# Own your social world…

## … with Decentralized Online Social Networks.

# Why Decentralized Online Social Networks (DOSNs)?

- This data should belong to the people not to the companies.
- A decentralized system can make it possible for individuals to host their own information at home.
- Ultimately people will hold and control their data without depending on big companies.

# DOSN projects: current status

**Peer2Peer:**

- Safebook
- PeerSoN
- Vis-à-Vis
- DECENT

**Federated:**

- Diaspora
- Friendica
- Lorea

# DOSN: Peer2Peer

The node of the user has an important role in the operation of the system. Each node contributes resources in order to support system's functionalities.

- **Advantages**
  - **Anonymity**
  - **Privacy**
    - **No central authority**
- **Disadvantages**
  - **Data availability**
  - **Privacy**
    - **Data ownership**
  - **Delays in data retrieval**

# DOSN: Federated

Main elements in the network are servers responsible for holding the data and maintaining the functionalities that the system provides.

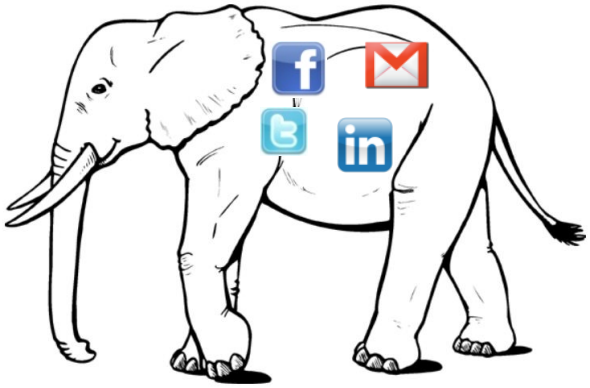
## Advantages

- Availability
- Reliability
- Near real-time data retrieval

## Disadvantages

- Privacy
- Maintenance cost
- Bootstrapping issue

# Things we have learnt…



DIASPORA*

jappix

pump.io

Tent

- **Privacy and data ownership is not enough to persuade users to move to a different platform.**
- **We cannot ignore the elephant(s) in the room…**
- **Address current limitations of DOSNs: Availability, Privacy, Bootstrapping, Maintenance cost, Performance**

# Digital Footprint

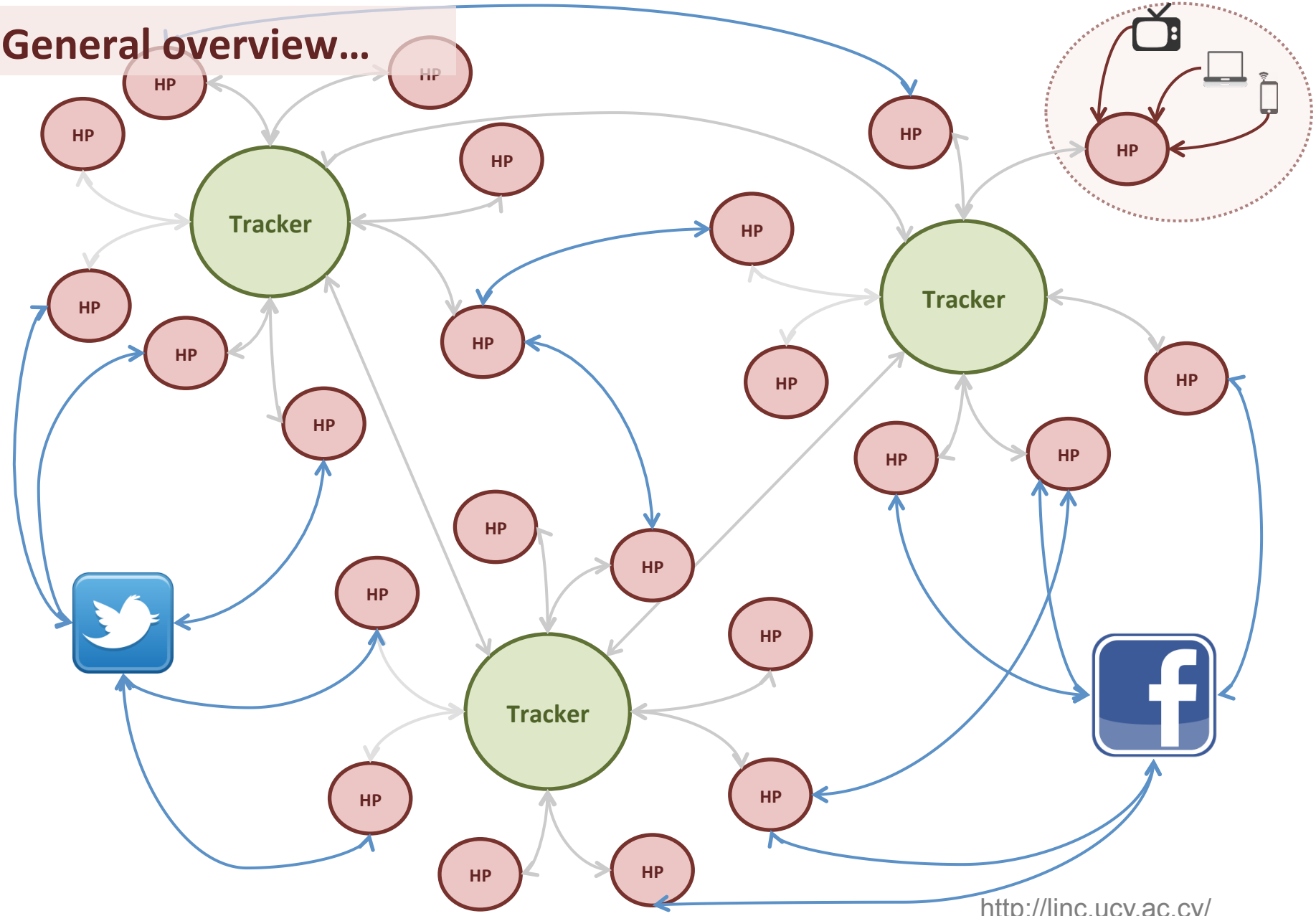
- **Do we need to care only about our social network data?**
- **We have much more sensitive data out there.**
- **Digital footprint:**
  - *"If asked to describe what would comprise this "footprint," likely responses would include things like your social network profiles, your web site or blog, your photos shared on an online service, videos you uploaded to YouTube, perhaps even mentions of you in the local paper or your school's web site."* **[Perez S., *Calculate Your "Digital Footprint" with New Tool from EMC*]**

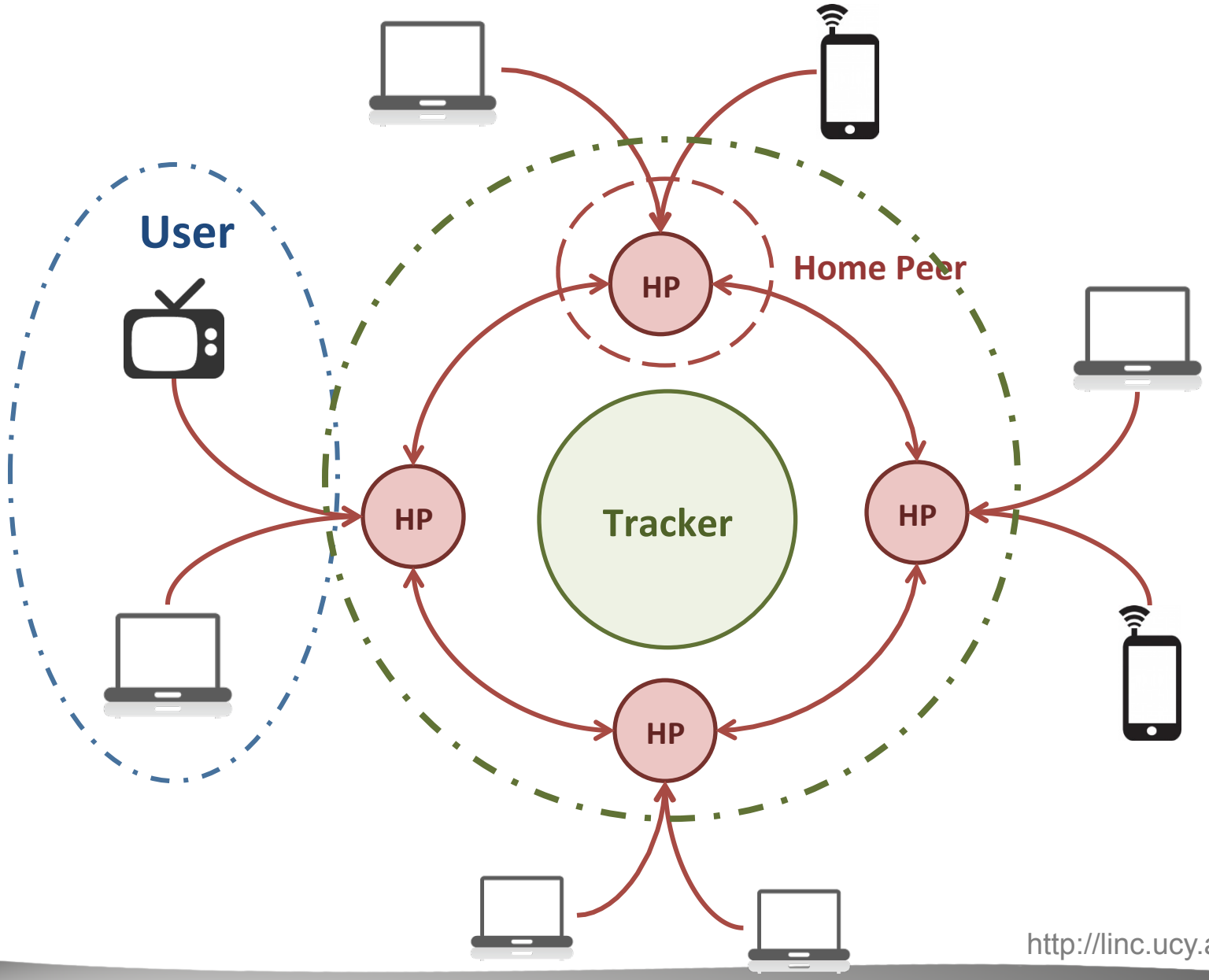
- **How about having the control of the most sensitive part of our footprint?**

digital
Own your ~~social~~ world…

# Proposed Architecture

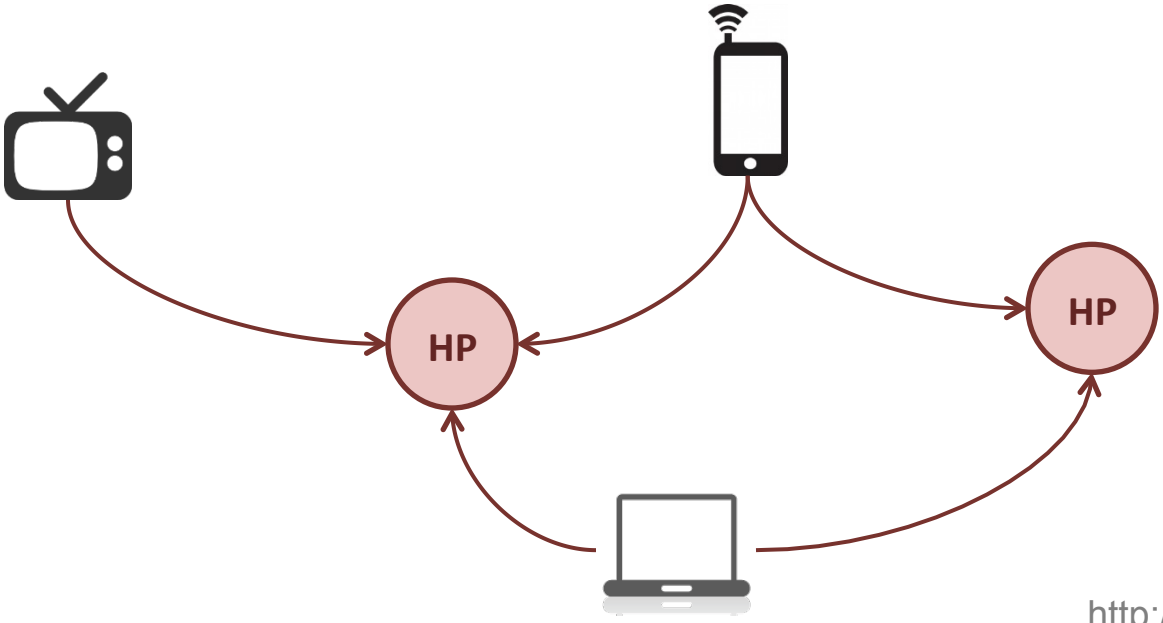
# General overview…




User
HP
Home Peer
HP
Tracker
HP
HP

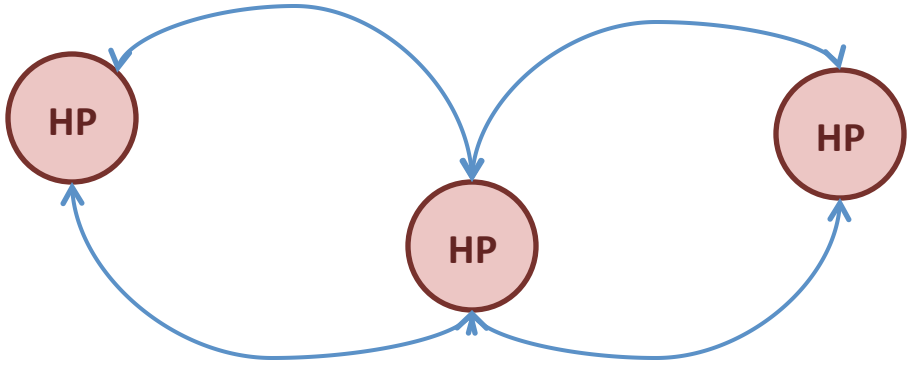
# The User

- Interaction through the web.
- From any web enabled device (desktop laptop, mobile phone, tablets, smart TVs, etc.)
- In full control of the data.



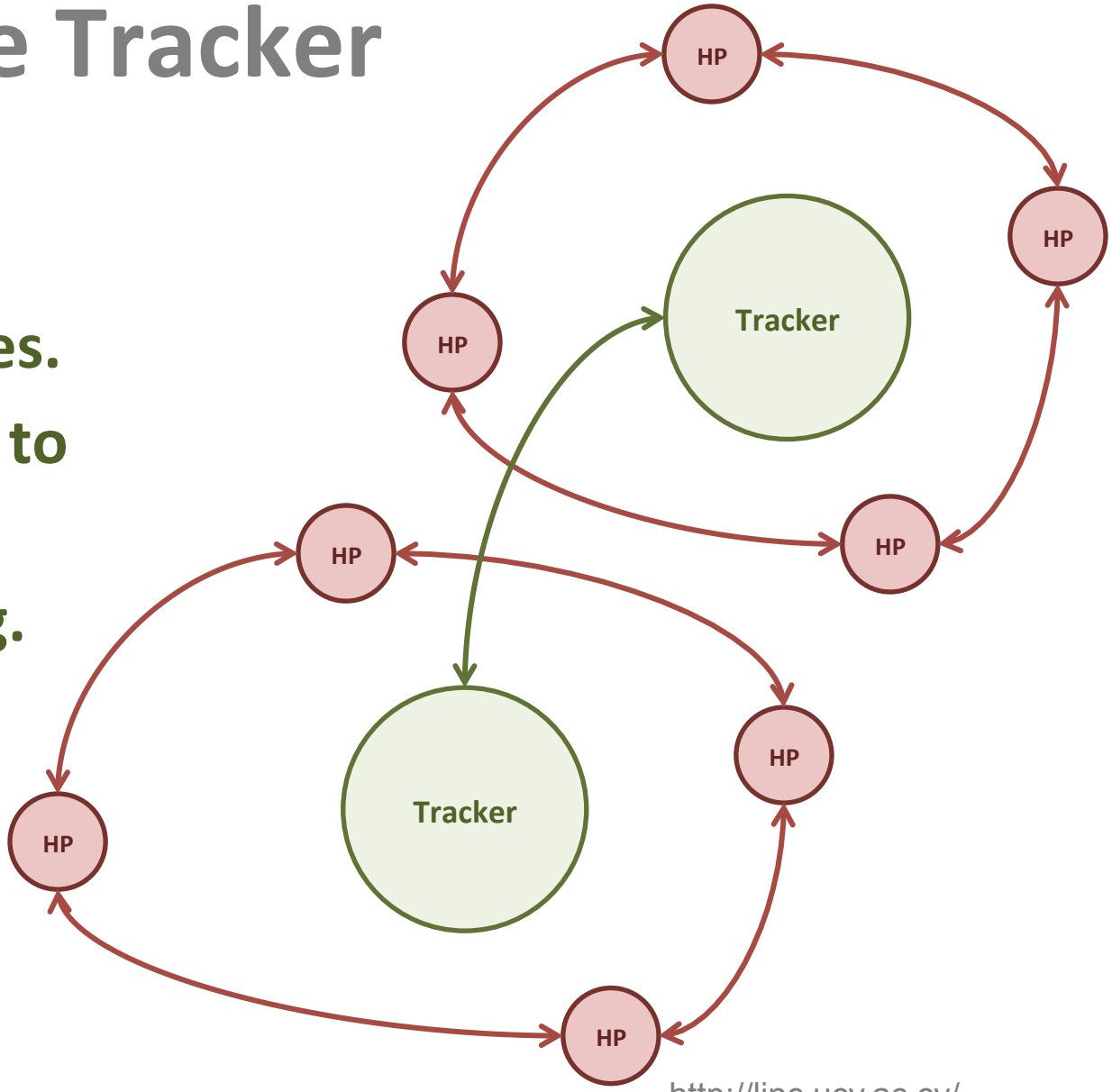
# The Home Peer

- Stores data..
- Satisfies client requests.
- Access based on permissions.
- Disseminates information on the network.
- Should be online 24/7 (though bad things might happen…).



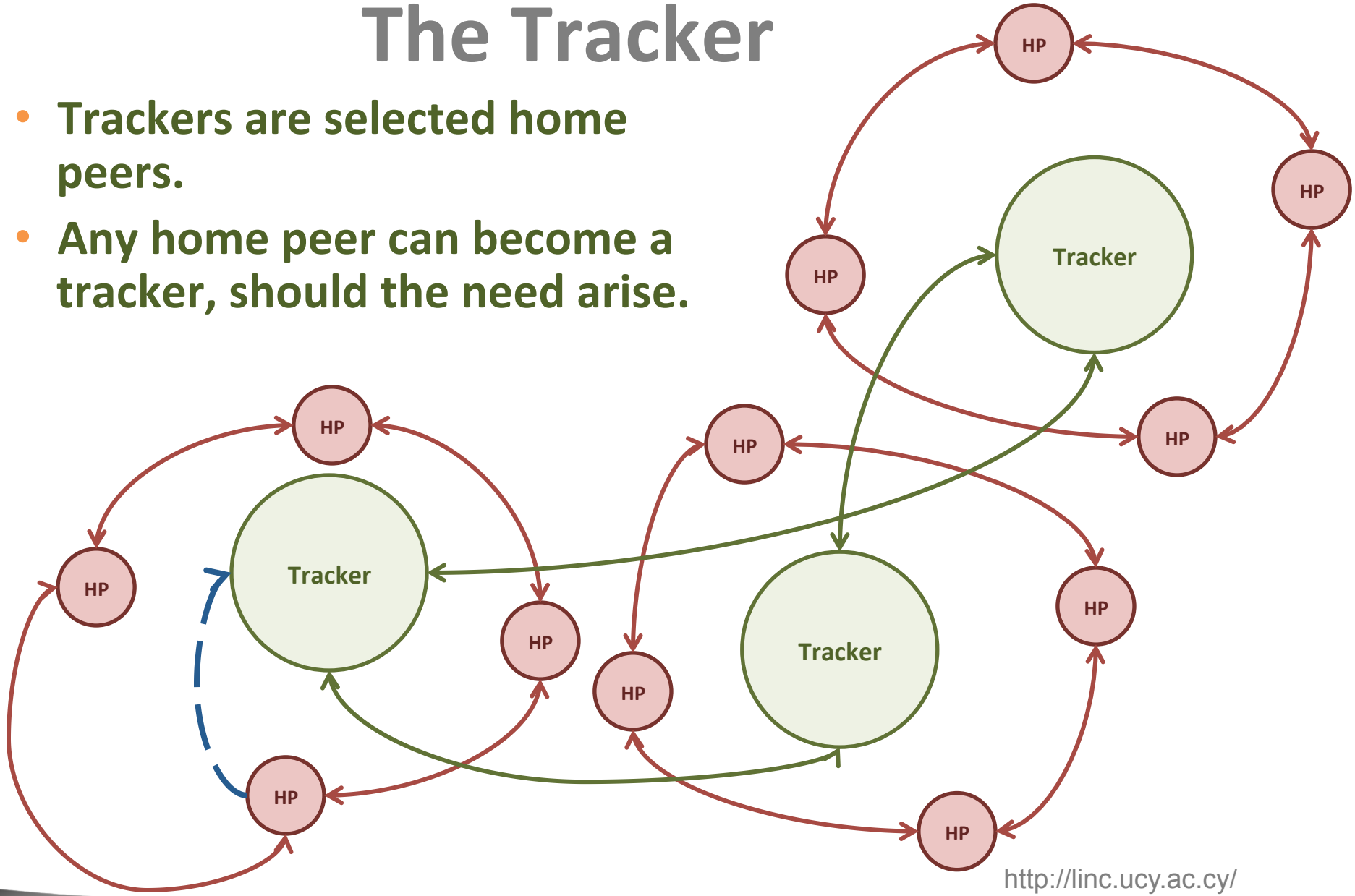
# The Tracker

- Facilitates communication between the nodes.
- Cluster the nodes to disseminate data.
- Supports indexing.
- Bridge clusters.



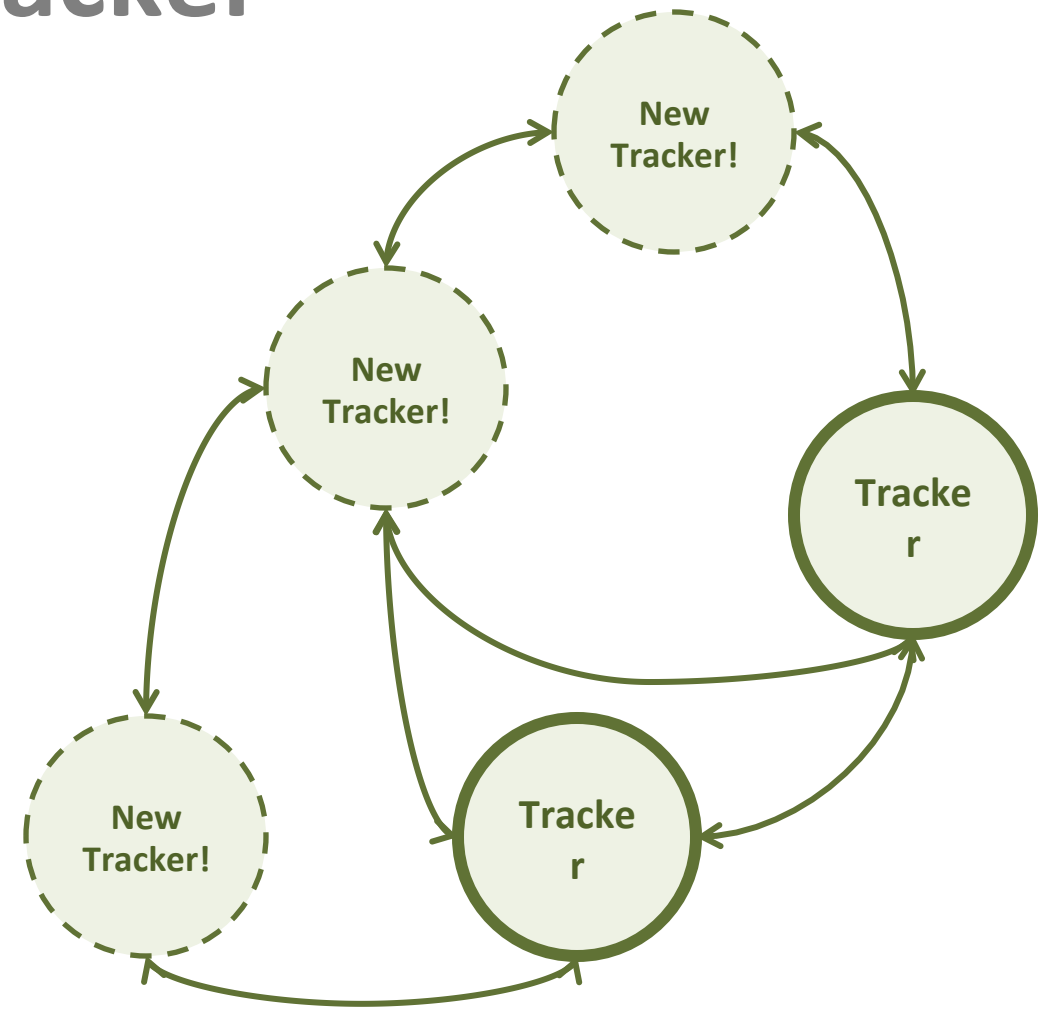
# The Tracker

- Trackers are selected home peers.
- Any home peer can become a tracker, should the need arise.

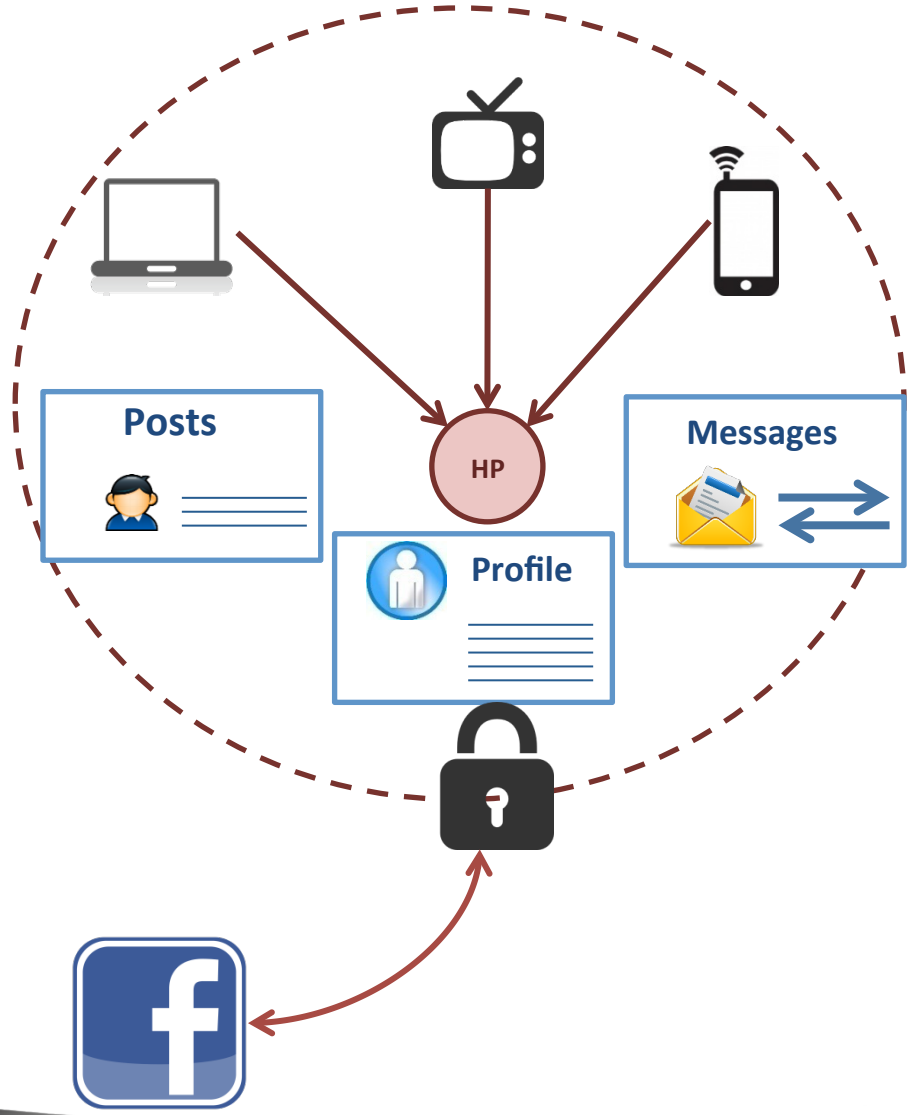


# The Tracker

- Selection based on collected statistics.
- They hold the address of other trackers.



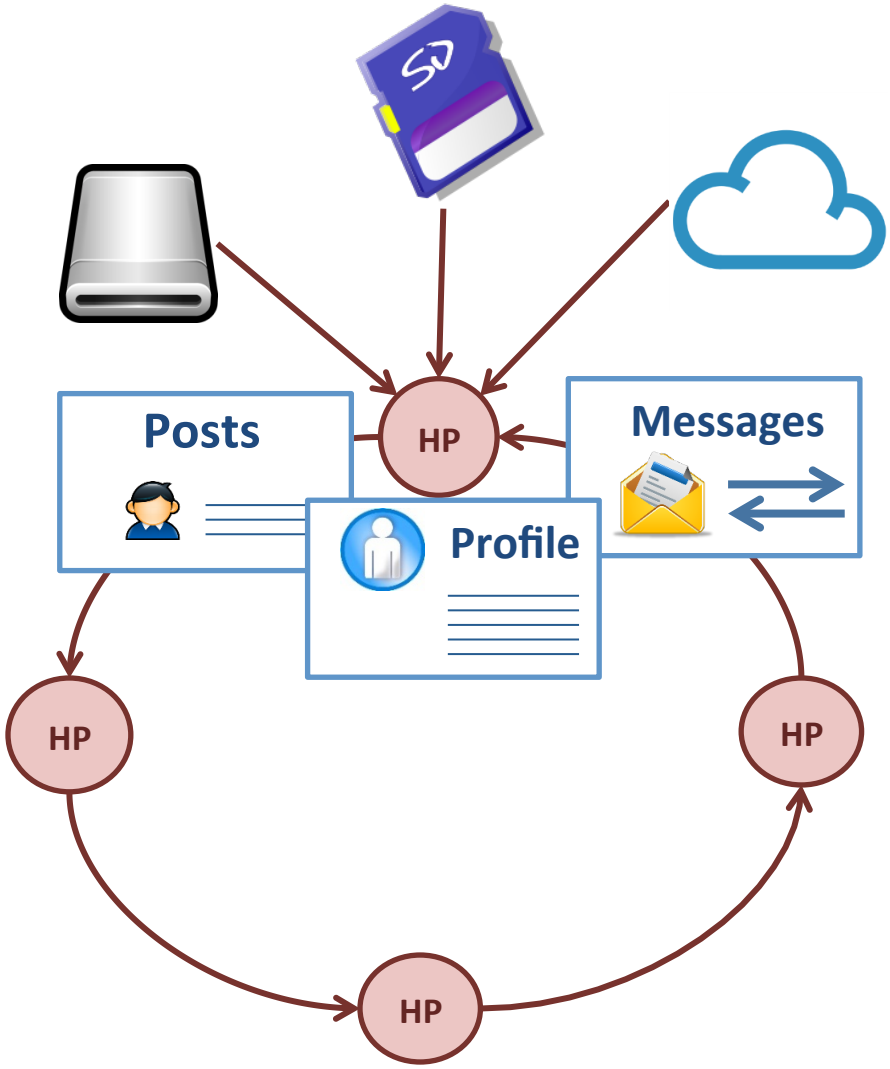
# Architecture Purpose




- Fulfill user privacy considerations.
- Home peer holds user data at home.
- Interact with existing online services.

# Materialize Data and Identities

- **Store data in** SD cards External Drives connected via USB or External Cloud Storage Services.
- **Store credentials for third-party services.**
- **Share with access control.**



# So what does this service offer me?

- A device that stays home and holds my data safely.
- Allows me to access my information via the Internet.
- Allows me to interact with other services (Facebook, Twitter, LinkedIn, Gmail, etc.)
- Allows me to connect my devices in a single private network via apps or browsers.

# Benefits

- I am in control of my own digital footprint.
- One place to access everything:
  - Social Networks from different providers.
  - Email accounts.
  - Devices connected at home (sensors and actuators).
  - File storage and sharing.
- 24/7 communication no matter where I am.
- Access through a browser or/and applications.

# How?

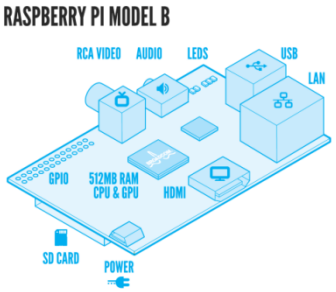
- Leverage from existing infrastructures (Internet and power supply at home).
- Low cost devices <u>could</u> run a software service.
- Users will own their data at their homes.

4xRaspberry Pi

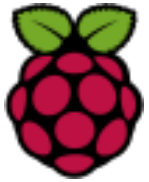
Arduino DUE

# Example of a Low Cost Device

- Raspberry Pi
  - CPU: 700 MHz ARM
  - Memory: 512 Mb (SDRAM)
  - Input: 2 UBS ports, 1 SD/MMC/ SDIO card slots
  - Output: Video (RCA, HDMI), Audio
  - 10/100 Ethernet
  - Supported OS: Raspbian OS , Arch Linux, ARM, Debian GNU/Linux, Fedora, FreeBSD, NetBSD etc.
  - Size: 0.85cm x 0.56cm x 0.21cm
- Storage
  - External Hard Disk Drive
  - Cloud Storage



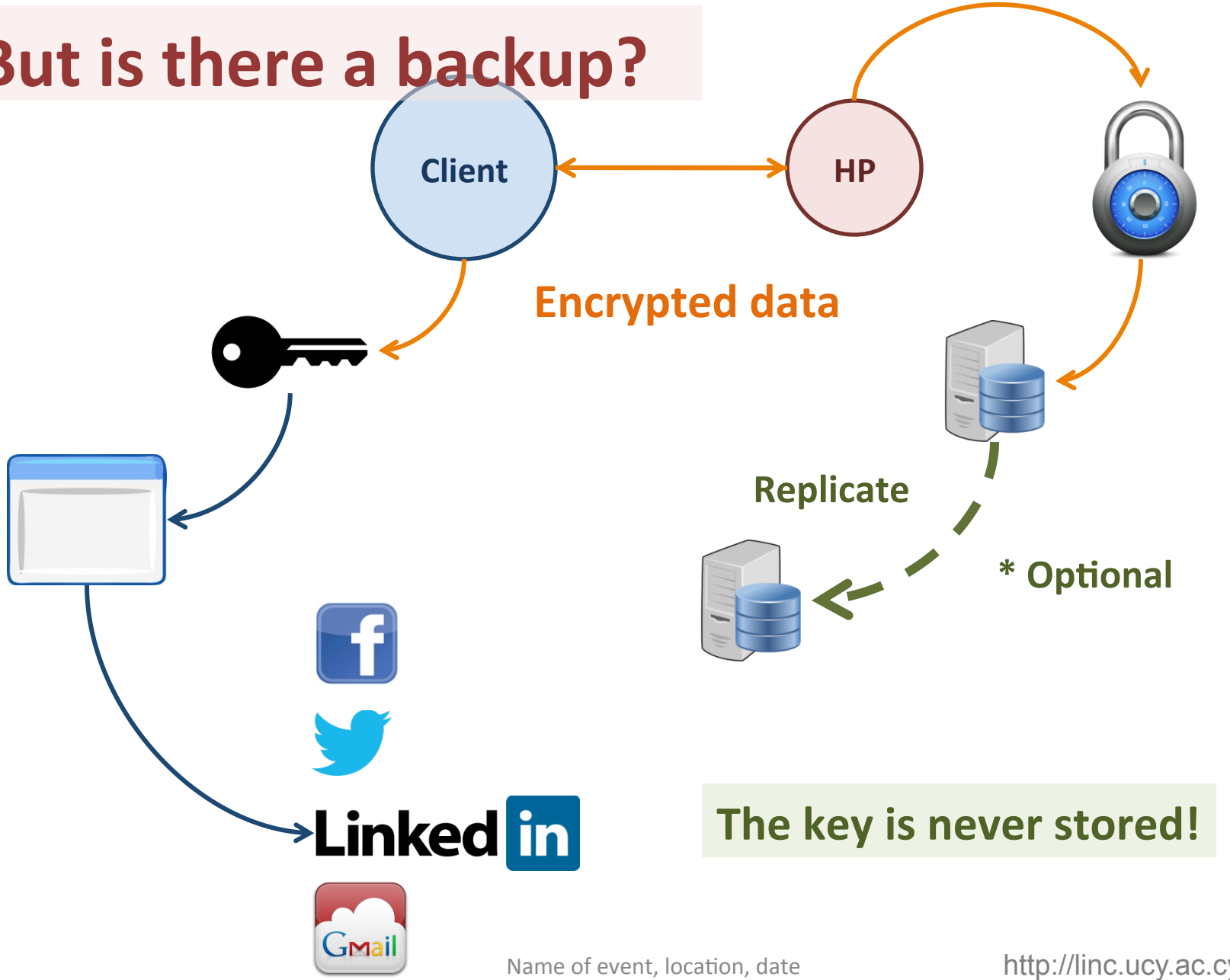
- **Cost for each Home-Peer**
  - **Raspberry PI kit: ~50 euros**
  - **External Hard Disk Drive:**
    - **16 GB USB flash drive (1 user): 17 euros**
    - **500 GB (1-5 users): 60 euros**
    - **1 TB (1-10 users): 80 euros**
- **Average household size in Europe ~ 3**
  - **User cost:**
    - **Min: 36,60 euros -> Storage 166,6 GB**
    - **Max: 43,33 euros -> Storage 333,3 GB**



# But is there a backup?

- Cost for each Home-Peer
  - Raspberry PI kit: ~50 euros
  - External Hard Disk Drive:
    - 16 GB USB flash drive (1 user): 17 euros
    - 500 GB (1-5 users): 60 euros
    - 1 TB (1-10 users): 80 euros
- Average household size in Europe ~ 3
  - User cost:
    - Min: 36,60 euros -> Storage 166,6 GB
    - Max: 43,33 euros -> Storage 333,3 GB

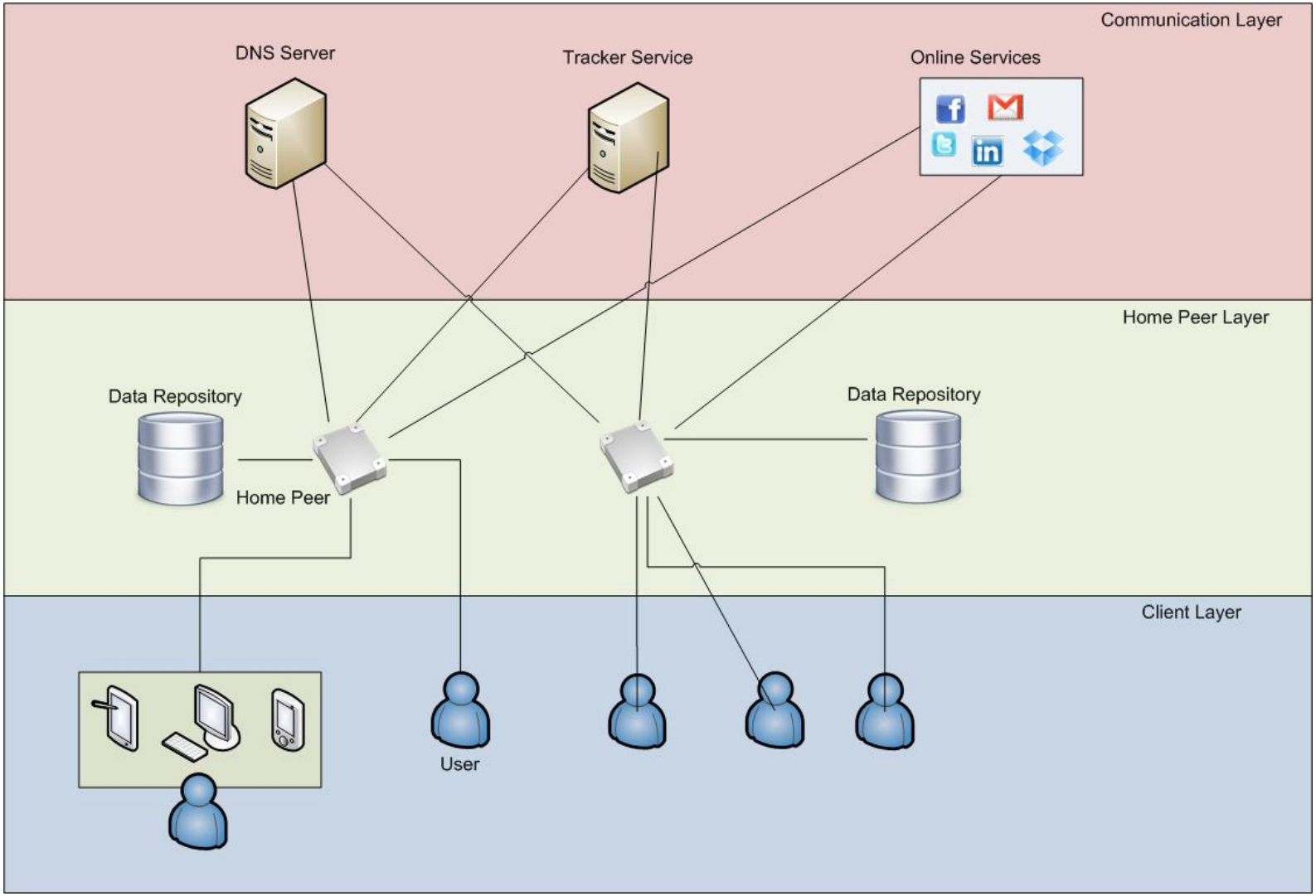
# But is there a backup?



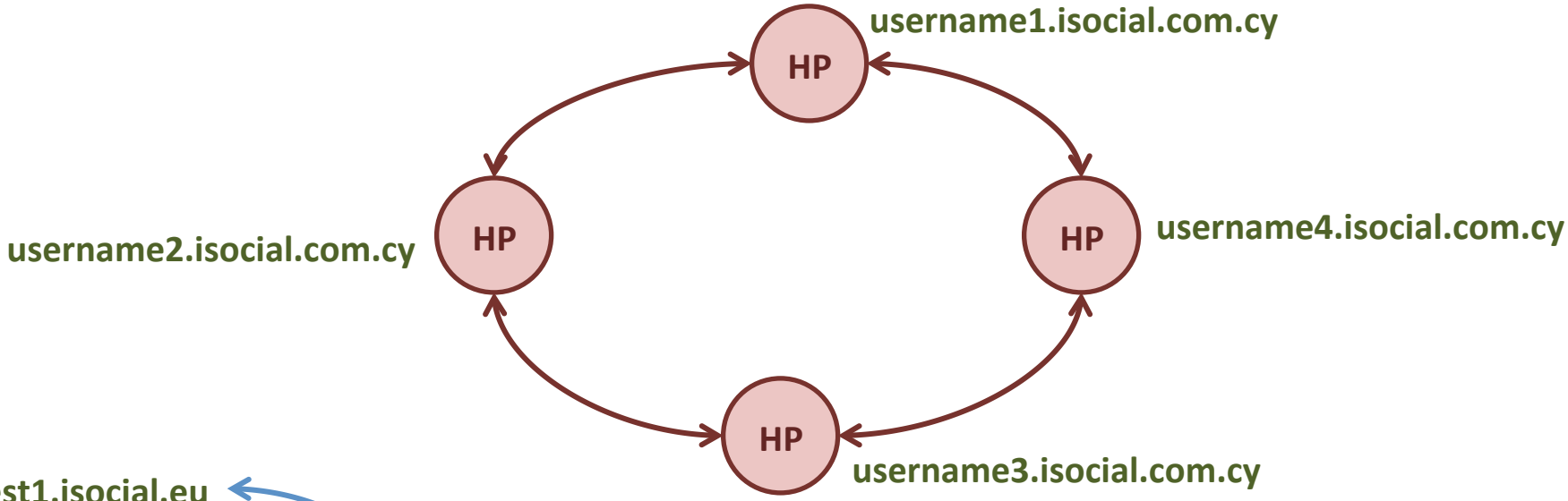

The key is never stored!

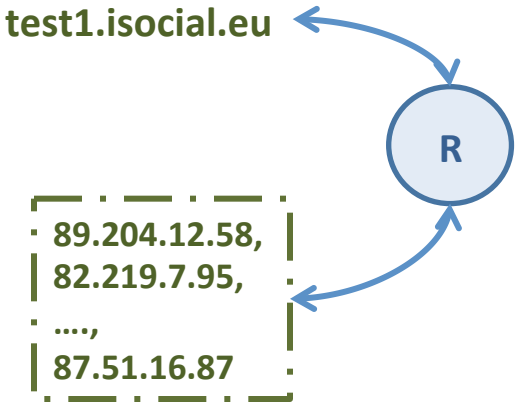
# ARCHITECTURE IN MORE DETAIL…

# Architecture Overview



# DNS is used to reach and identify the Home peers.



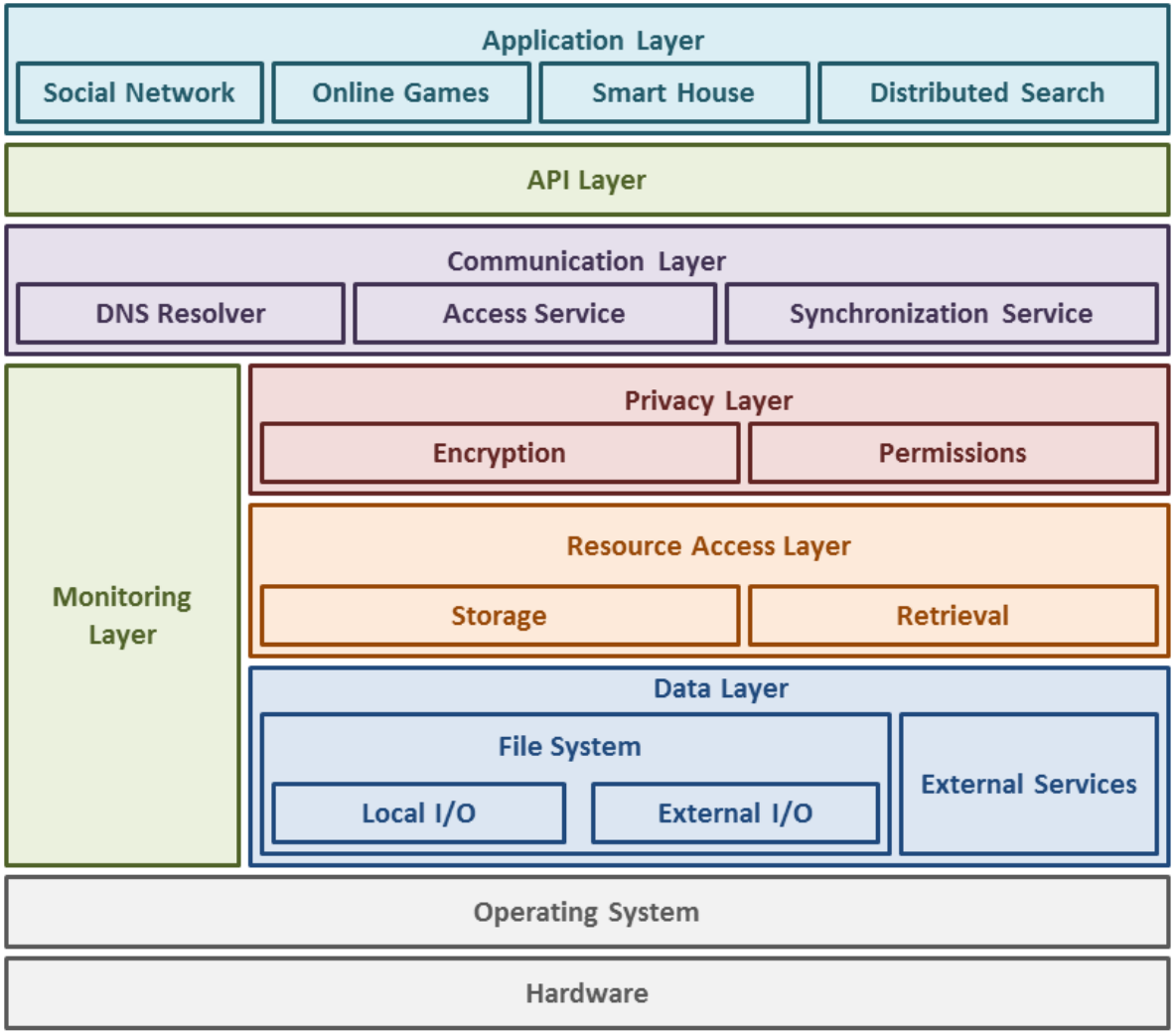




**Most home routers support dynamic DNS**

**Otherwise, there are options…**
**- Or implement our own with Power DNS!**

- DynDNS.com
- No-IP
- EasyDNS
- ZoneEdit
- DNSPark
- NameCheap
- DSLReports
- FreeDNS (Afraid.org)
- OpenDNS
- dy.fi (Finland only)

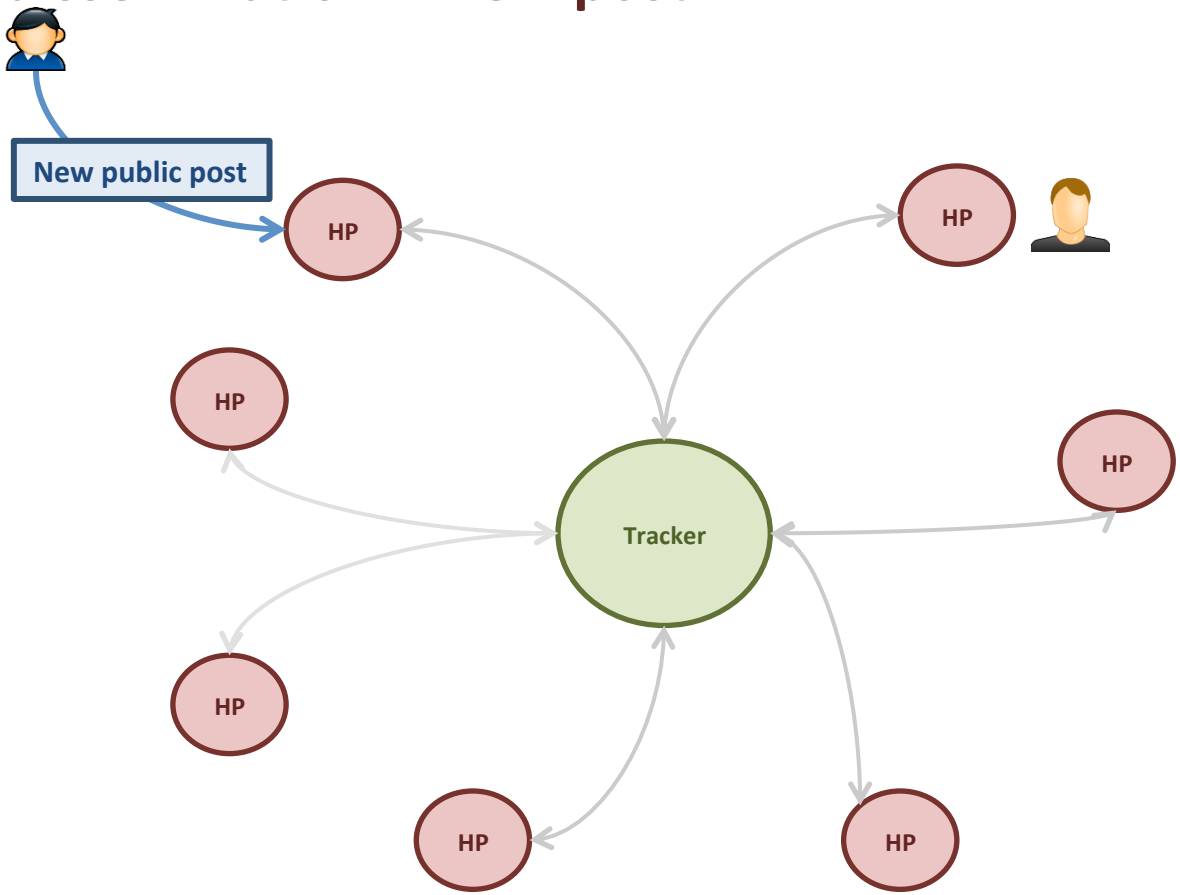
# Home Peer's Architecture

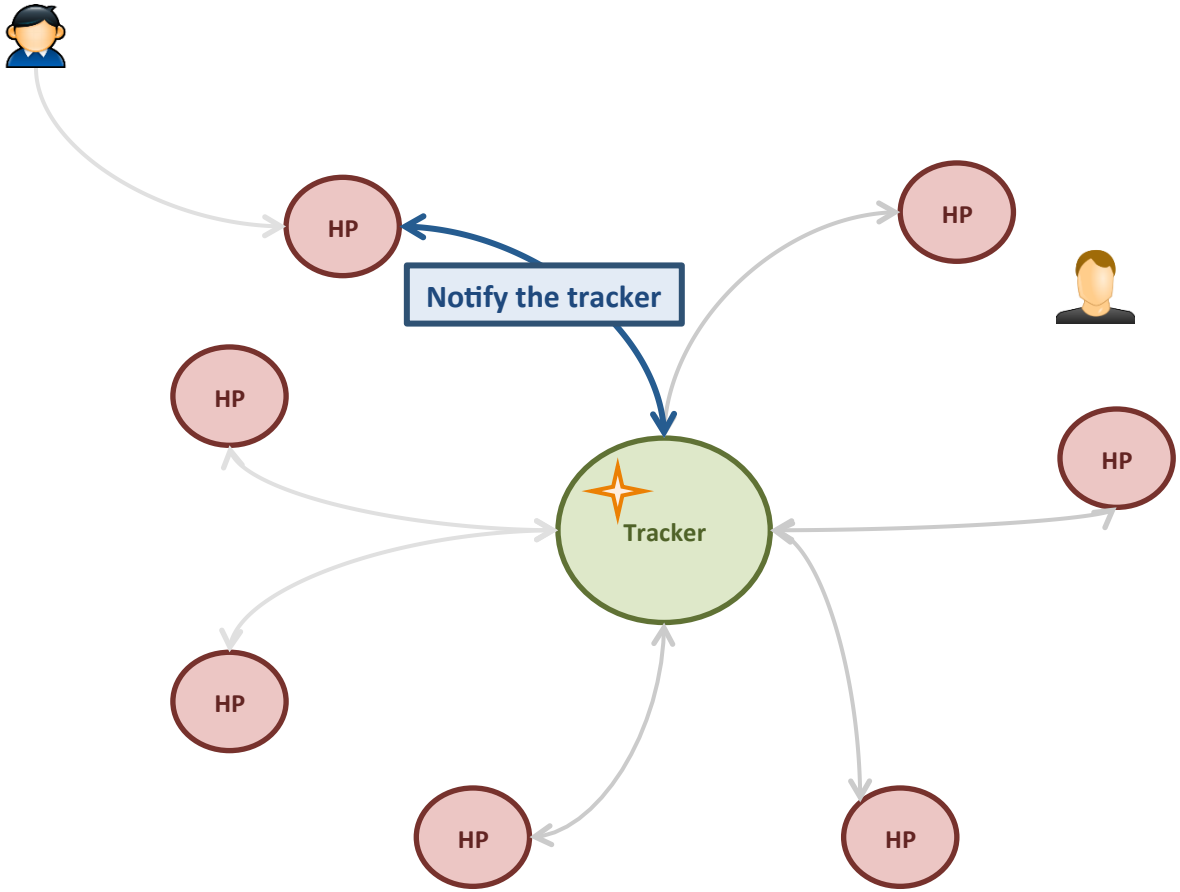


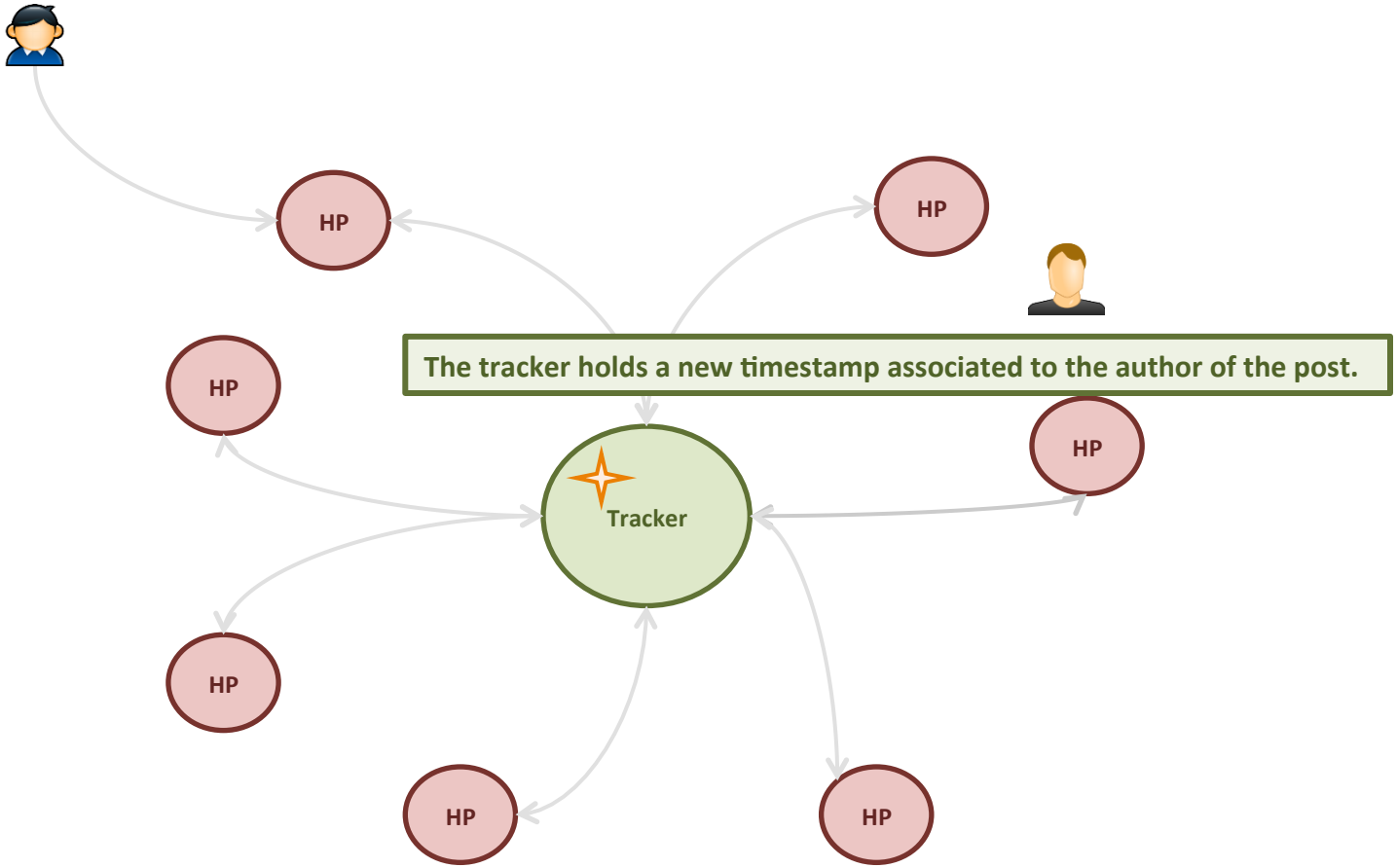
API
Gmail

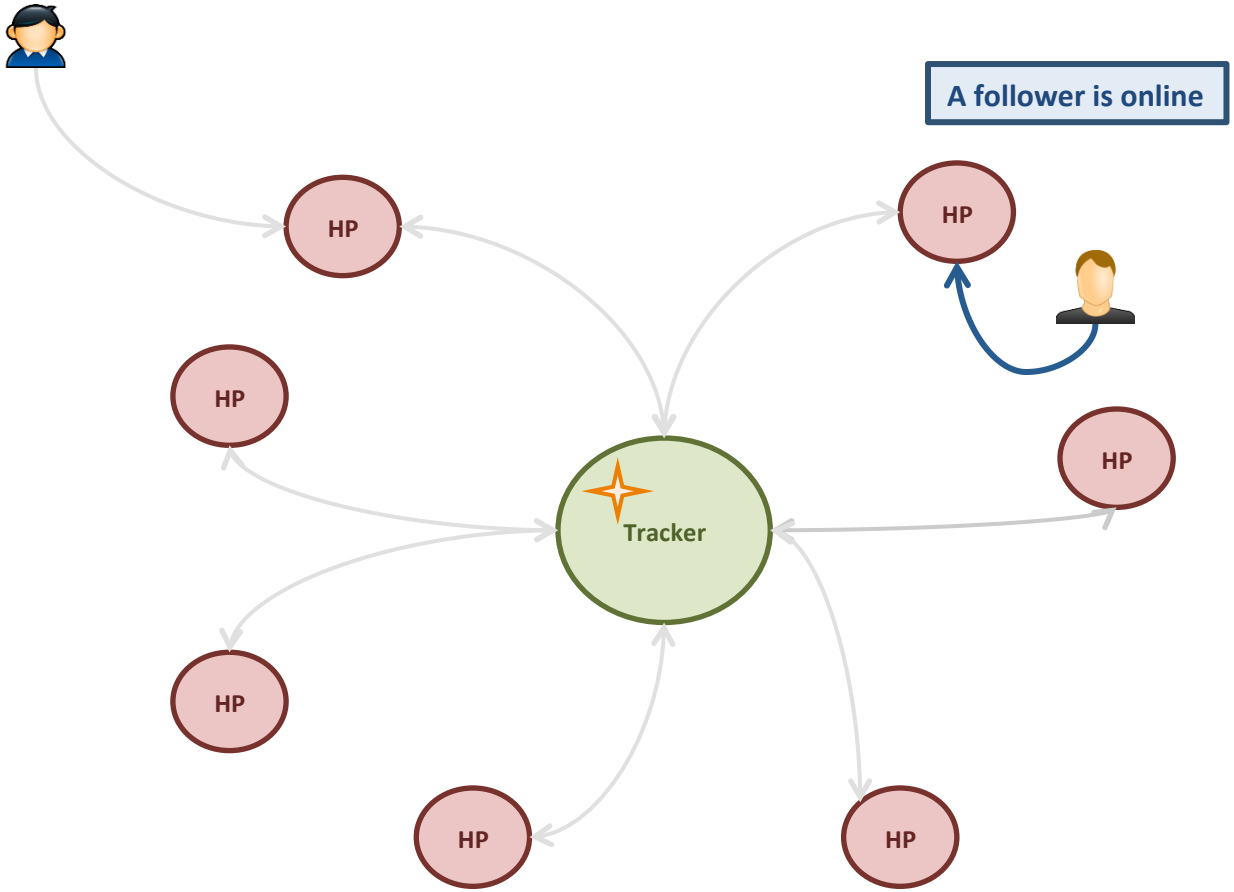
# EXAMPLE SCENARIO

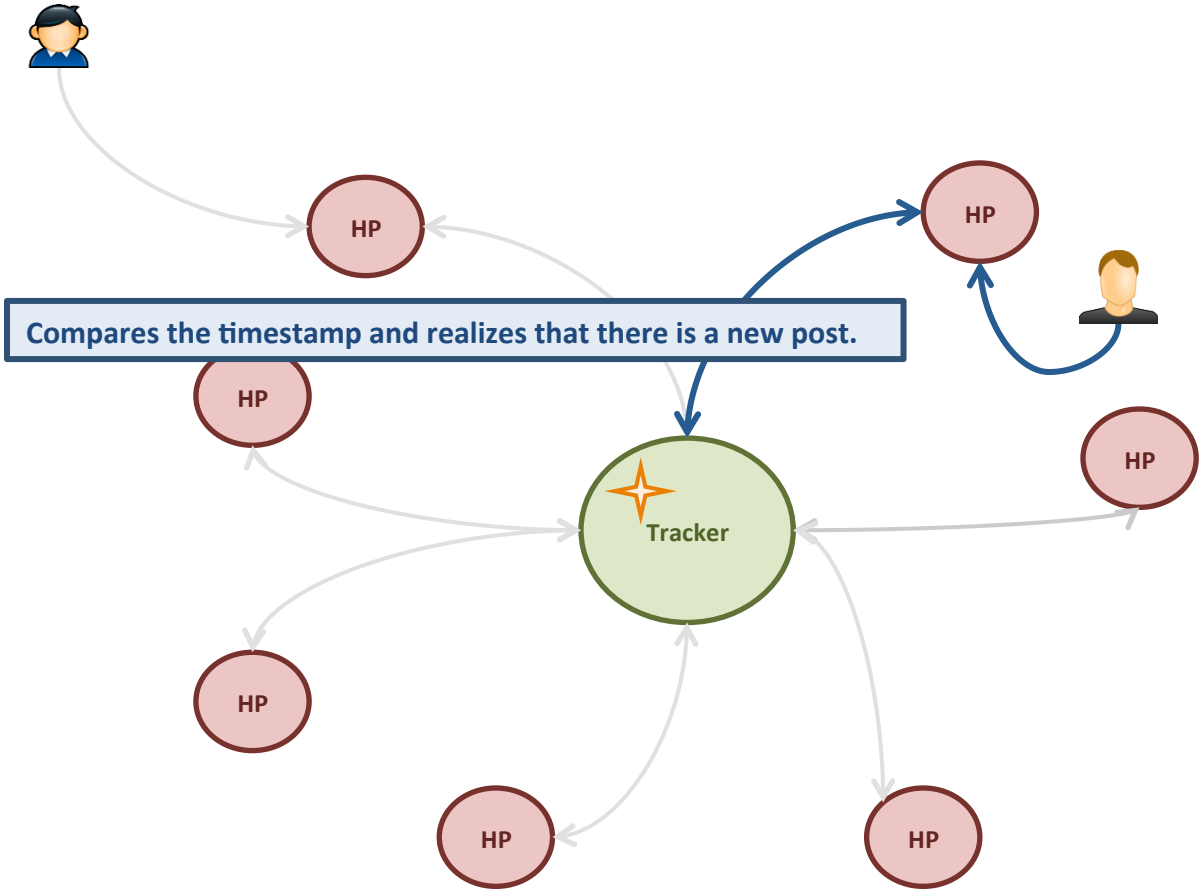
# Data dissemination… New post

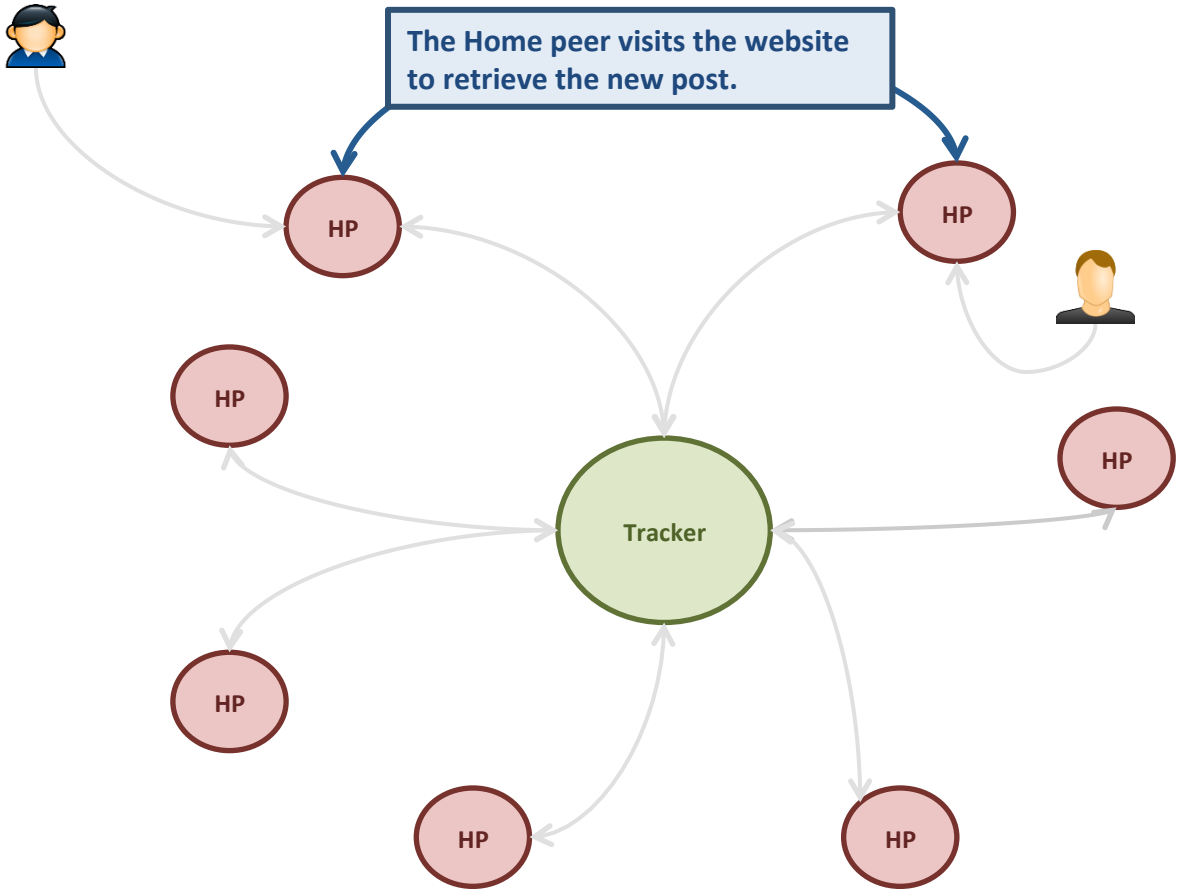



HP
Notify the tracker
HP
HP
HP
Tracker
HP
HP
HP
HP

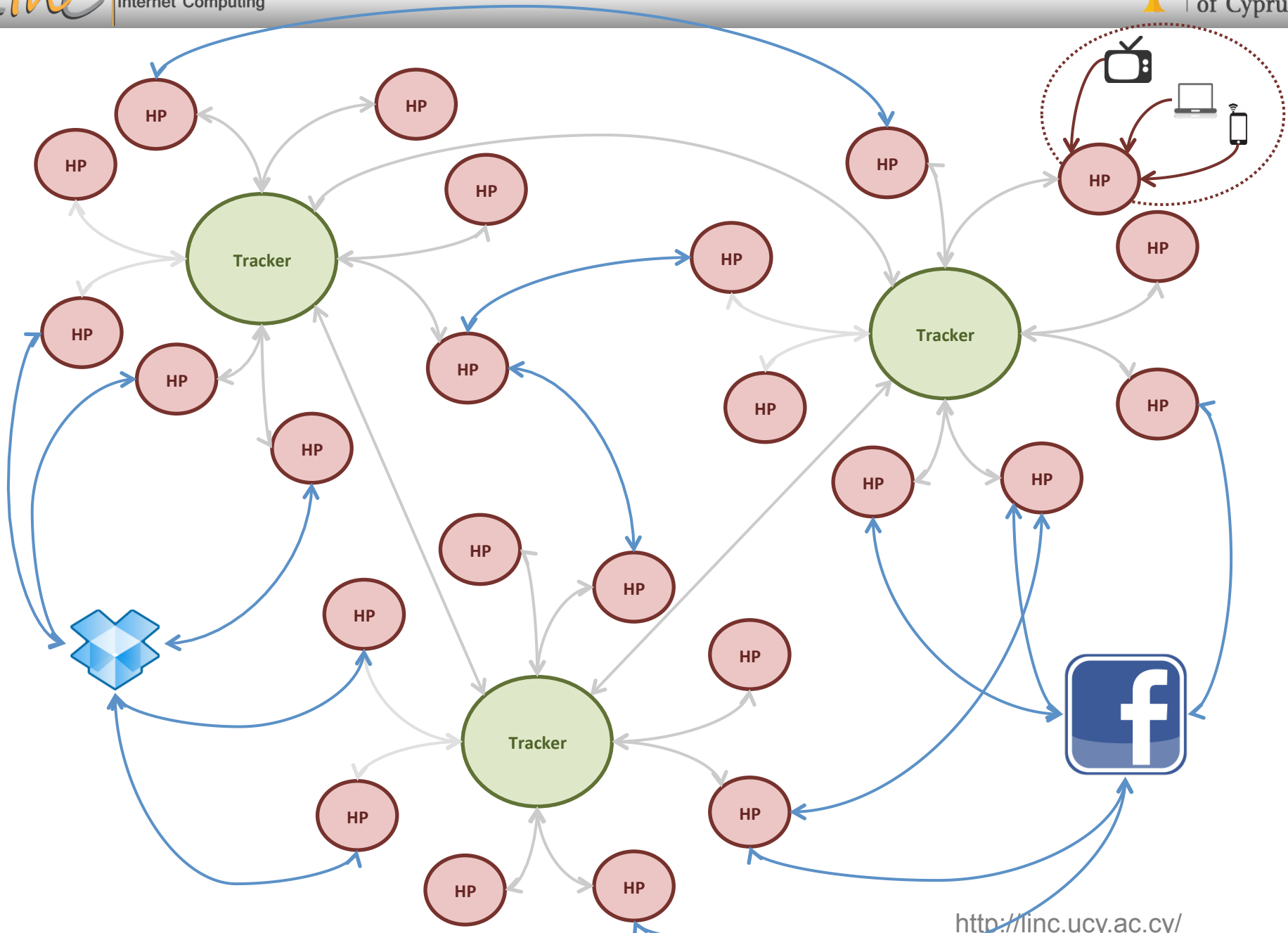

HP
HP
HP
The tracker holds a new timestamp associated to the author of the post.
HP
Tracker
HP
HP
HP
HP


A follower is online
HP
HP
HP
HP
HP
HP
HP
Tracker


HP
HP
Compares the timestamp and realizes that there is a new post.
HP
HP
Tracker
HP
HP
HP
HP


The Home peer visits the website to retrieve the new post.
HP
HP
HP
HP
Tracker
HP
HP
HP
HP

# RECAP!

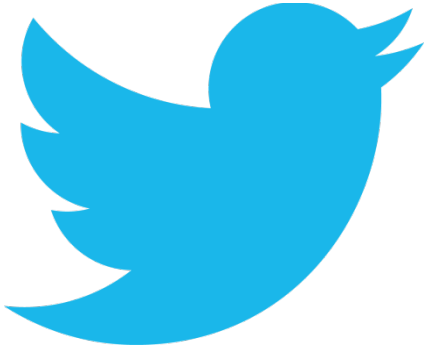

HP
Tracker
Tracker
Tracker

# Privacy: your data stays home.

# Bring your devices together.

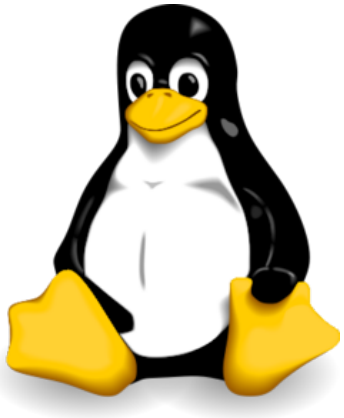
# Host your profile at home.

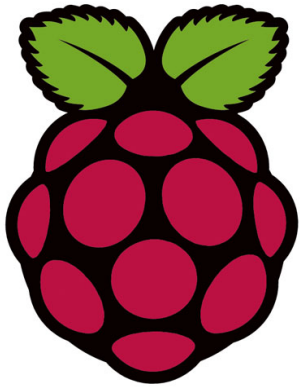
# Bring your services to one place.



LinkedIn

# Access your data from anywhere.





# Do all this with less than 50 euros.

## (with a Raspberry Pi and a lot of software development…)

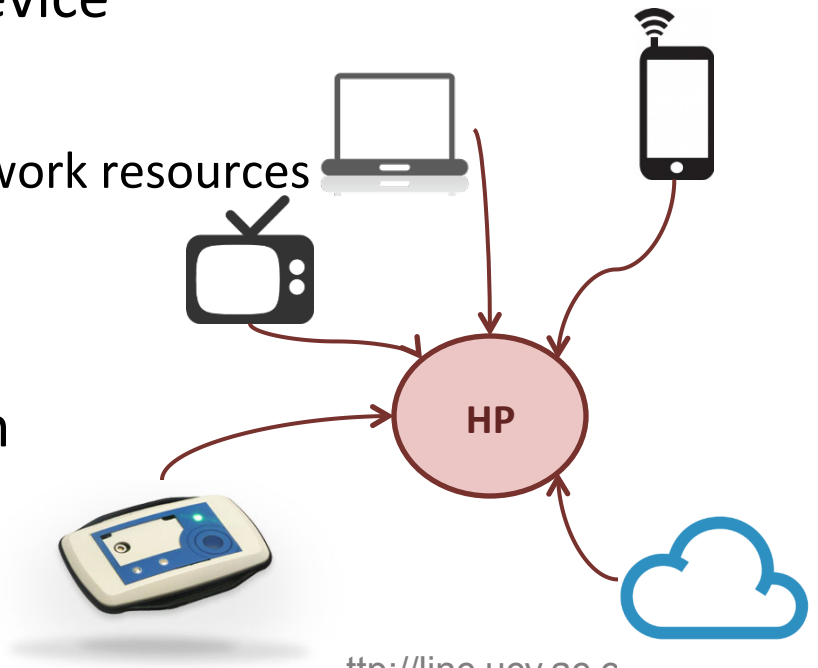
# NEXT STEPS

# Next Steps

- Figure out a good authentication mechanism.
- Data management under encryption.
- And some more…

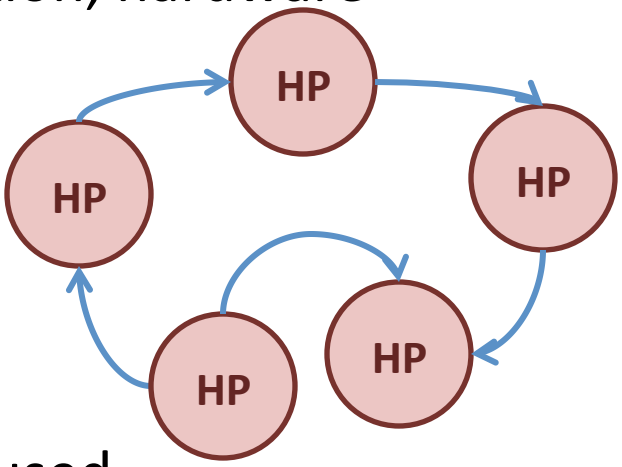
# Home Network (n to 1)

- How can we target the problem of dynamic data gathering considering the limitations of low-resource devices (HomePeers and external devices)?
  - Protocol that maintains efficiently the package transfer
  - Middleware between protocol-device
  - Investigate tradeoffs
    - Energy consumptions VS Home Network resources
    - Resources VS Reliability
  - Data model
  - Developers API for data collection



# Data Dissemination in the Network

- How can we efficiently disseminate data in a P2P network of low-resource devices?
  - Extreme cases: Popular profiles, public information, real-time notification, large-data dissemination, hardware failure
  - Investigate tradeoffs
    - Resources VS Reliability
    - Devices Resources VS Network resources
    - Etc.
  - Investigate infrastructures that can be used
  - Knowledge representation
  - Developers API for data dissemination in our infrastructure

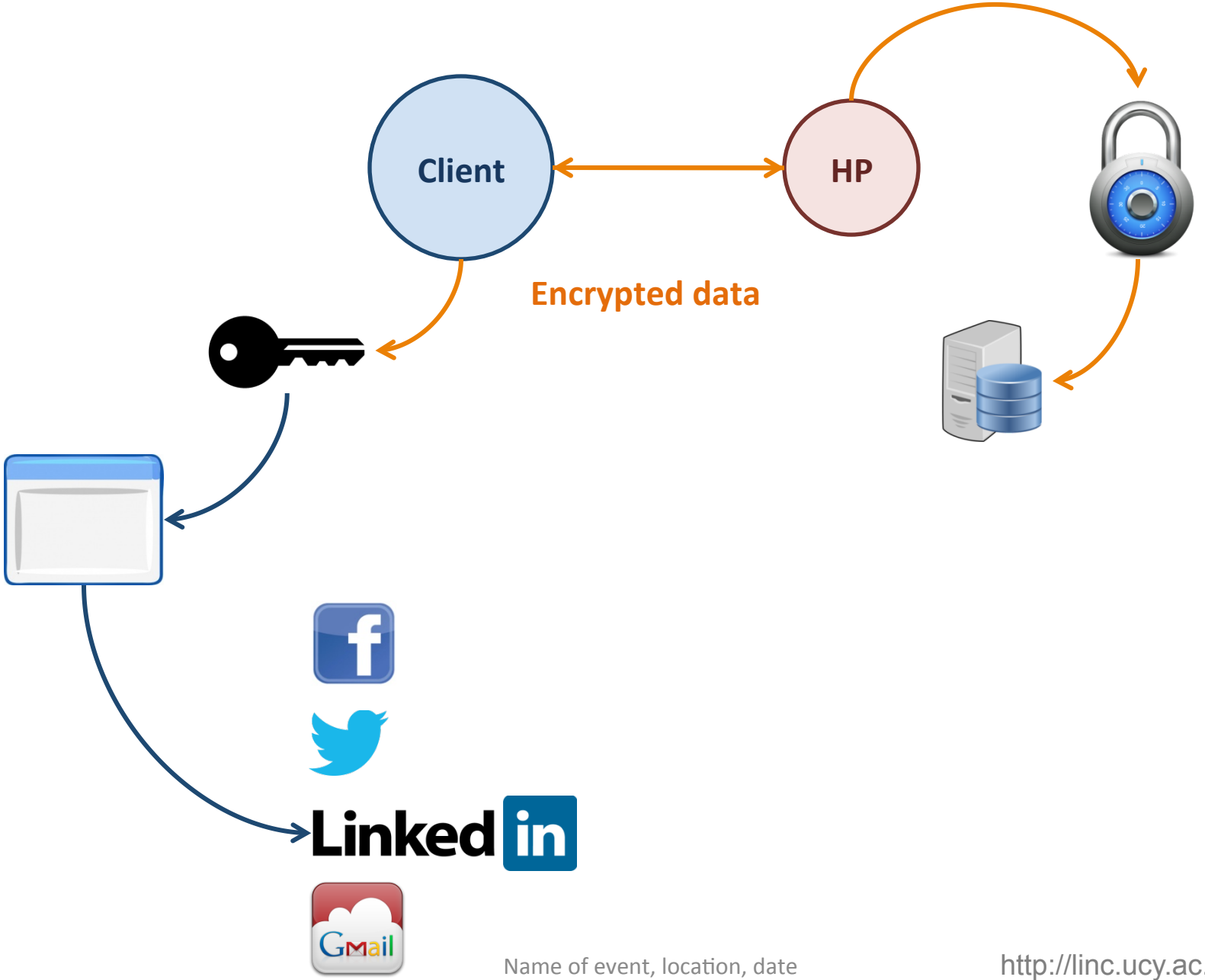


# Ideas - Feedback – Questions

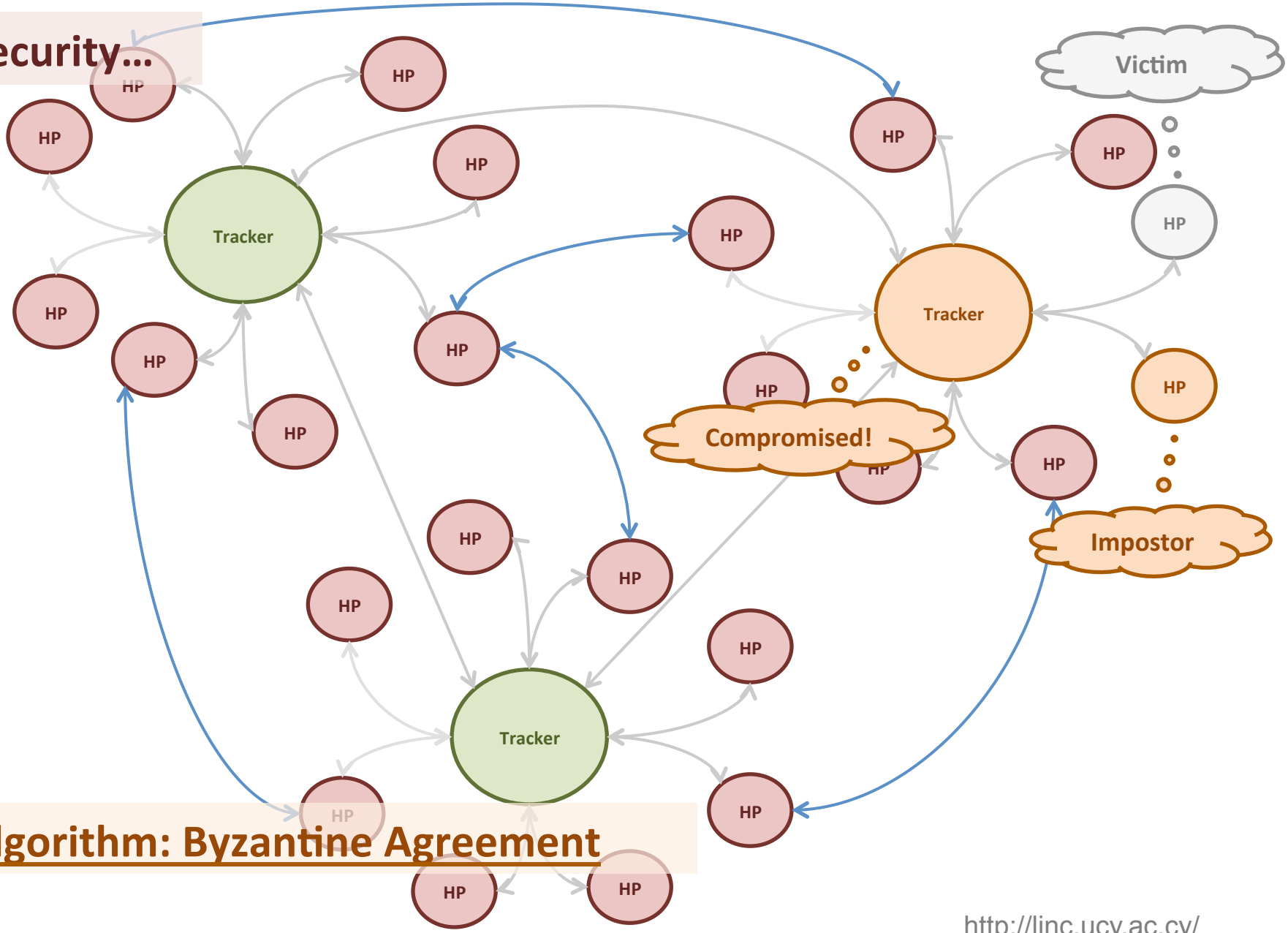
# IDEAS ABOUT SECURITY

# How do we protect the privacy?

- Content encrypted with AES.
- The key is :
  - never stored and
  - supplied at runtime.
- Encryption at end-points.

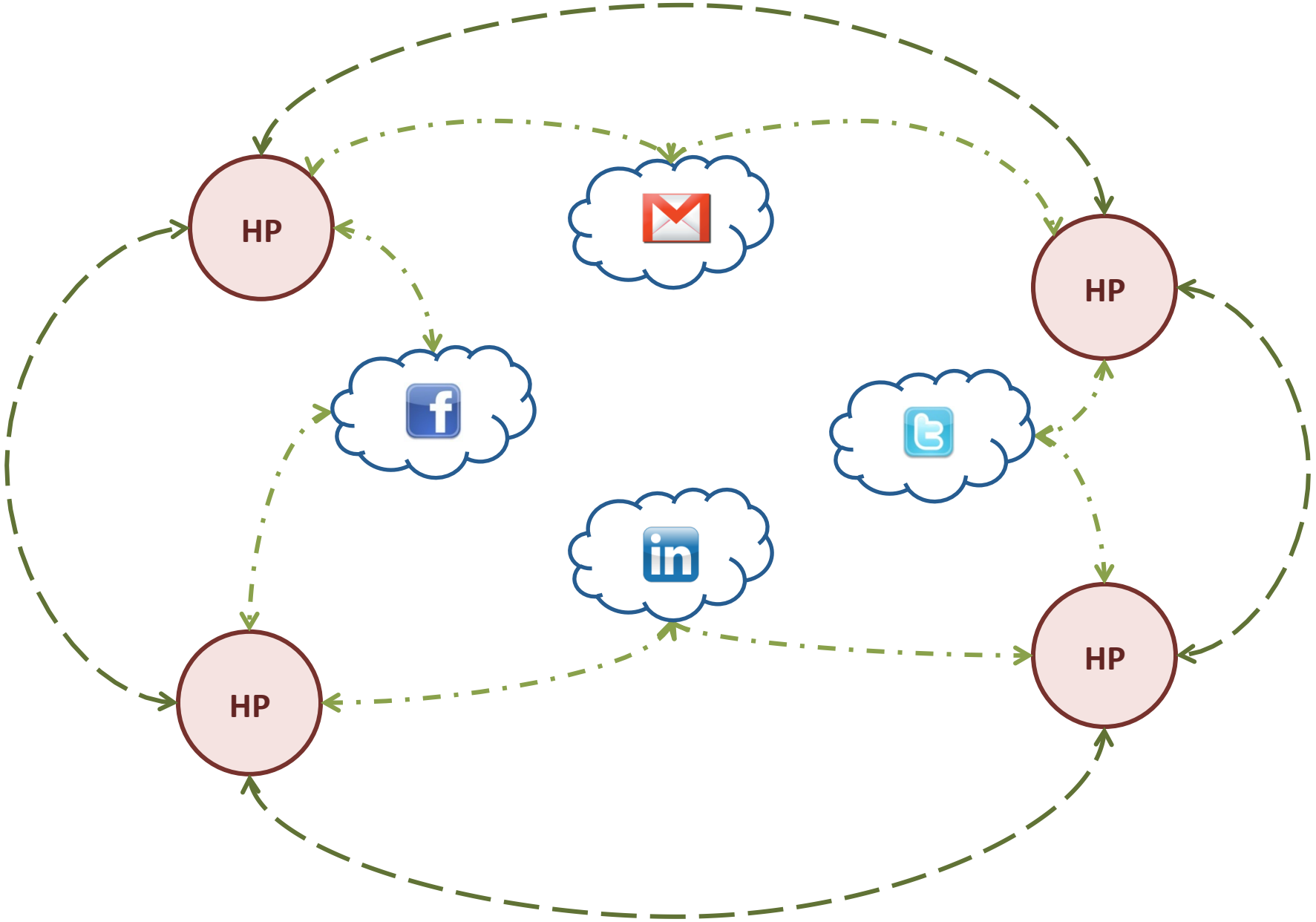

Client
HP
Encrypted data
Linked in
Gmail

# Security…




## Algorithm: Byzantine Agreement

# DATA DISSEMINATION THROUGH ONLINE SERVICES


HP
HP
HP
HP

# IDEAS ABOUT TRACKER AND DISSEMINATION

# Small notifications…

andres.isocial.com.cy — source

1382531430 — Unix timestamp

george.isocial.com.cy, marios.isocial.com.cy, … — List of addressees

{source:andres.isocial.com.cy,timestamp:1382531430,addressees:[,]}

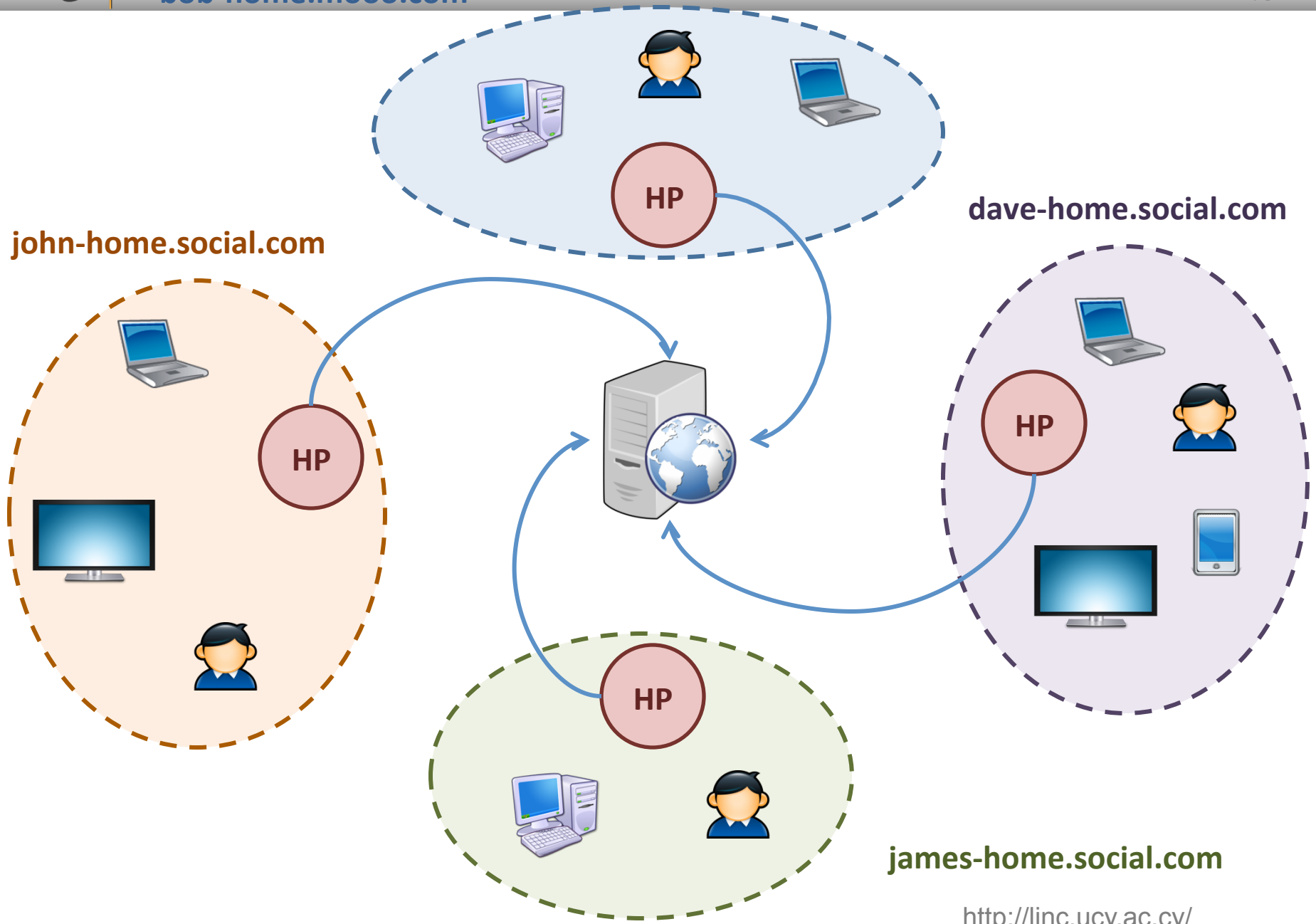
~ 66 bytes

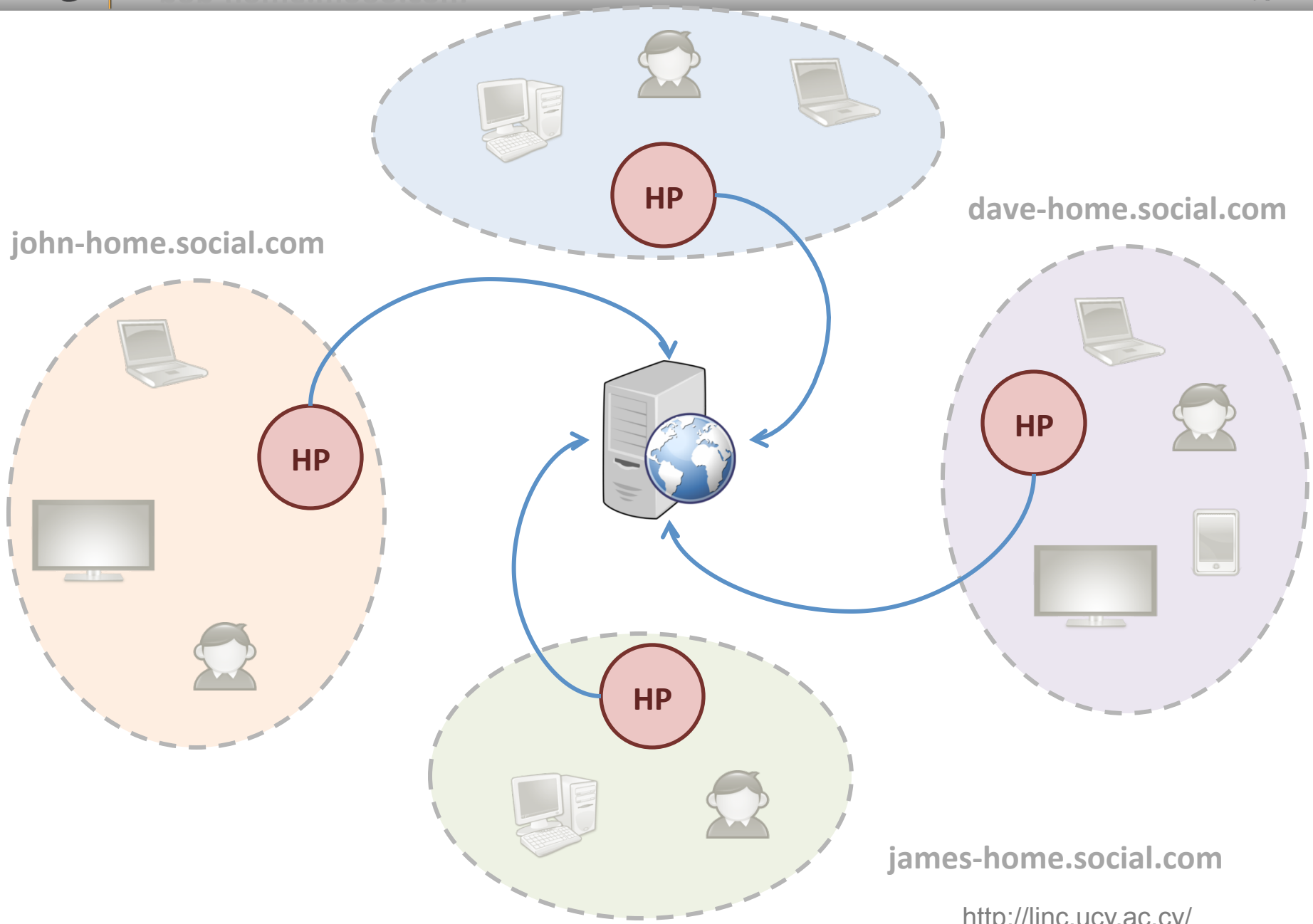
{source:andres.isocial.com.cy,timestamp:1382531430,addressees:[george.isocial.com.eu,]}

~ 87 bytes

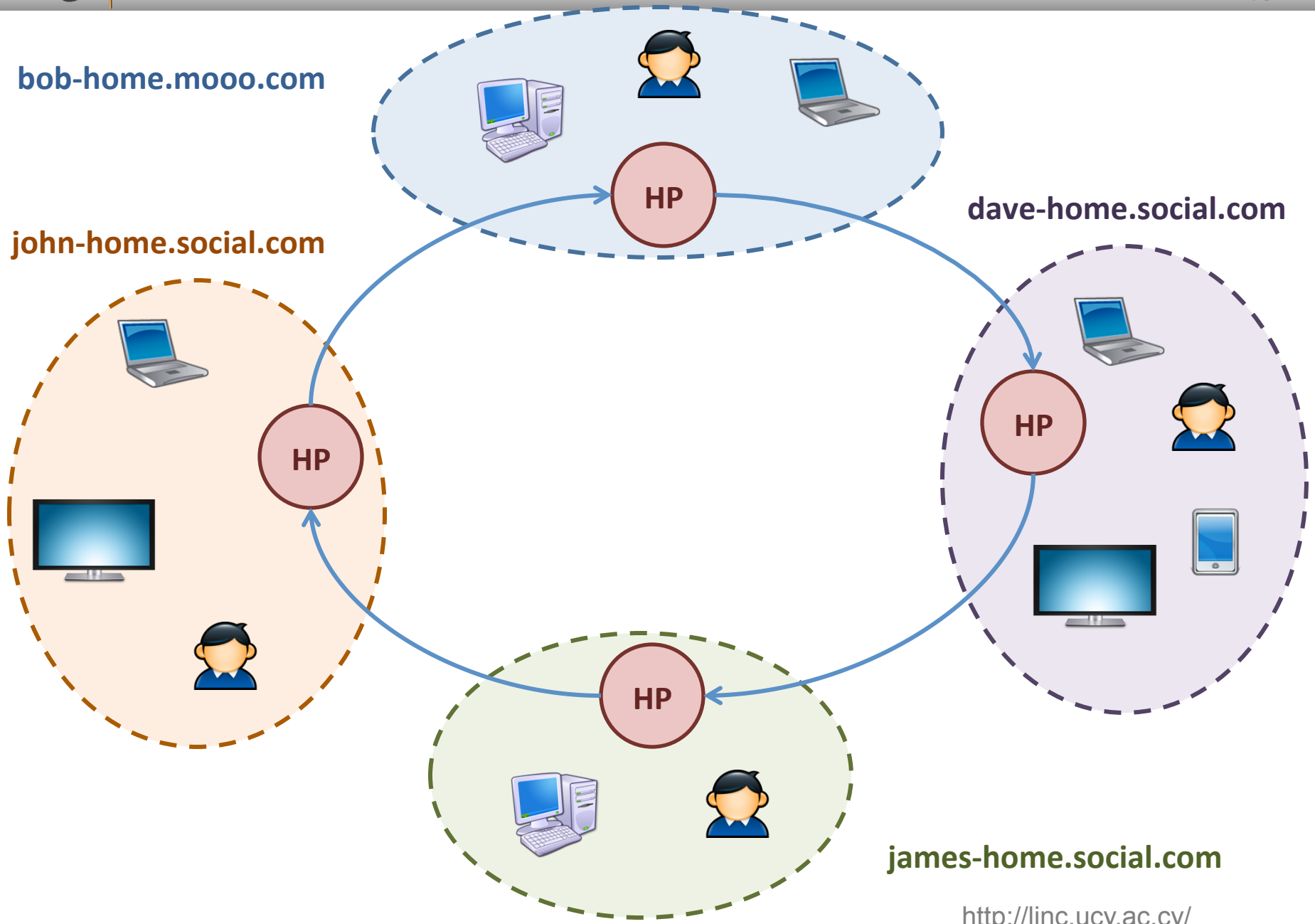
- Roughly 25 bytes per addressee.
- With 729 we have ~17 Kilobytes per notification.
- *( A song in mp3 format is around 3 584 Kilobytes )*

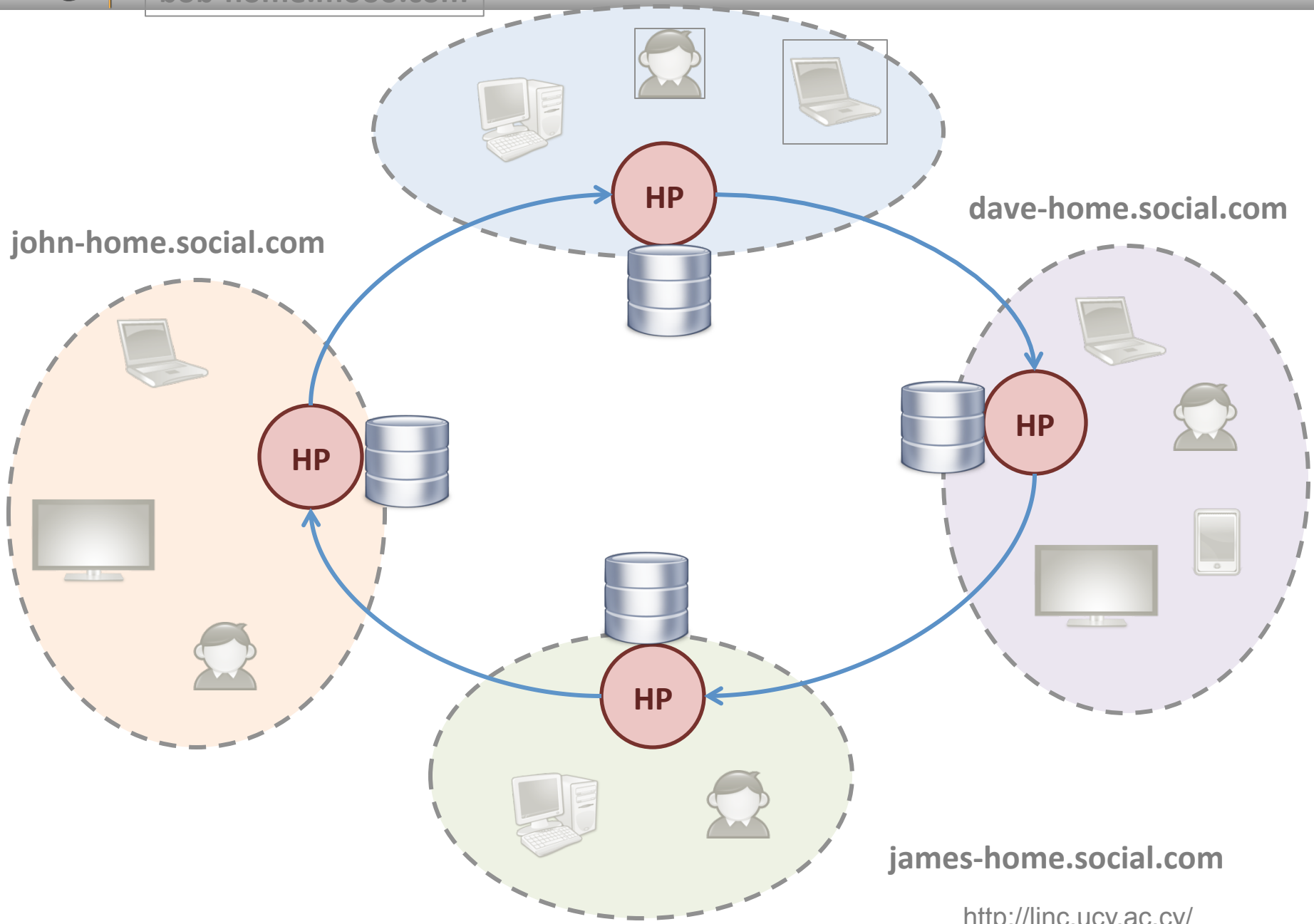
# CENTRAL DIRECTORY SERVICE.


bob-home.mooo.com
HP
john-home.social.com
HP
dave-home.social.com
HP
HP
james-home.social.com

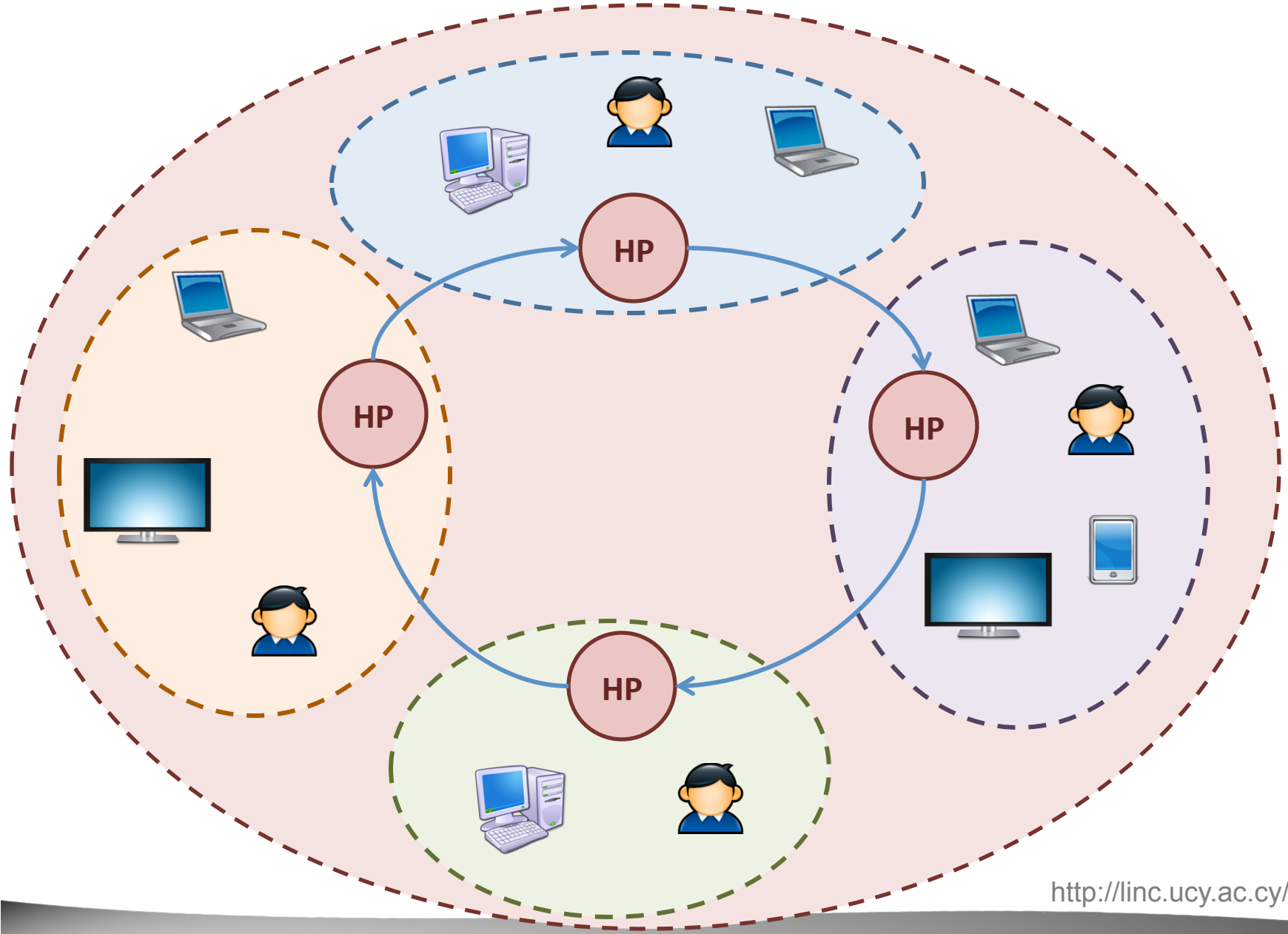

bob-home.mooo.com
HP
dave-home.social.com
john-home.social.com
HP
HP
HP
james-home.social.com

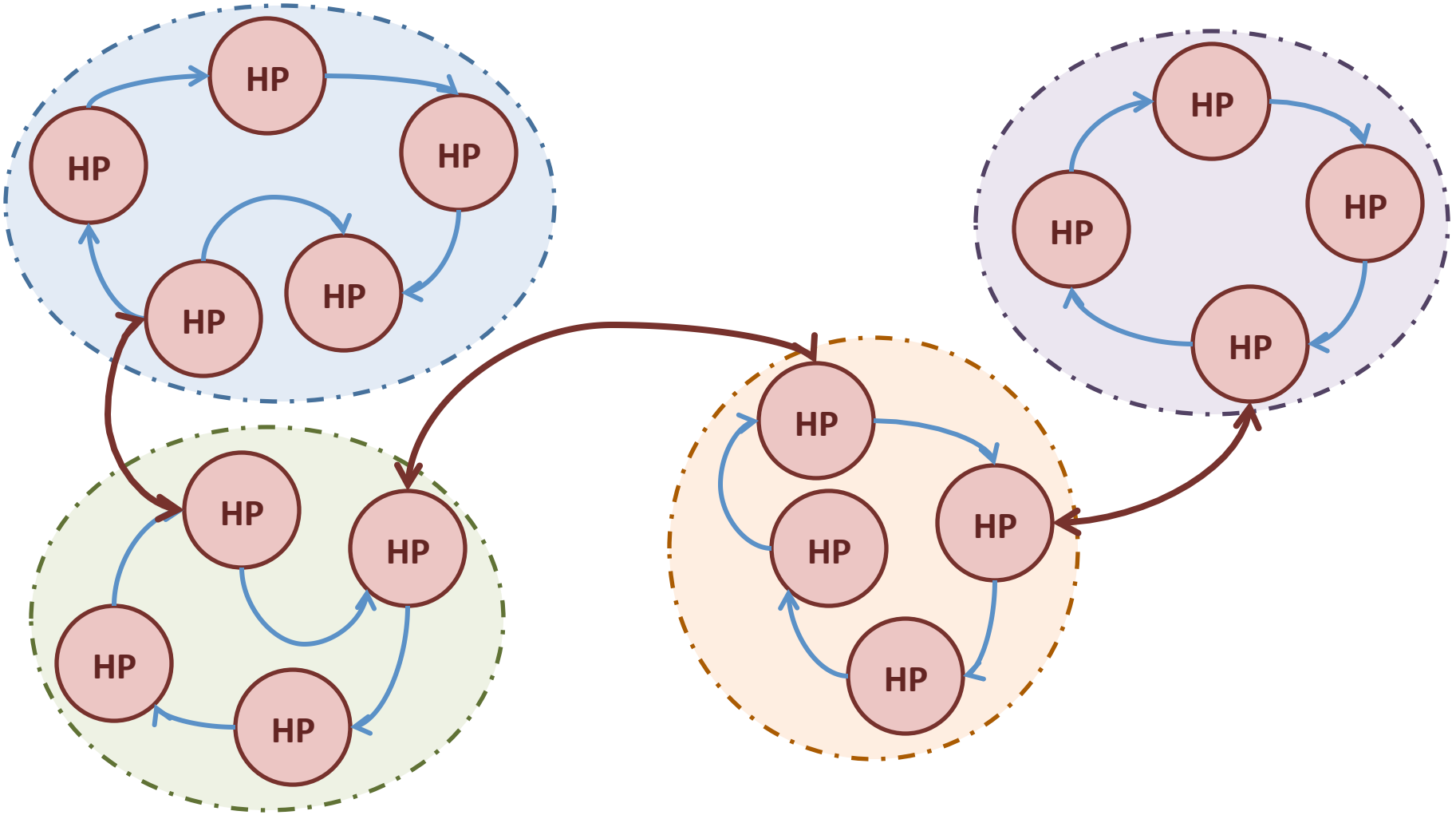
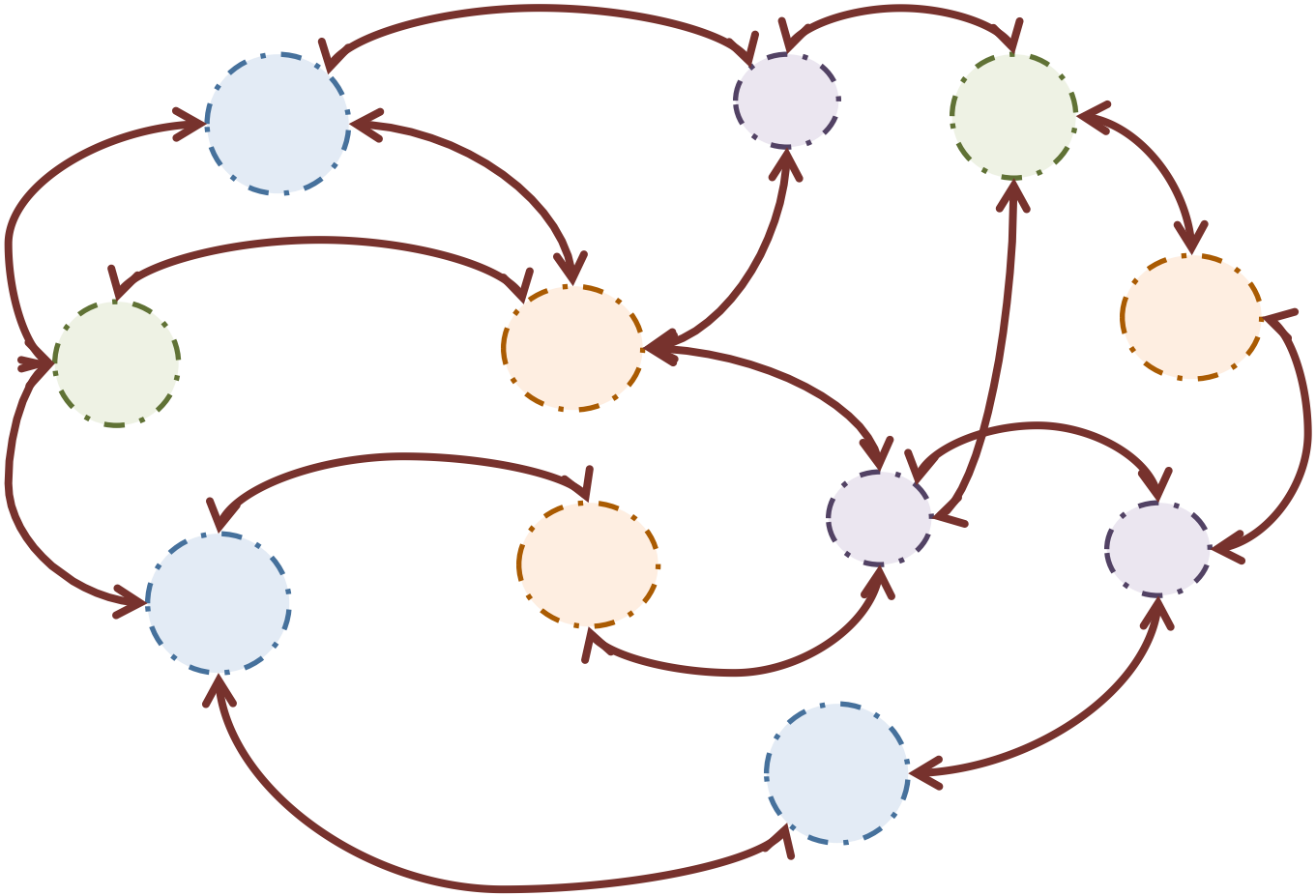
# DIVIDE THE DIRECTORY AMONG THE PEERS.


bob-home.mooo.com
HP
dave-home.social.com
john-home.social.com
HP
HP
HP
james-home.social.com


bob-home.mooo.com
HP
john-home.social.com
dave-home.social.com
HP
HP
HP
james-home.social.com

# EACH PEER HOLDS ITS OWN DIRECTORY.


HP
HP
HP
HP


HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP
HP