **cellular core** is the "backend" of the cellular network.



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

Data-plane components (forward users' data traffic):

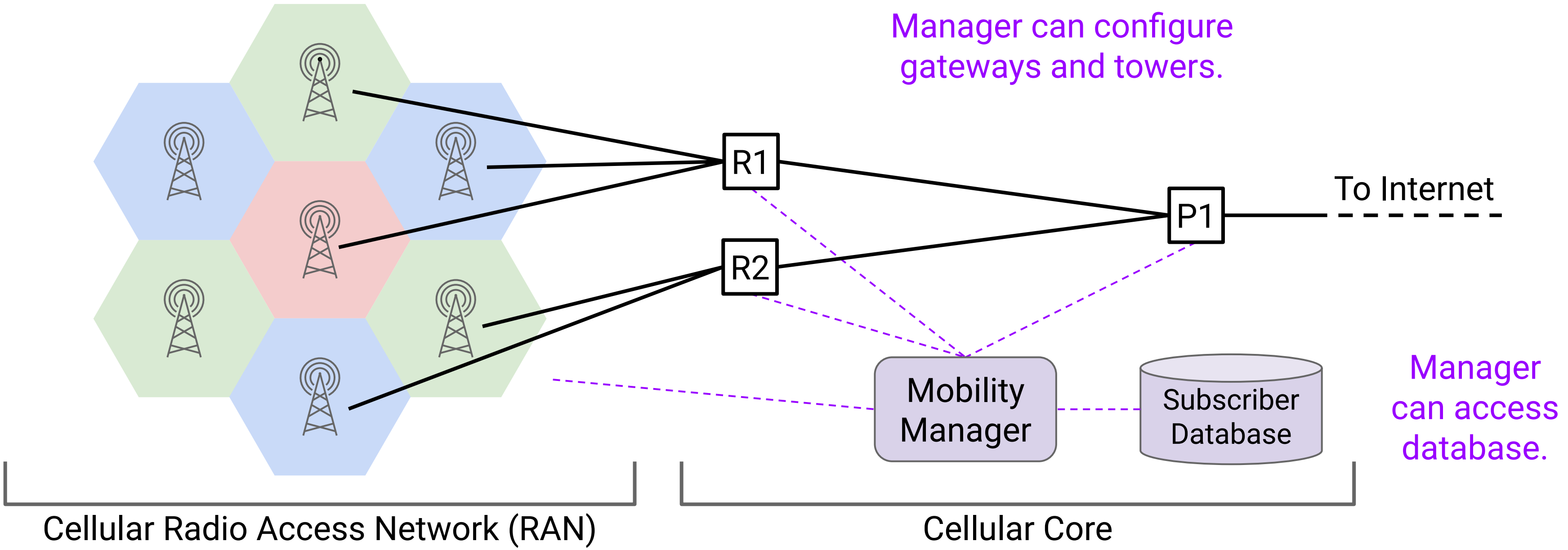
- **Radio gateway**: Boundary between RAN and core.
- **Packet gateway**: Boundary between cellular network and rest of Internet.



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

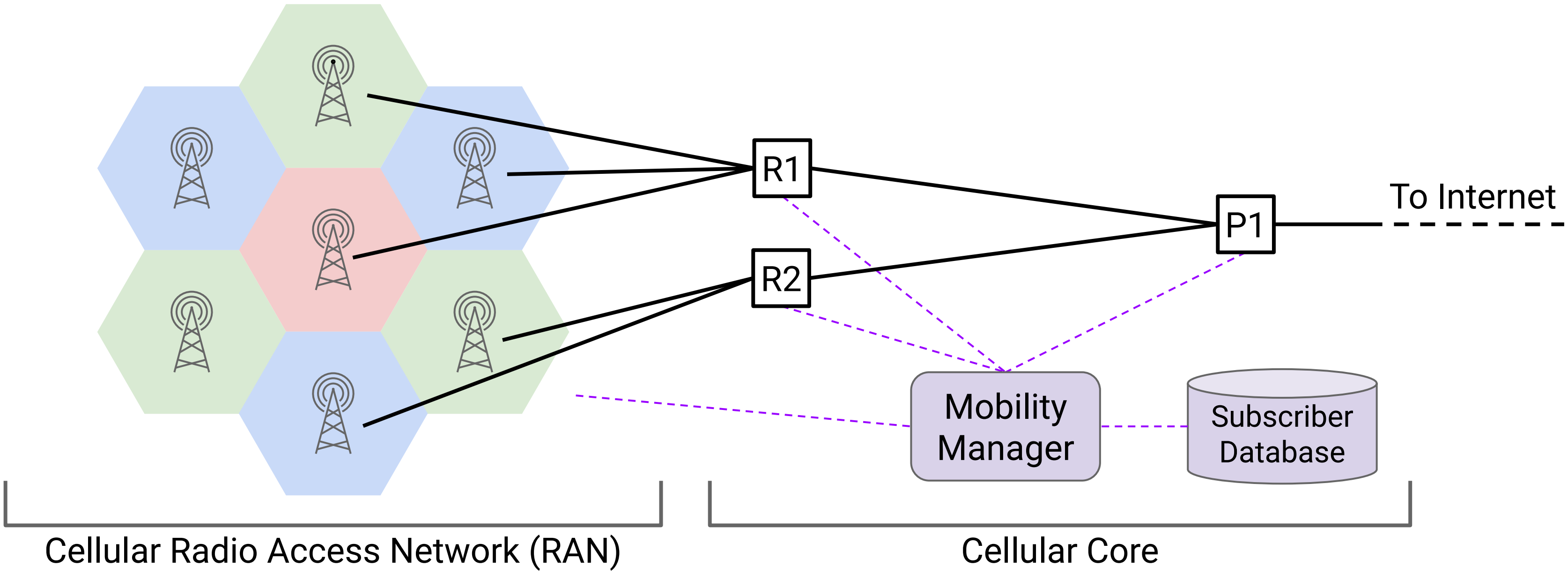
Control-plane components:

- **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, Subscriber database.



High-Level View

Why is Cellular Different?

- Brief History
- Standards
- Challenge: Mobility

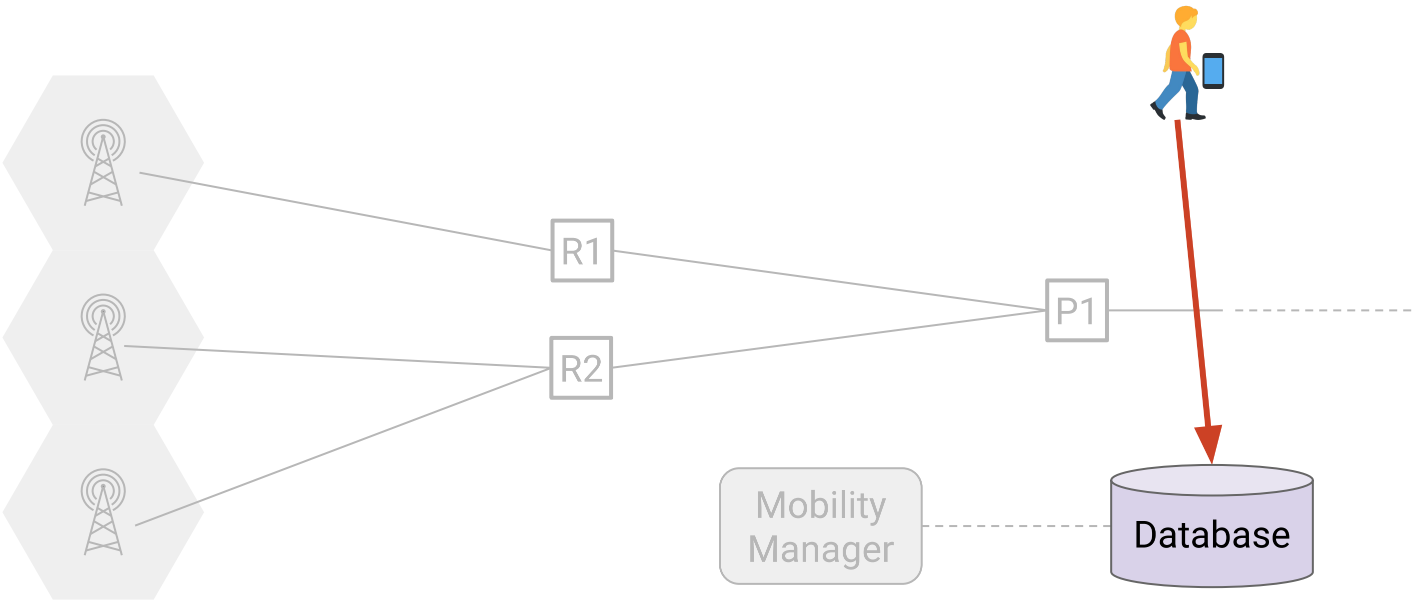
Cellular Networks

- 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**.

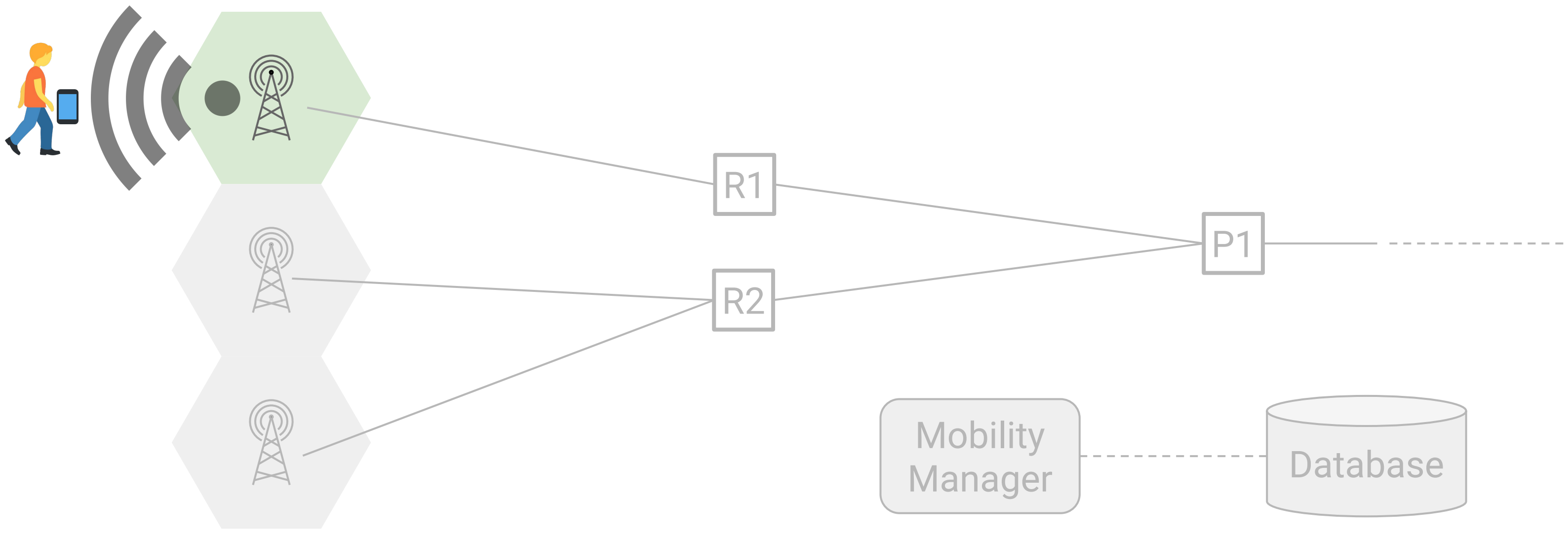
- User registers for the service. Database is updated.



High-Level View (1/4) – Discovery

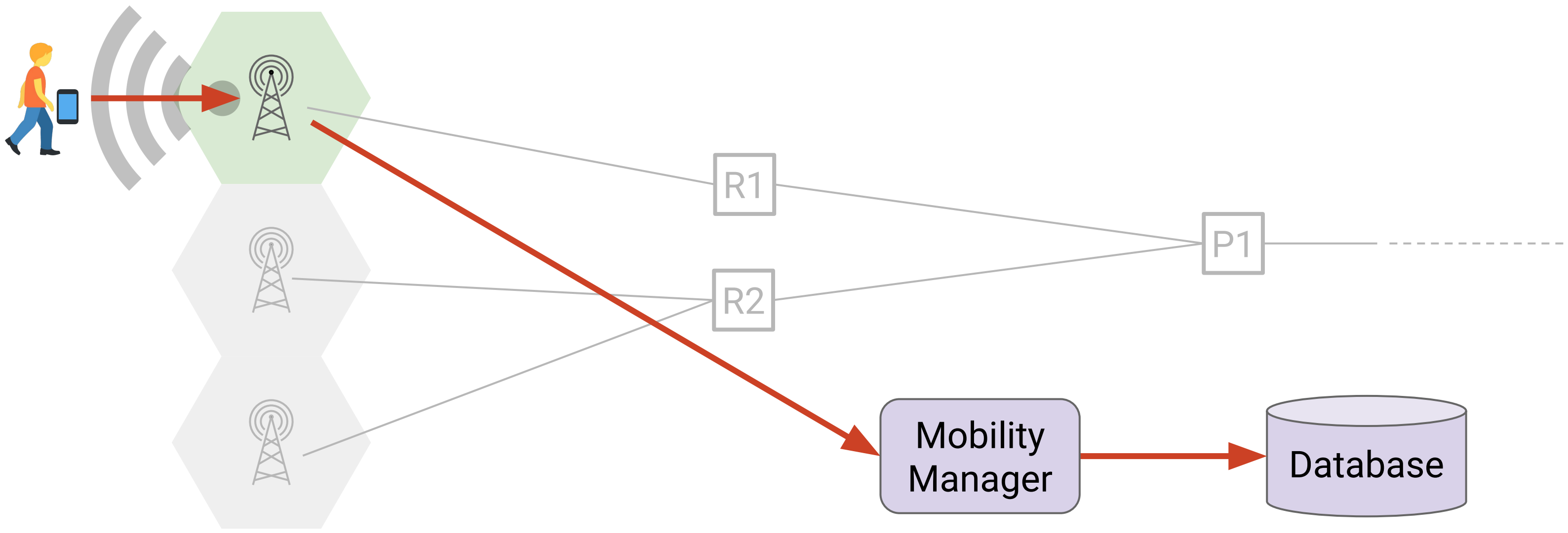
Step 1: **Discovery**.

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



Step 2: **Attachment**.

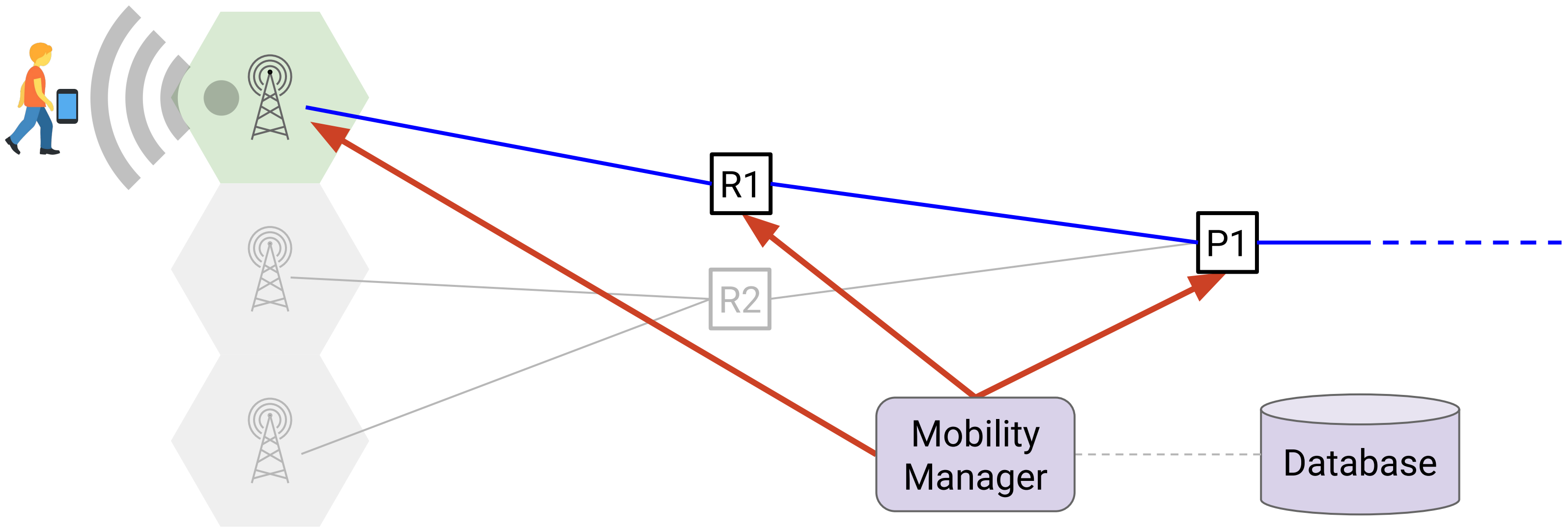
- Device asks the tower to connect.
- Tower checks with mobility manager if connection is allowed.



High-Level View (2/4) – Attachment

Step 2: **Attachment**.

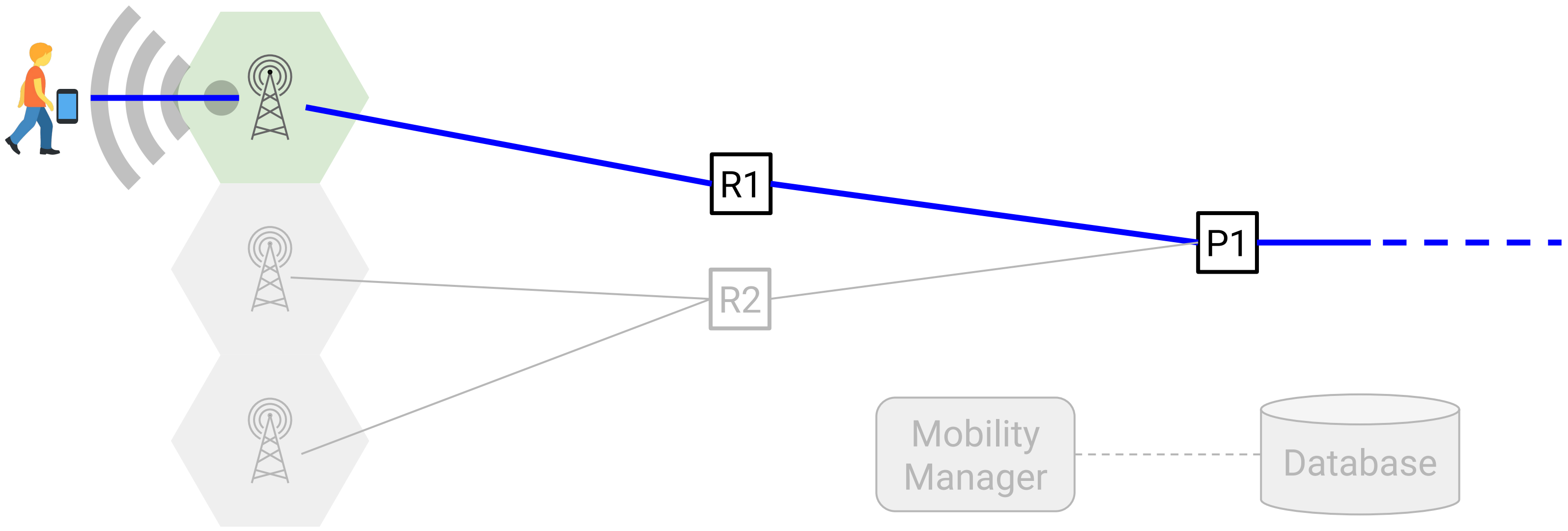
- If manager approves request, it configures a path between user and Internet.



High-Level View (3/4) – Data Exchange

Step 3: **Data exchange**.

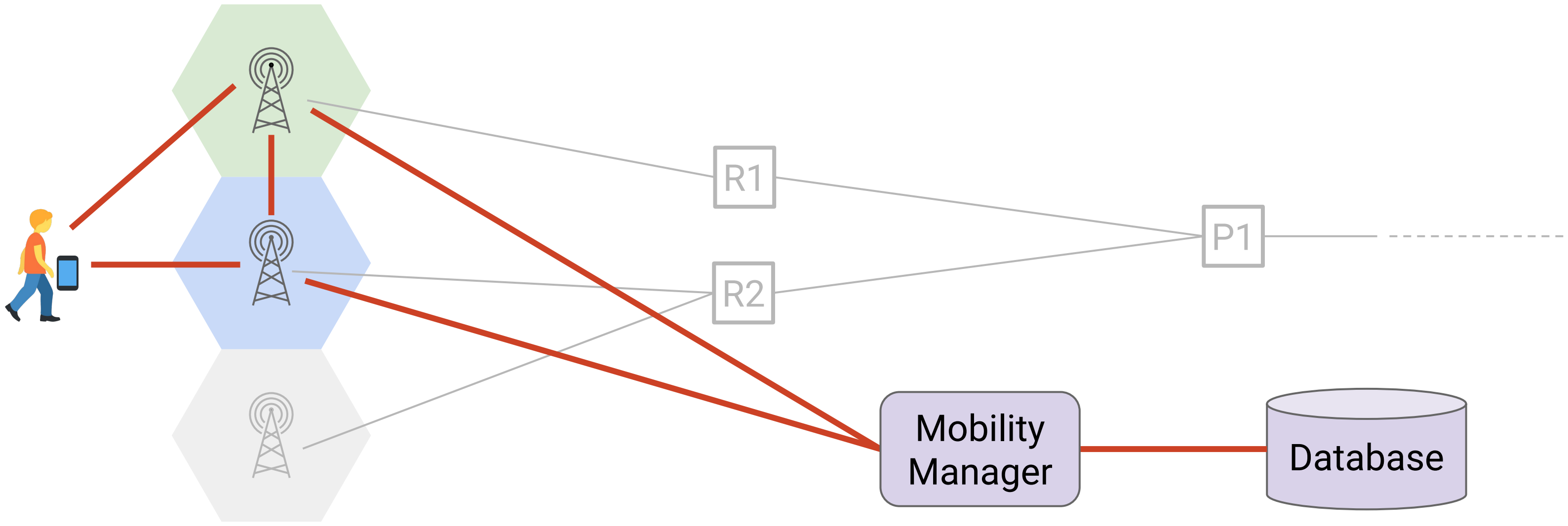
- User can now send and receive data!
- Packets travel along the path configured in previous step.



High-Level View (4/4) – Handover

Step 4: **Handover**.

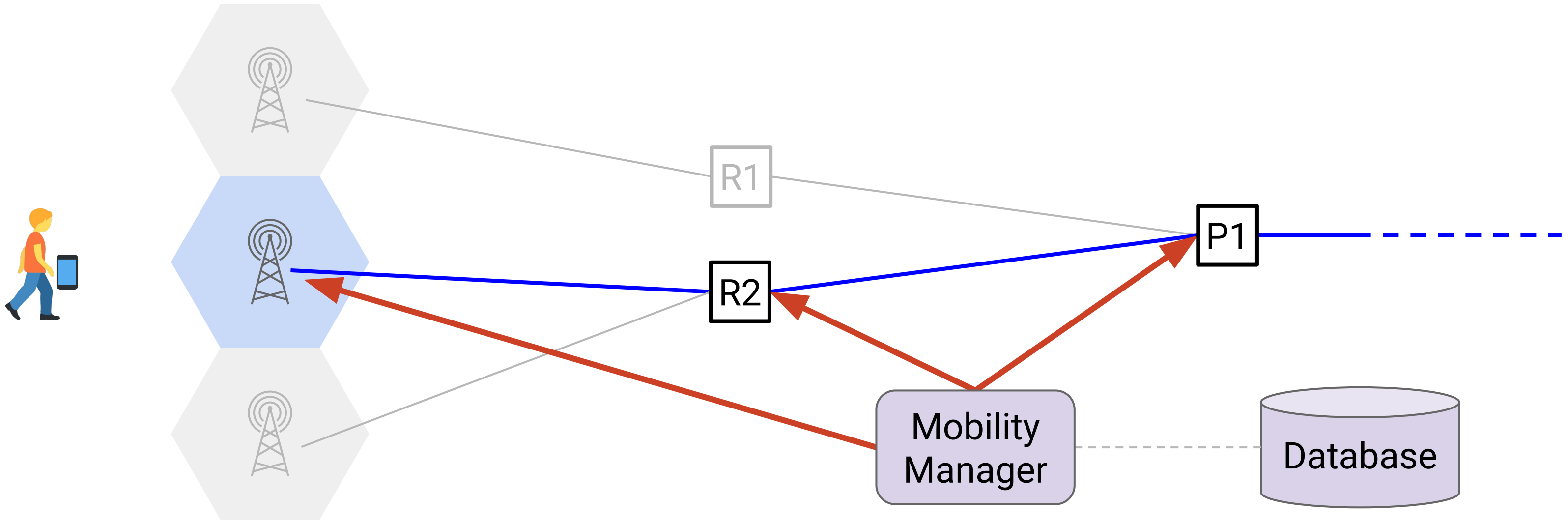
- Device might move away from old tower, closer to a new tower.
- Device, old tower, new tower, and manager work together to switch towers.



High-Level View (4/4) – Handover

Step 4: **Handover**.

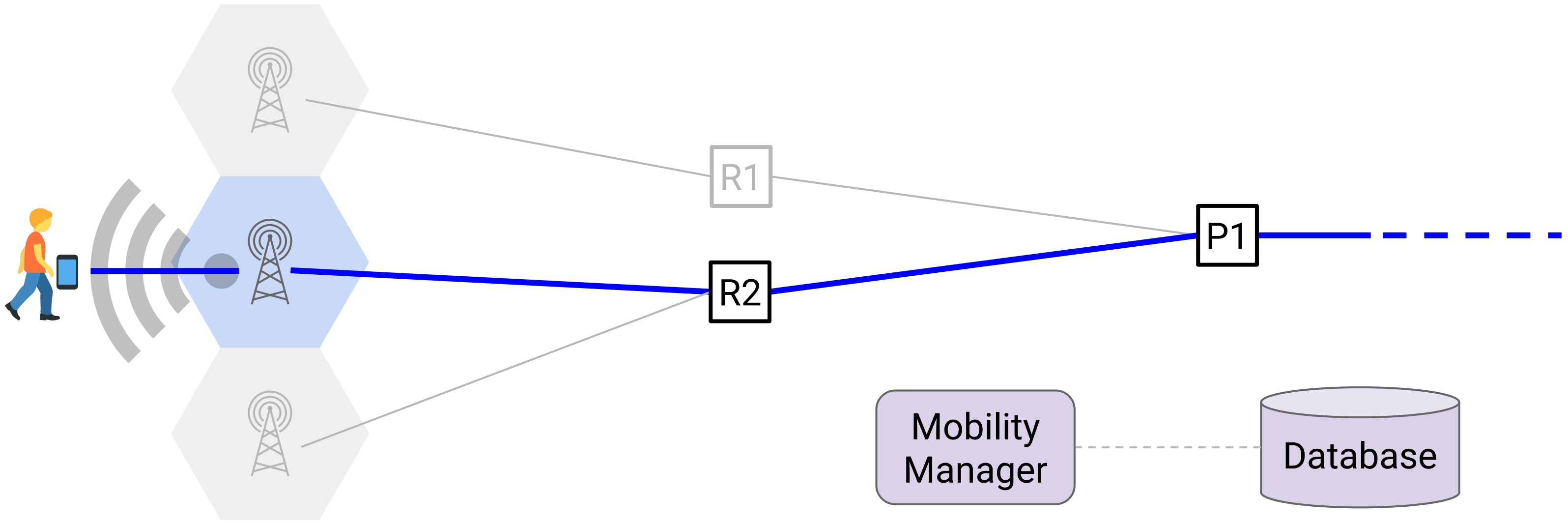
- Manager configures a new path through the network for the user.
- Handover must be seamless. We can't interrupt the user's connection!
    - User's IP address must stay the same *(why?)*



High-Level View (4/4) – Handover

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

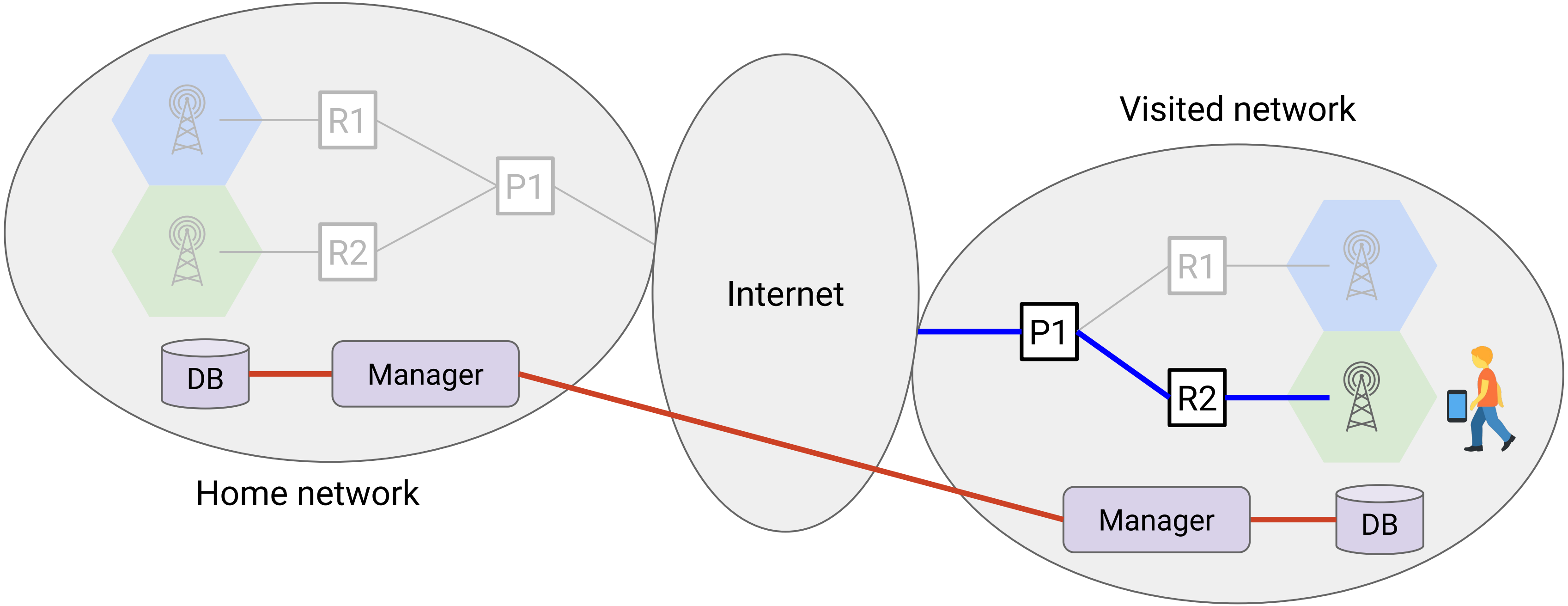
Step 3 (Data Exchange) and Step 4 (Handover) repeat as the user moves around.



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.

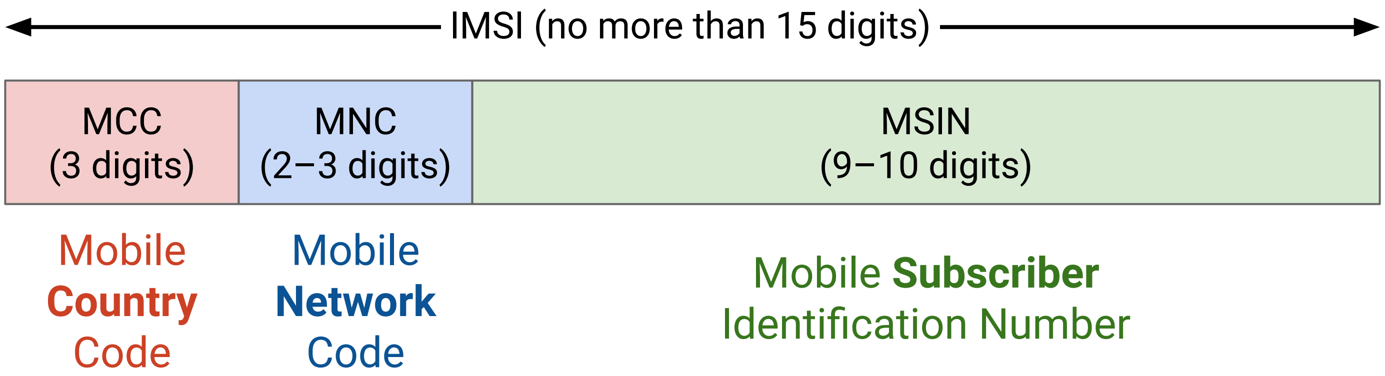


Step 0: Registration

Identifiers: 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



Additional identifiers: IP, IMEI, MSISDN

- **IMSI**: Identifies a user subscription.

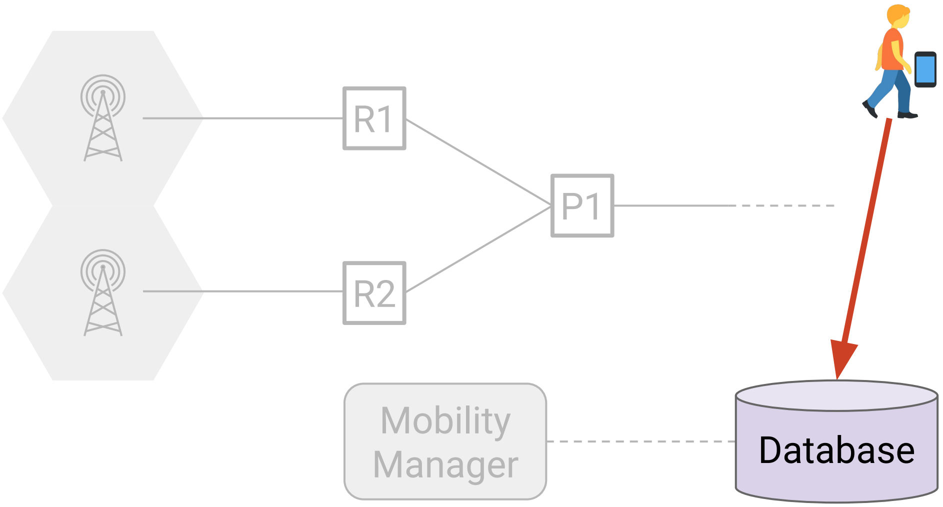
- **IP address**: Assigned to device on attachment, typically retained across handovers
    - Can change each time you attach to the network.

- **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 Subscriber database.



Step 1: Discovery

Step 1: Discovery

Towers transmit periodic *beacons* to announce their presence.

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

Step 1: Discovery

Towers transmit periodic *beacons* to announce their presence.

- Beacons transmitted on a dedicated control channel from tower’s frequency range
  - Avoids beacons interfering with each other
  - Avoids interfering with data
- 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 (10s - 100s)
- Optimization: at registration, pre-configure device with list of frequency channels
- Optimization: Cache previously-used channels.

Discovery: Finding Control Channel

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

- Scan all frequencies.
  - Slow, but sometimes unavoidable (10s - 100s)
- Optimization: at registration, pre-configure device with list of frequency channels
- Optimization: Cache previously-used channels.

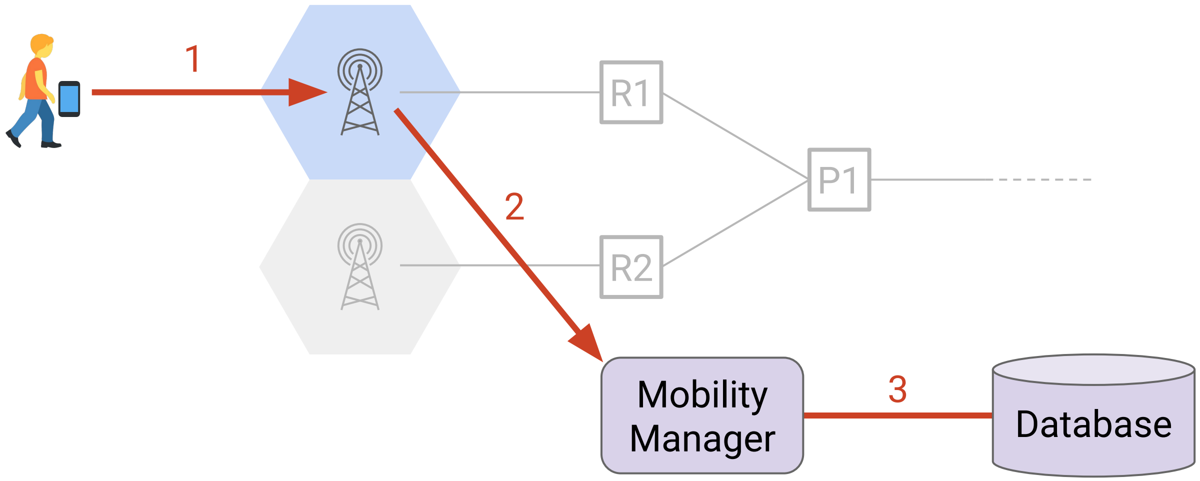
Note: During handovers, the old tower tells the user the channel on the new tower.

- No need to scan! Handovers take 0.01s–0.1s

Step 2: Attachment

Step 2: Attachment

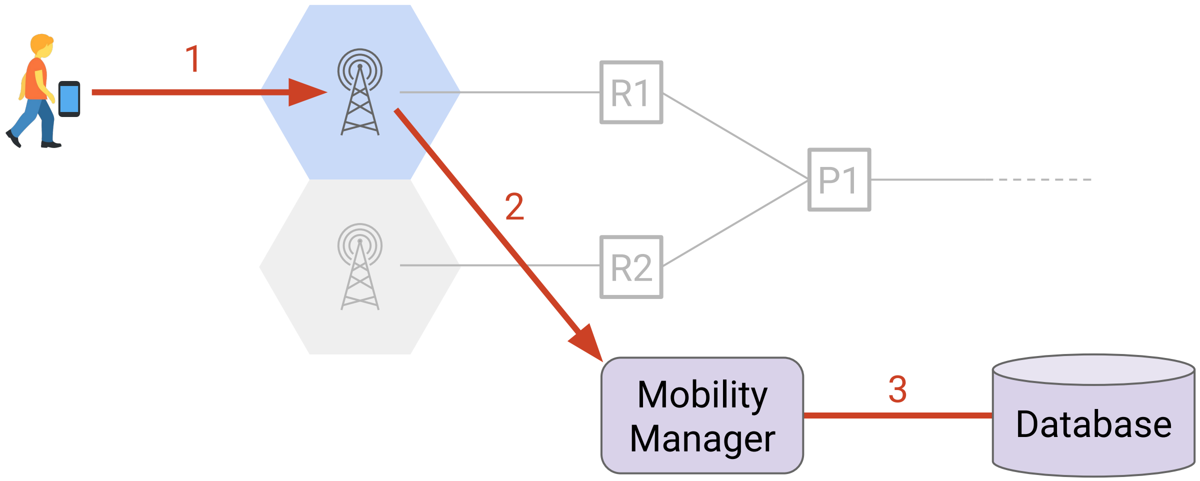
1. User sends attach request to tower, containing user's IMSI.
2. Tower forwards request to mobility manager.
3. Mobility manager processes the request, by looking up the IMSI in database.



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.

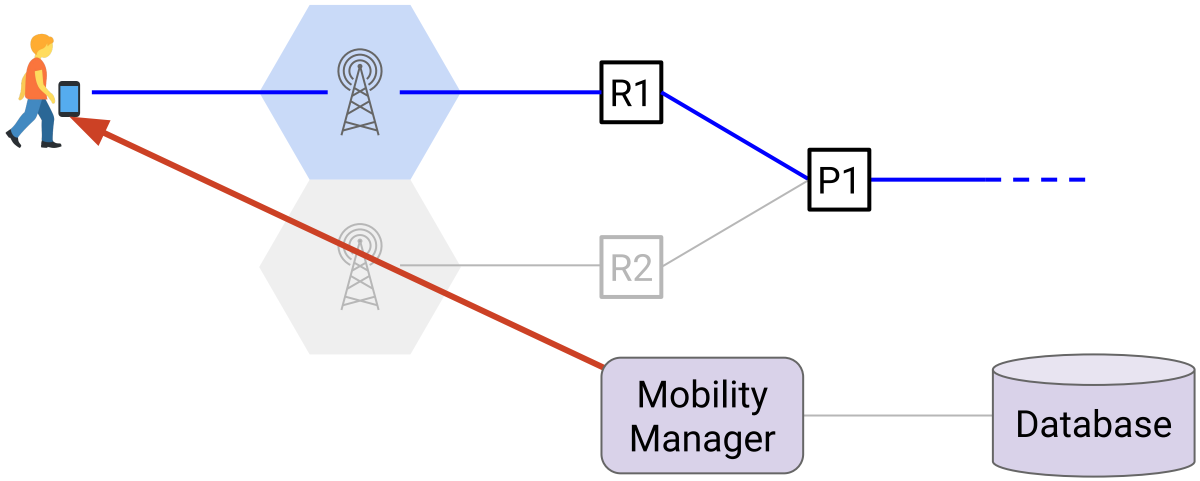
- Use secret key to authenticate: Is the user who they claim to be?
- Check service parameters: how many minutes/bytes left in this billing cycle?



Step 2: Attachment

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

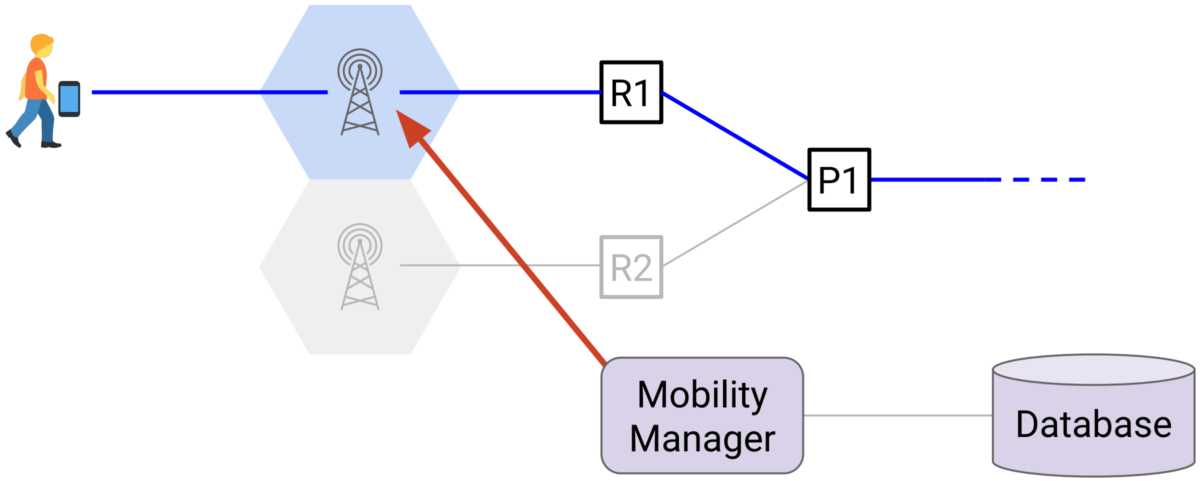
- Assign an IP address to the user.



Step 2: Attachment

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

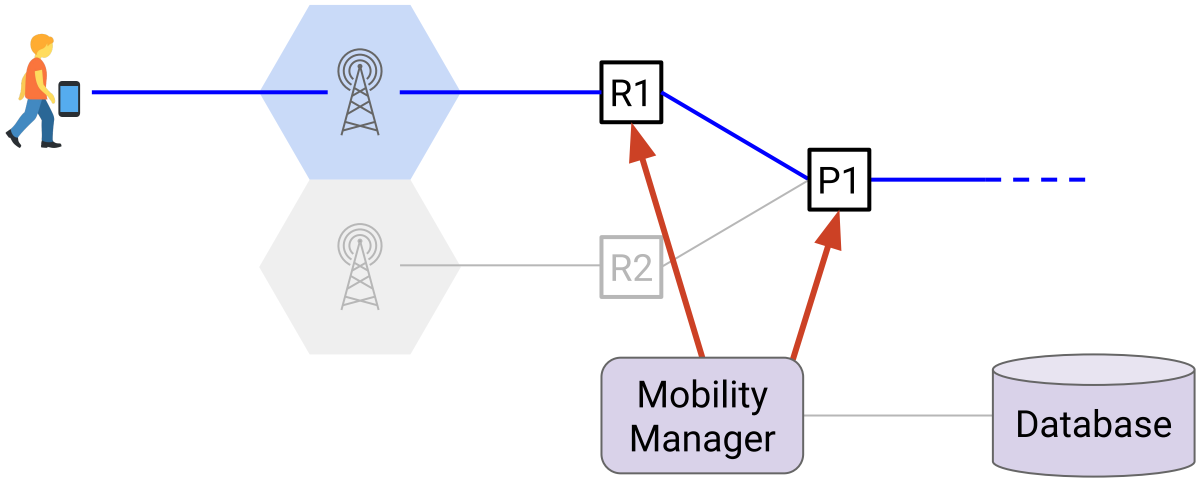
- Assign an IP address to the user.
- Tell the tower how many resources to allocate for this user.



Step 2: Attachment

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

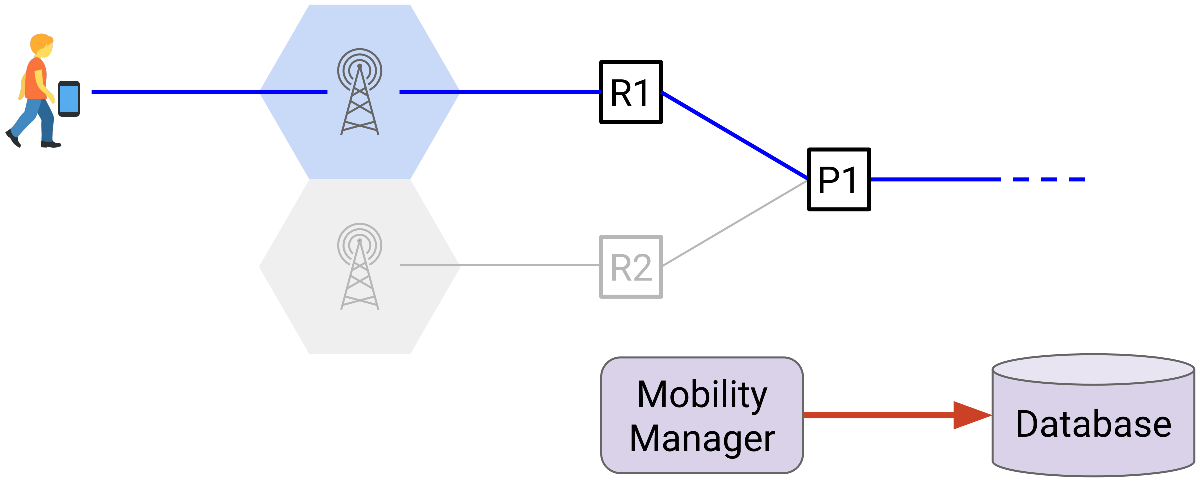
- Assign an IP address to the user.
- Tell the tower how many resources to allocate for this user.
- Configure tower and routers to create a path from user to Internet.
- Initialize counters to track the device's usage.



Step 2: Attachment

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

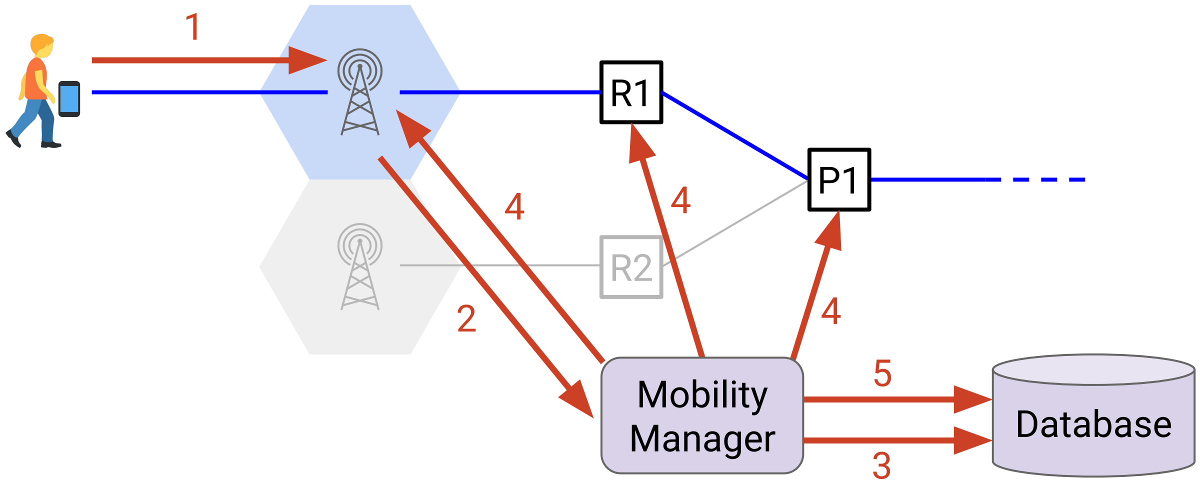
- Location (tower).
- Path to the Internet (radio gateway, packet gateway).
- IP address.



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 on the control plane and the radio control channel



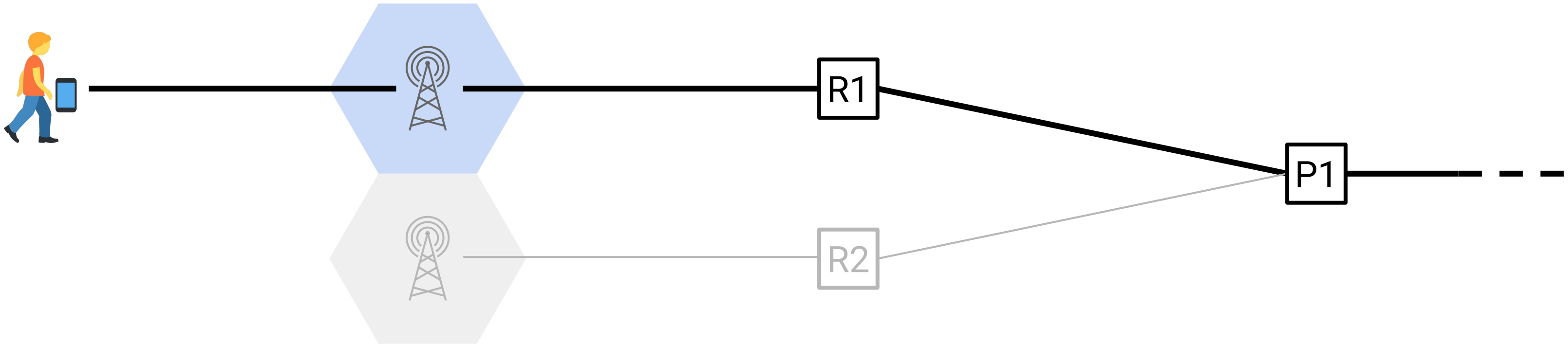
Step 3: Data Exchange

Step 3: Data Exchange

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

How does the network know how to forward packets?

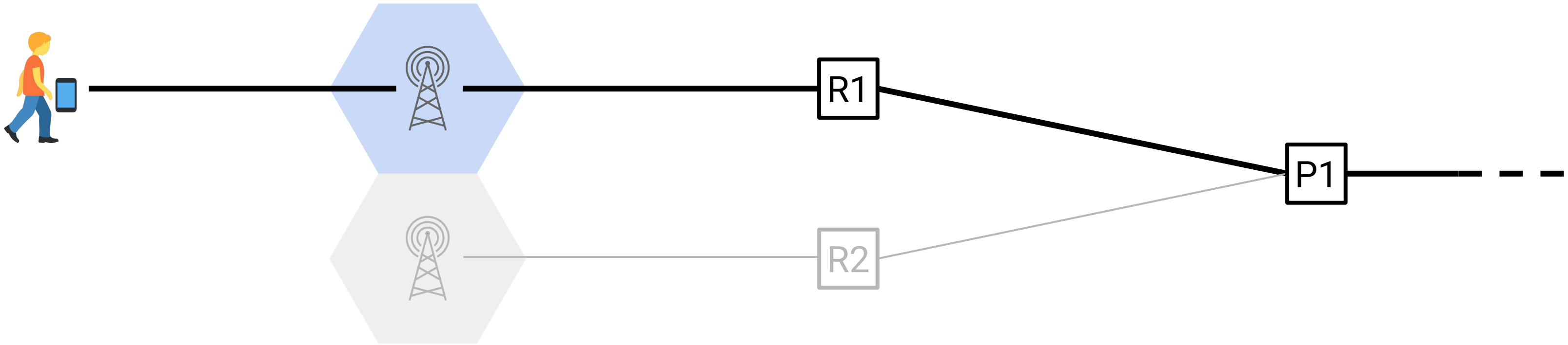
- Users are constantly moving
- Traditional routing algorithms won't converge *(why?)*



Step 3: Data Exchange with Tunnels

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

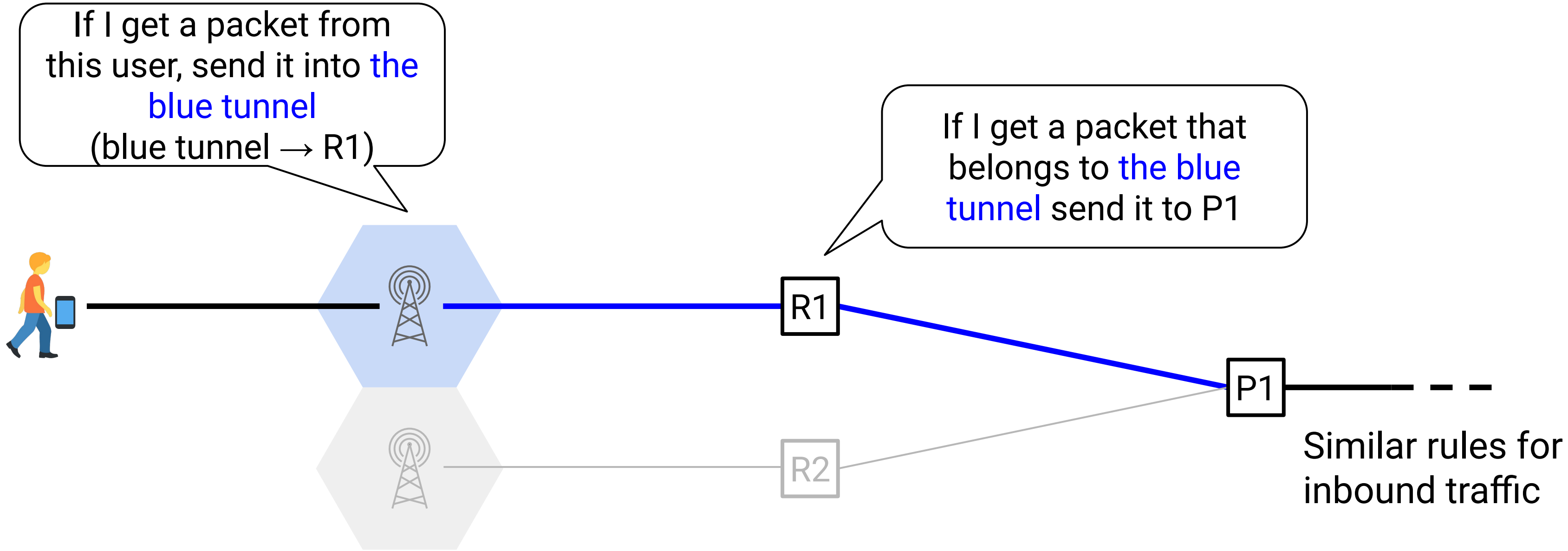
- No direct forwarding on the user's IP address!
- Requires installing per-user state in the network.



Step 3: Data Exchange with Tunnels

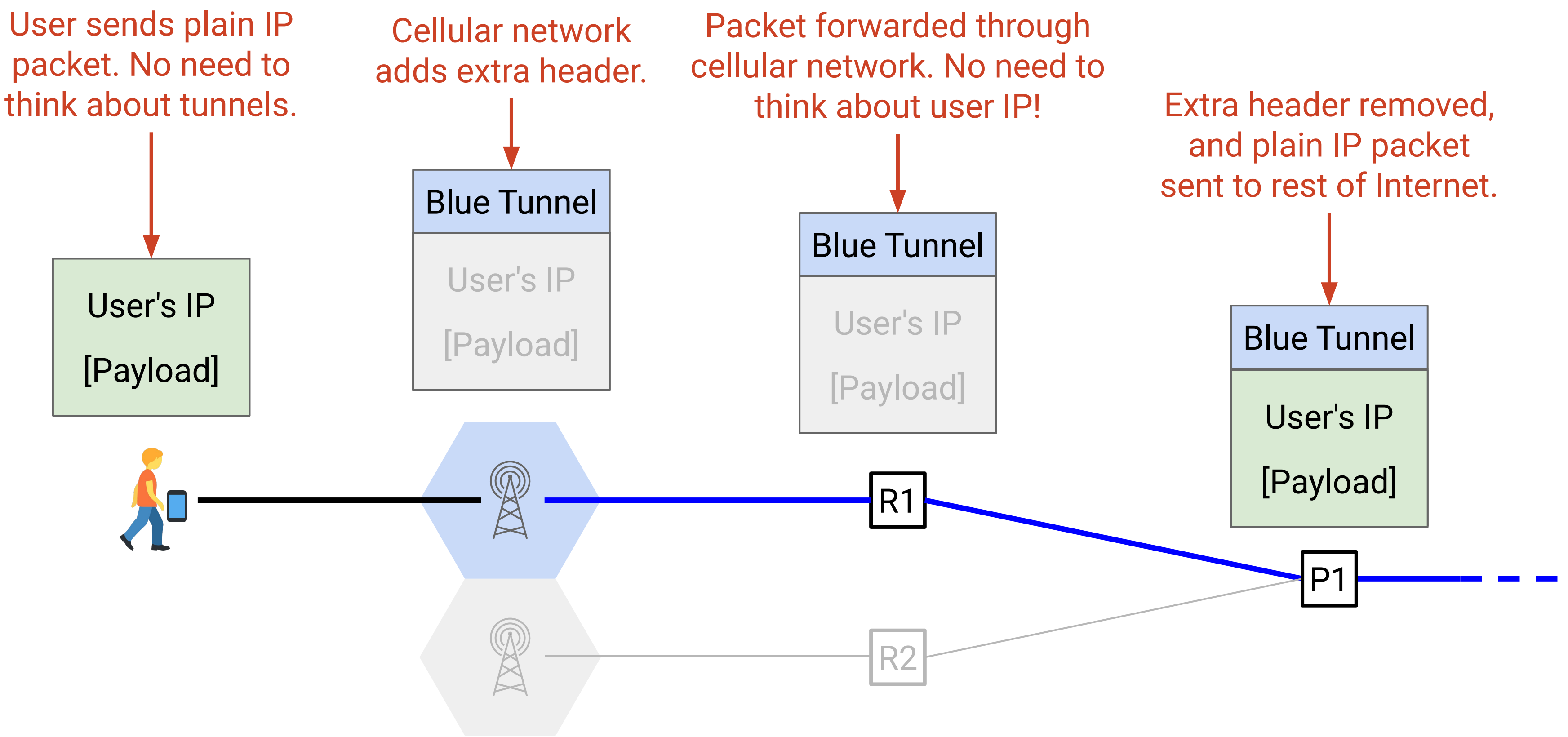
Solution: Mobility manager configures a path from user to Internet using **tunnels**

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



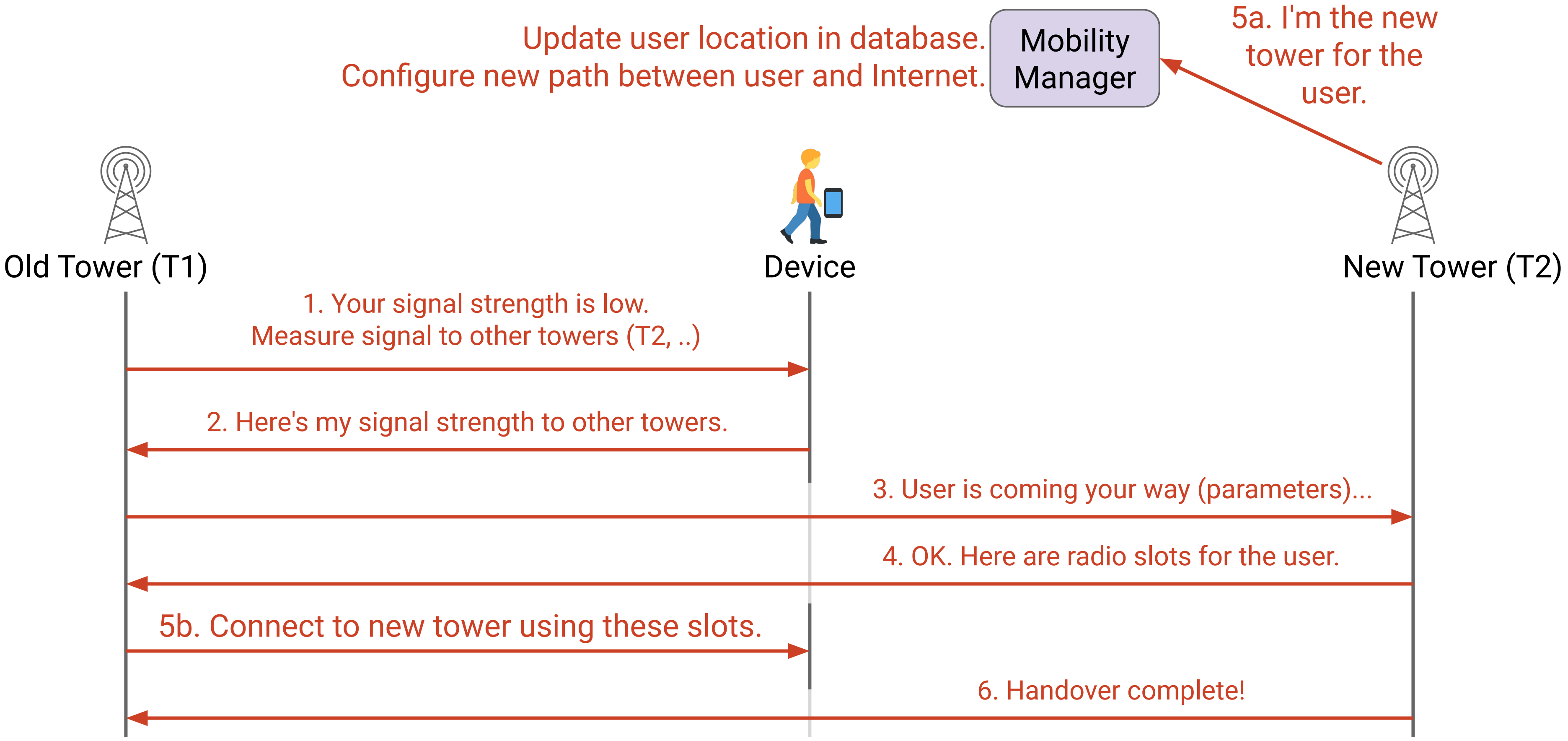
Step 3: Data Exchange with Tunnels

Implemented using **encapsulation**.



Step 4: Handover

Step 4: Handover



Step 4: Handover

Handovers are an intricate process

- 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 and gateways buffer data they receive during handover.
- Relay buffered data to new tower after handover is successful

Handover decisions are made by the operator.

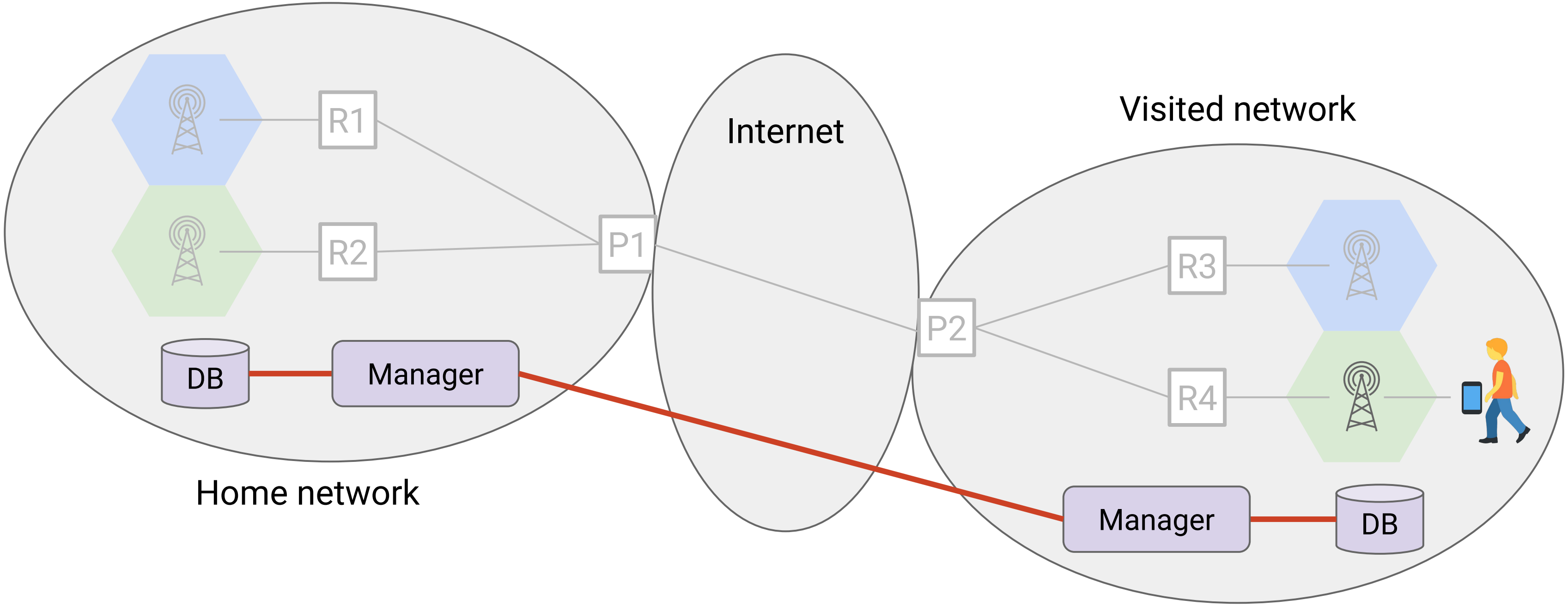
- Device reports signal strength, but old tower chooses the new tower.
- Benefit: Operator has more control, e.g. for load-balancing.
- Drawback: Slower, requires extra round-trips.

Roaming and Other Features

Roaming

Visited and home networks must establish a roaming agreement

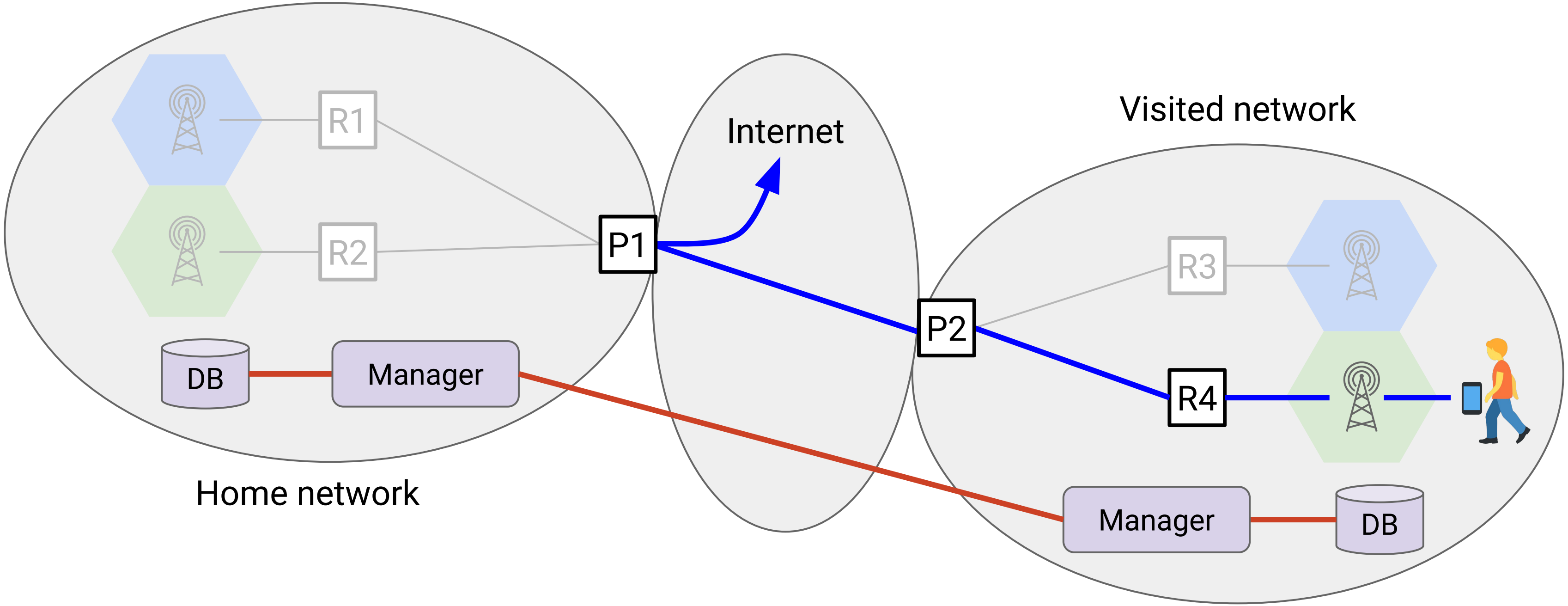
- Visited network uses device's network code (in IMSI) to learn the home network
- Need home network's help to authenticate user.
- Need to update home network's database with user's location.



Roaming

Two common ways to configure the data path from user to Internet.

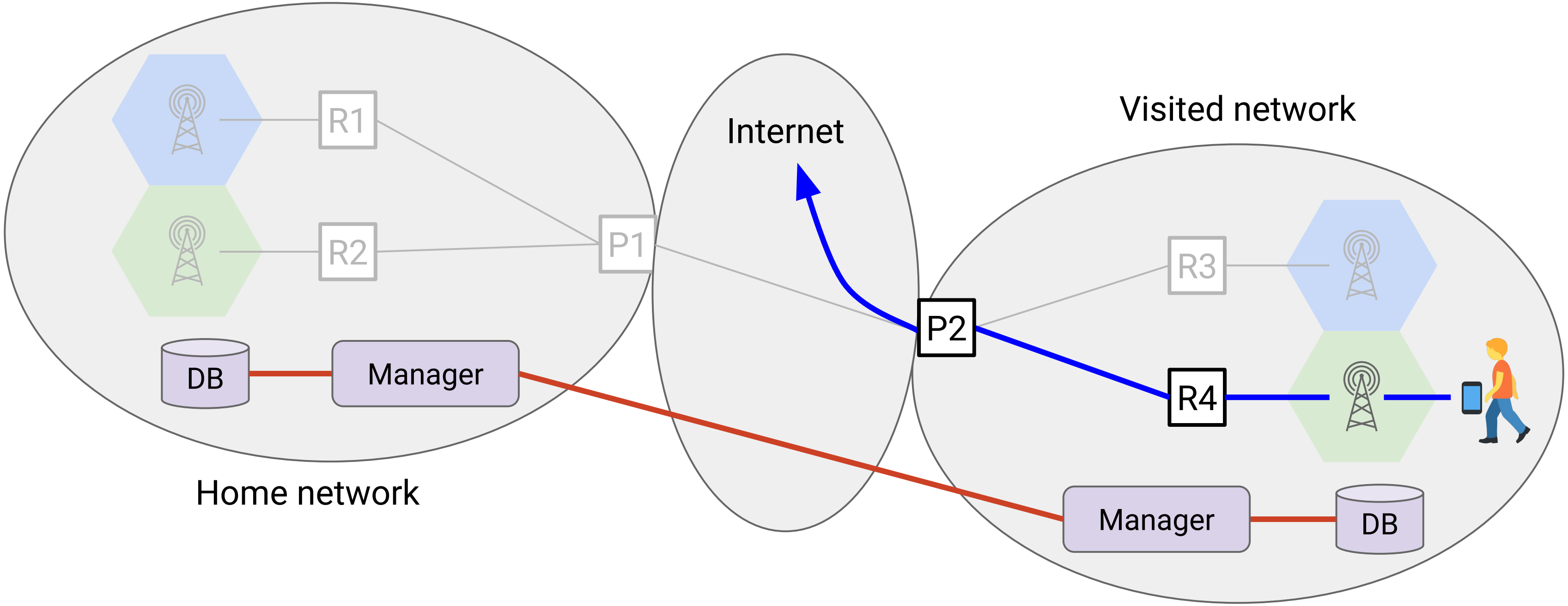
- **Home routing**: Tunnel traffic through the **home** network's packet gateway.
- Benefit: Home network can track user.
- Drawback: Packets takes longer path to Internet.



Roaming

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 and location tracking

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 complex coordination to maintain seamless communication

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 complex coordination to maintain seamless communication

- Alternate design: Change IPs on every handover!
  - Benefit: Much simpler cellular core (no need to setup/reconfigure tunnels, etc.)
  - Drawback: TCP connections break when IPs change
  - Solution? QUIC, an alternate L4 protocol that allows changing IPs

Summary: Cellular Networks

Based on a very different design philosophy:

- Authentication and accounting 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

Evolved from a standalone voice network, to being an integral part of the Internet.

- Testament to the Internet's ability to accommodate heterogeneous architectures
- While exploring greater consolidation between the architectures