

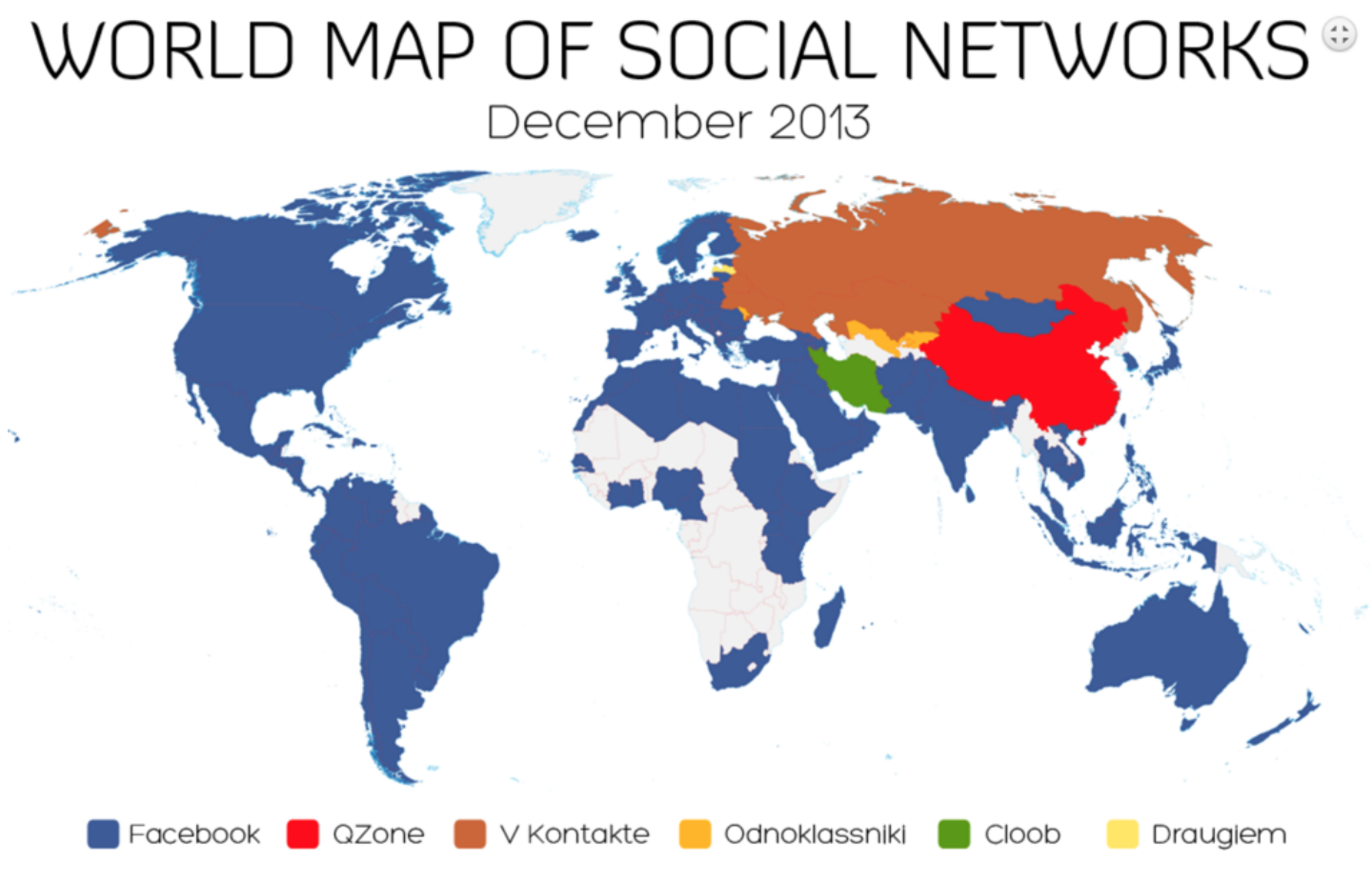
UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Institute of Computer Science
Research Group – Theory of Distributed Systems

A peer to peer Framework for Social Networks

Project Group 2013/2014

Introduction



http://vincos.it/world-map-of-social-networks

Introduction

Issues with current Social Networks

- Centralized - High server maintenance cost
- Security - no Privacy and Protection from massive data-mining
- Single point(s) of failure



Introduction

Issues with current Social Networks



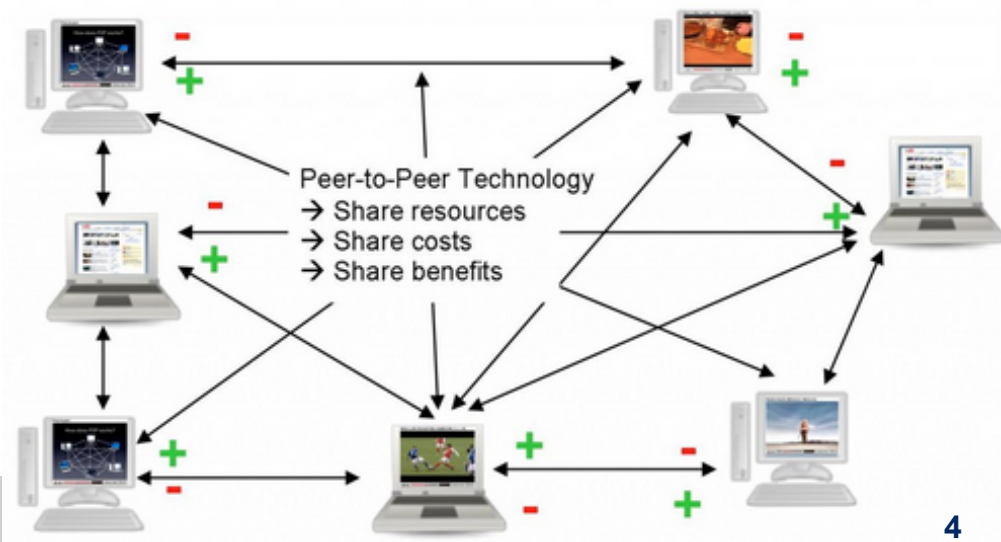
http://swiss-lupe.blogspot.de/2013/07/prism-und-nsa-sei-dank-mein-papi-ist.html

Introduction

Solution: Peer-to-Peer (P2P) Framework



- No server needed - distributed storage
- Data is encrypted **before** it is sent across the network
- Controlled access to data items
- Usable in oppressed countries
- Fault tolerant



Contents

1. LifeSocial - Overview and Results

1.1. Overlay

1.2. Framework

1.3. Plugins and GUI

2. Testing

3. Conclusion

4. Further Steps

Overview of LifeSocial

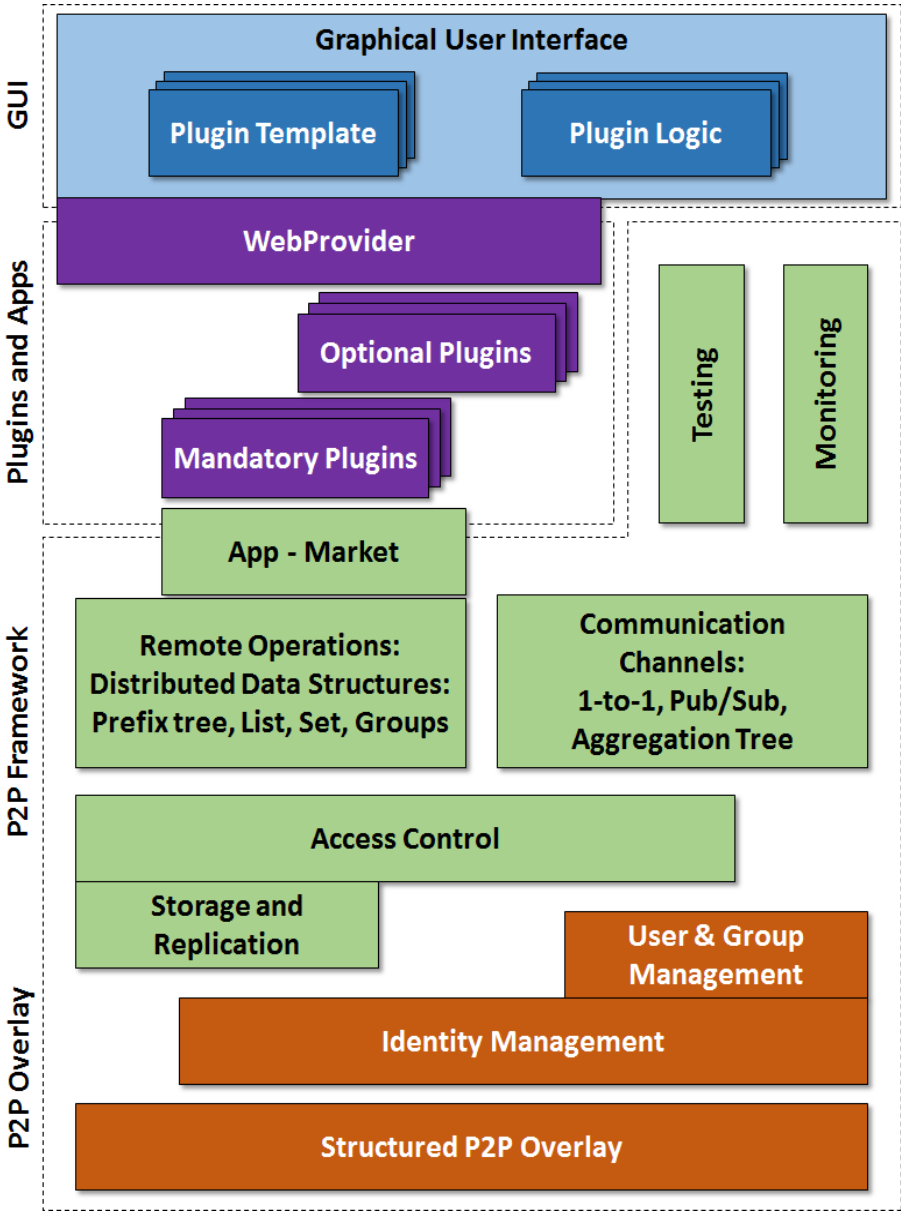


LifeSocial

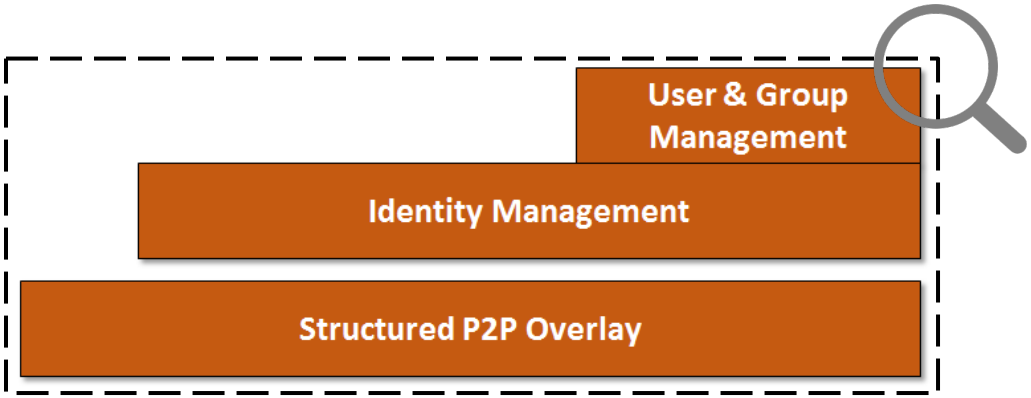
- A social network
- Based on our P2P Framework
- No central servers required
- Use of standard technologies:
  - HTML5
  - AJAX
  - jQuery

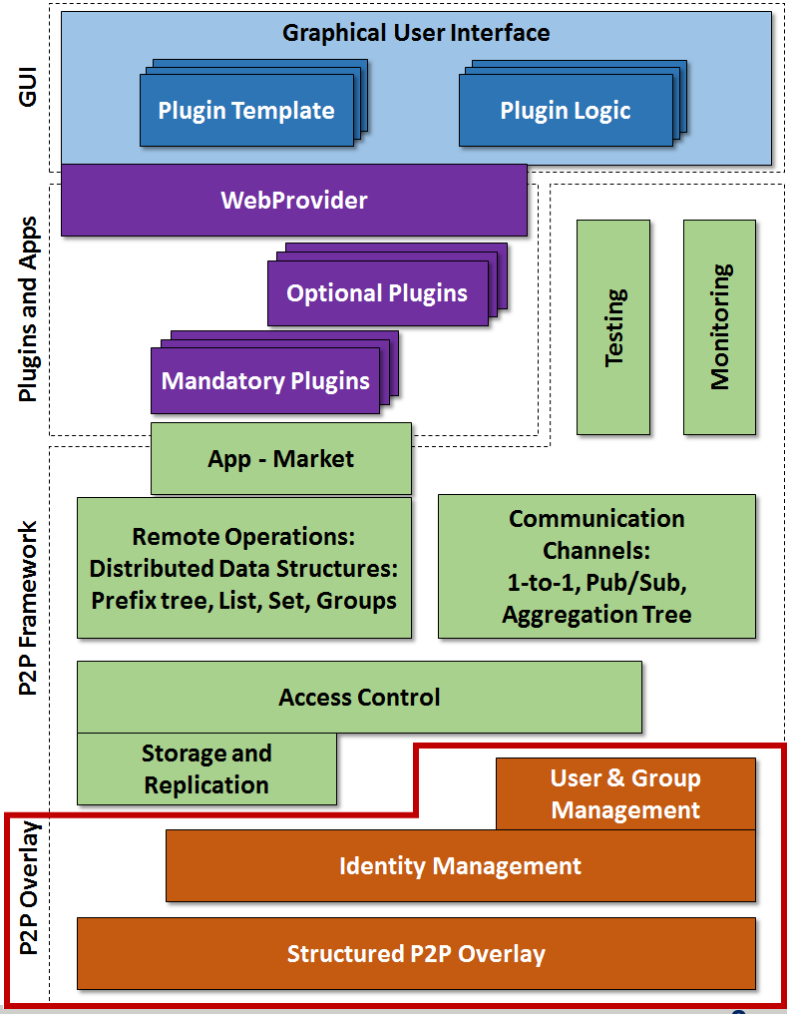
Overview of LifeSocial





1.1 Overlay

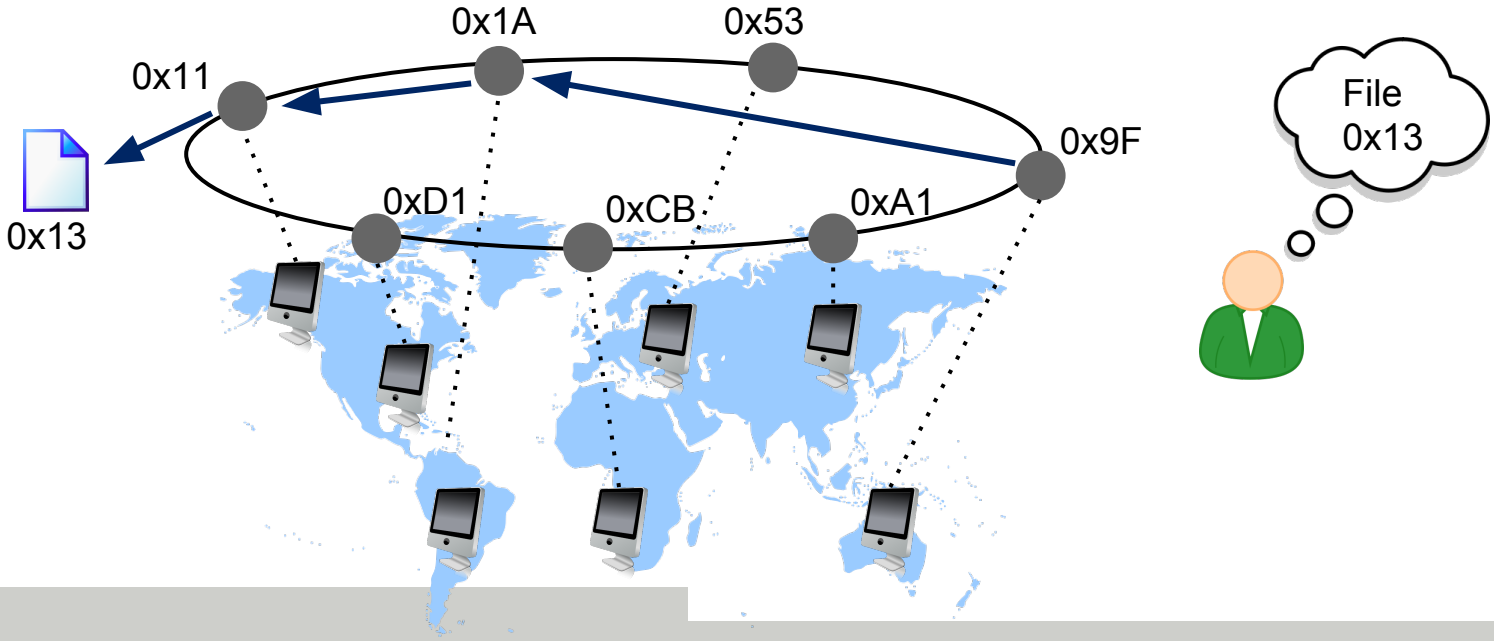

User & Group Management
Identity Management
Structured P2P Overlay


GUI
Graphical User Interface
Plugin Template
Plugin Logic
Plugins and Apps
WebProvider
Optional Plugins
Mandatory Plugins
Testing
Monitoring
App - Market
P2P Framework
Remote Operations: Distributed Data Structures: Prefix tree, List, Set, Groups
Communication Channels: 1-to-1, Pub/Sub, Aggregation Tree
Access Control
Storage and Replication
P2P Overlay
User & Group Management
Identity Management
Structured P2P Overlay

The Overlay

Pastry:

- Computers form a logical ring (the overlay)
- Each user and each item has an unique ID
- ID-based Routing is used (logarithmic many steps)



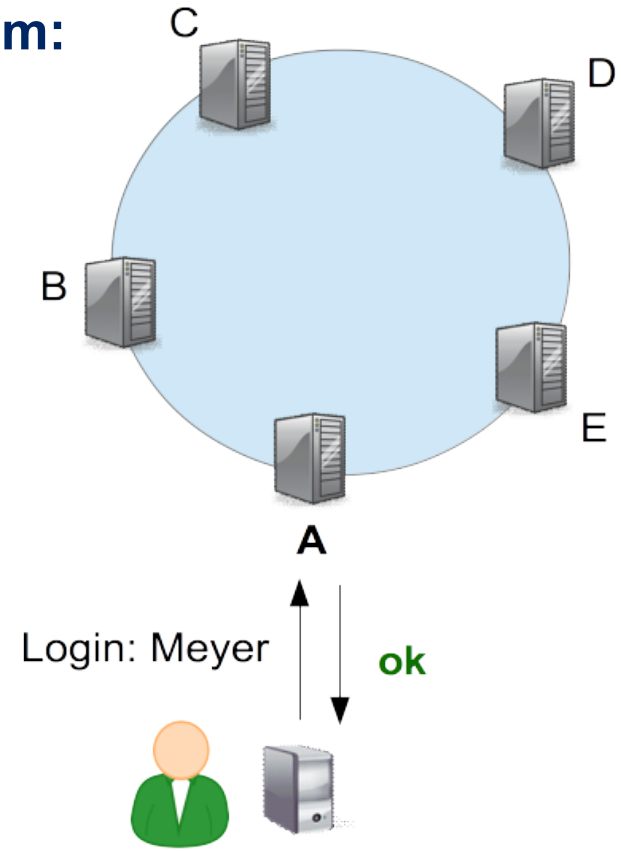
Overlay - Rings

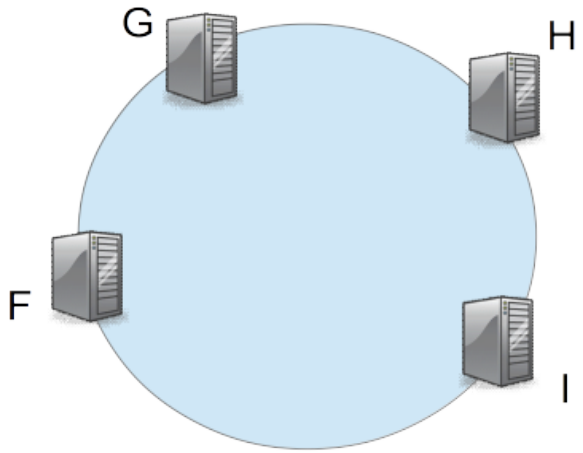
Issues so far:

- User has to know a node to boot each time he logs in
- User does not know to which ring he connects
- There is no possibility to distinguish between rings

Overlay - Rings

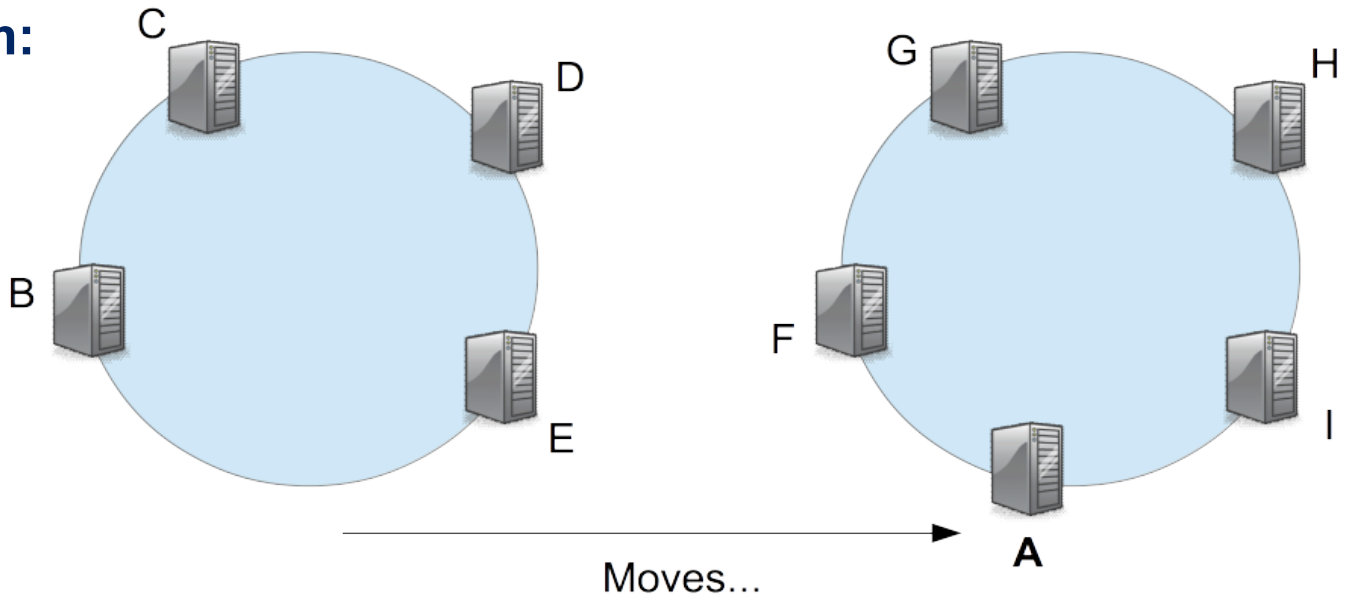
Problem:





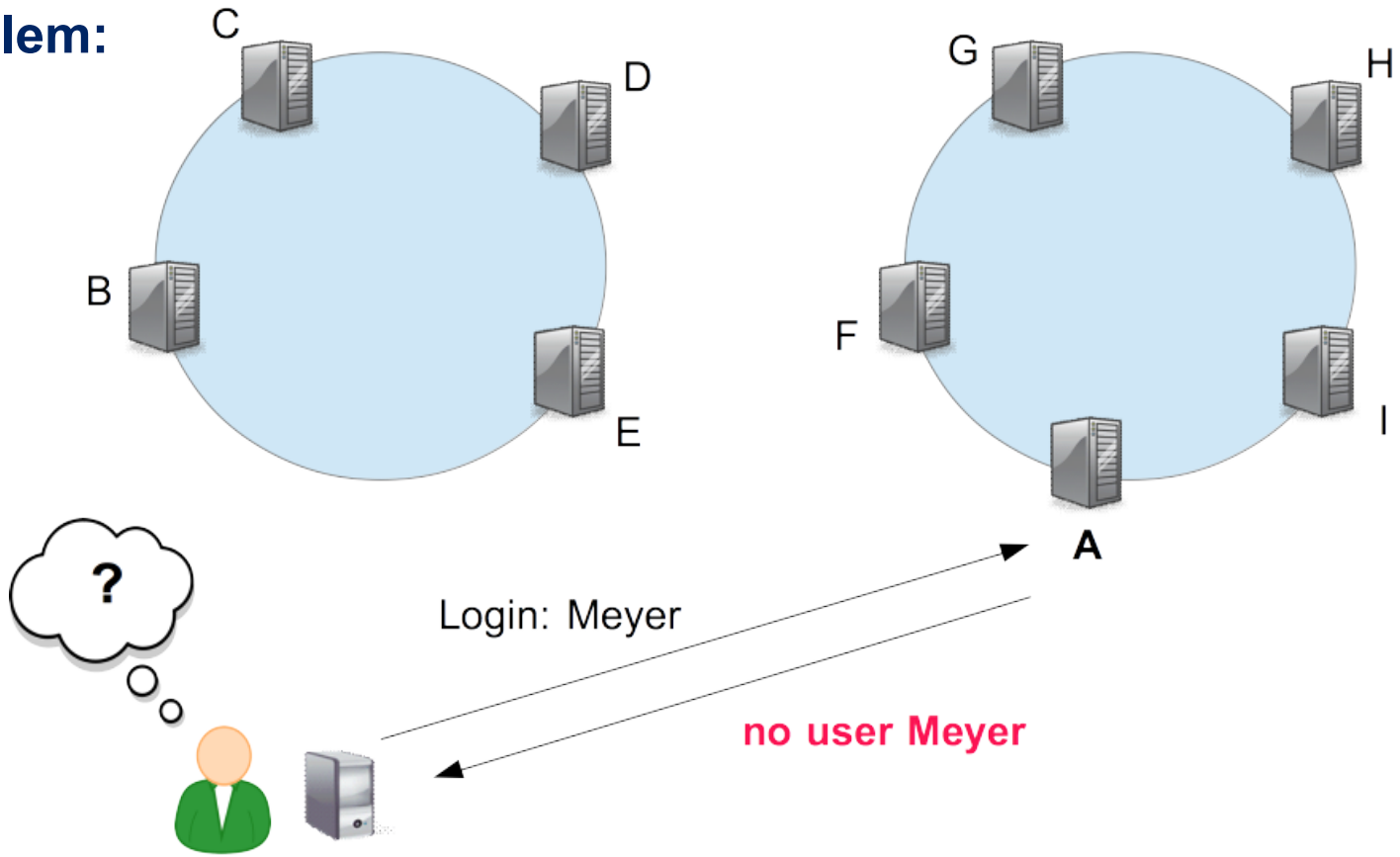
Overlay - Rings

Problem:



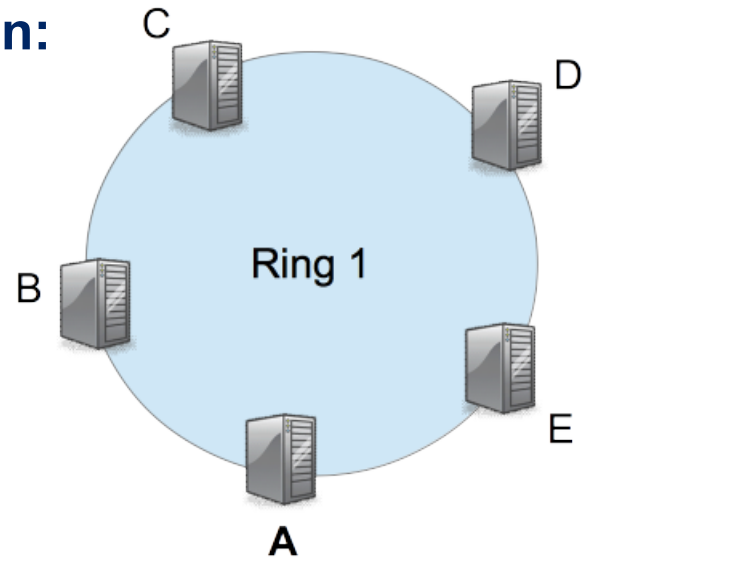
Overlay - Rings

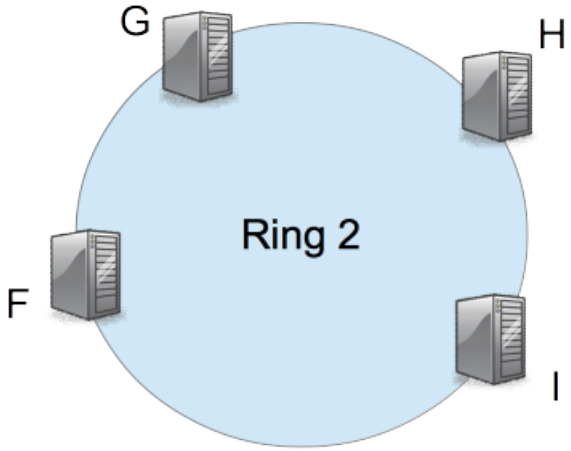
Problem:



Overlay - Rings

Solution:

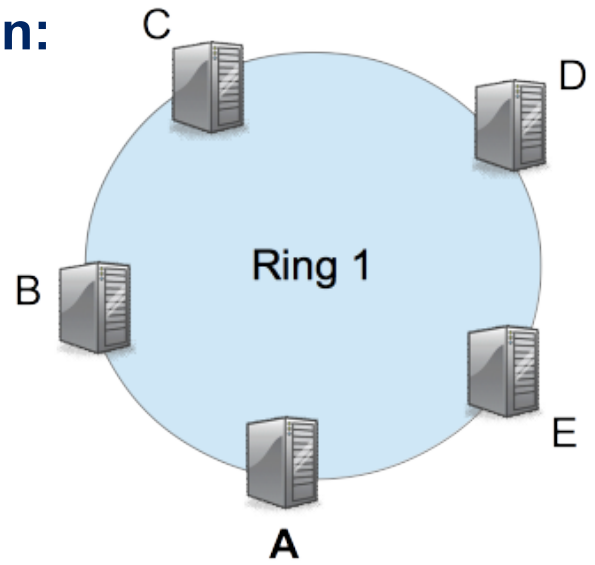


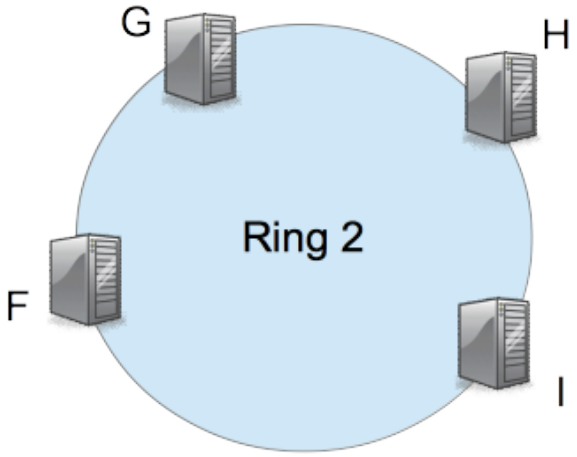




Overlay - Rings

Solution:



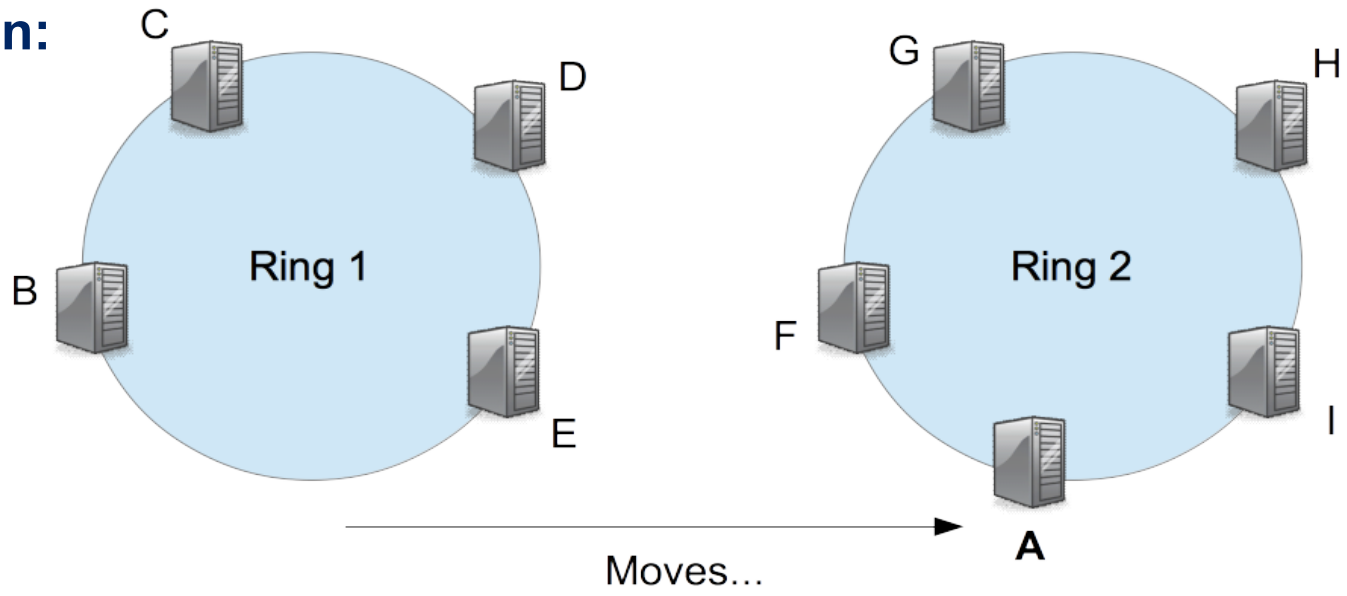




Local Bootstrap Cache:
A
B
C

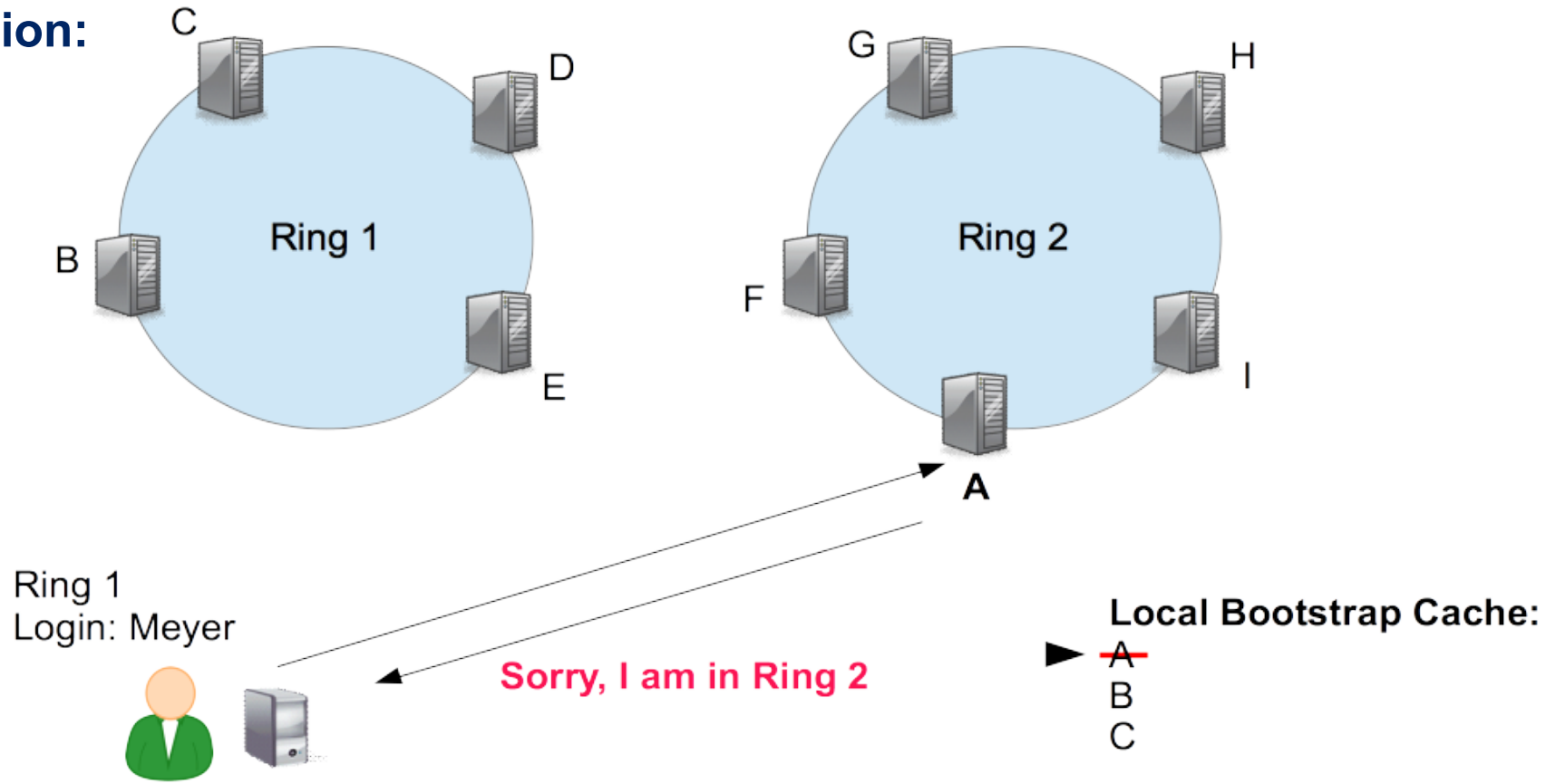
Overlay - Rings

Solution:



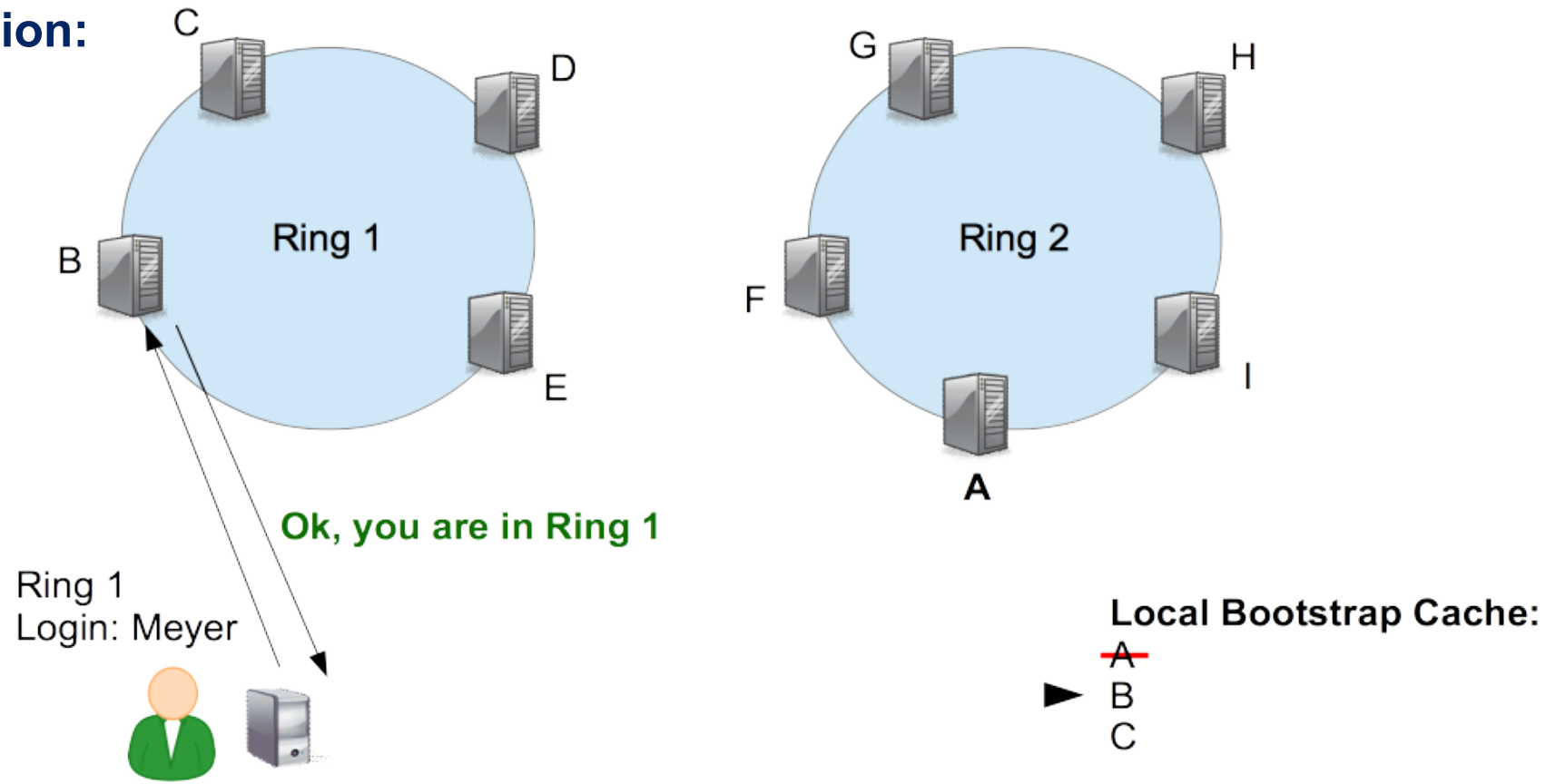
Overlay - Rings

Solution:



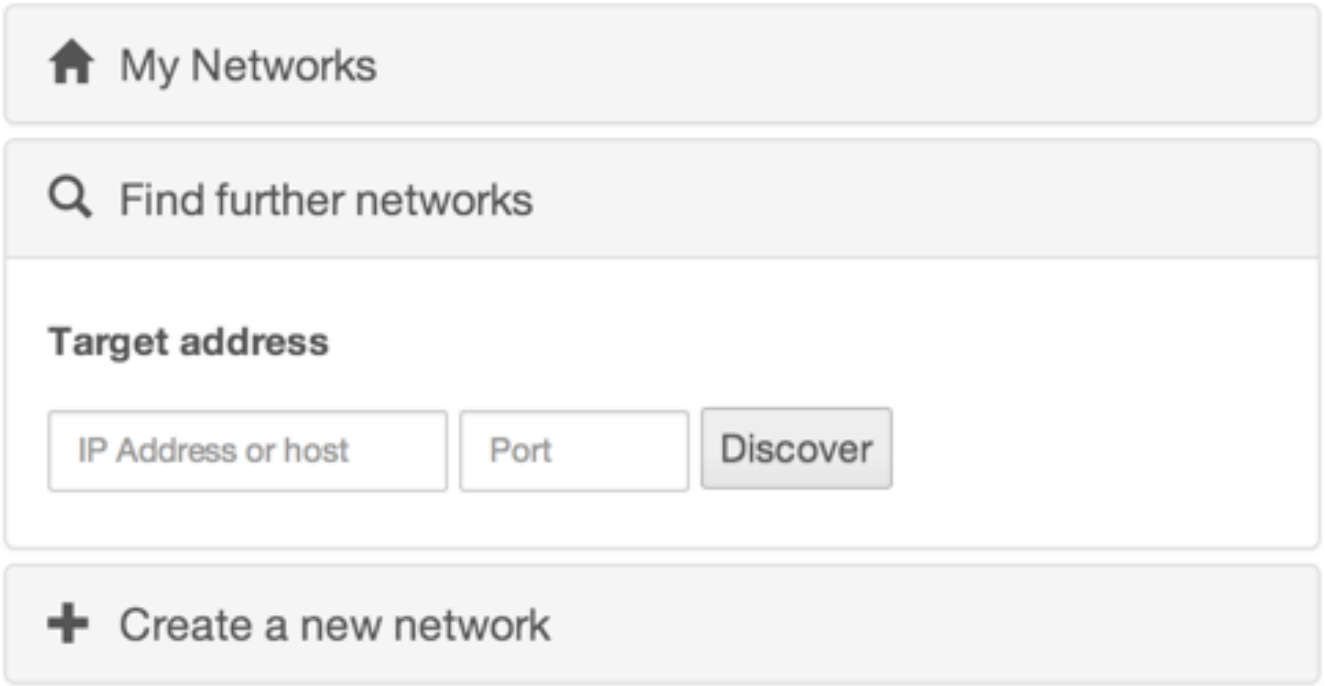
Overlay - Rings

Solution:



Overlay - Rings

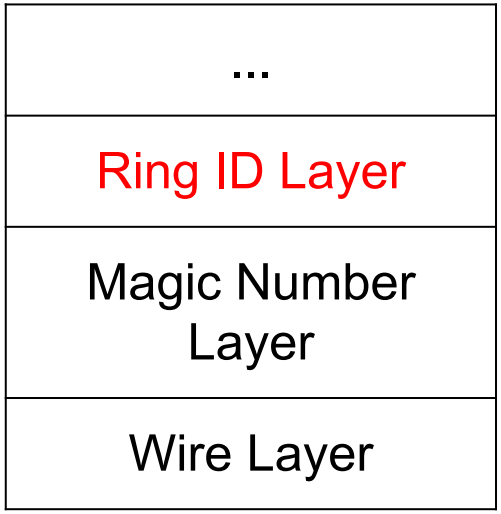
Use Cases:



Overlay - Rings

Changes to Free Pastry:

new Transport Layer:



new Ring Manager:

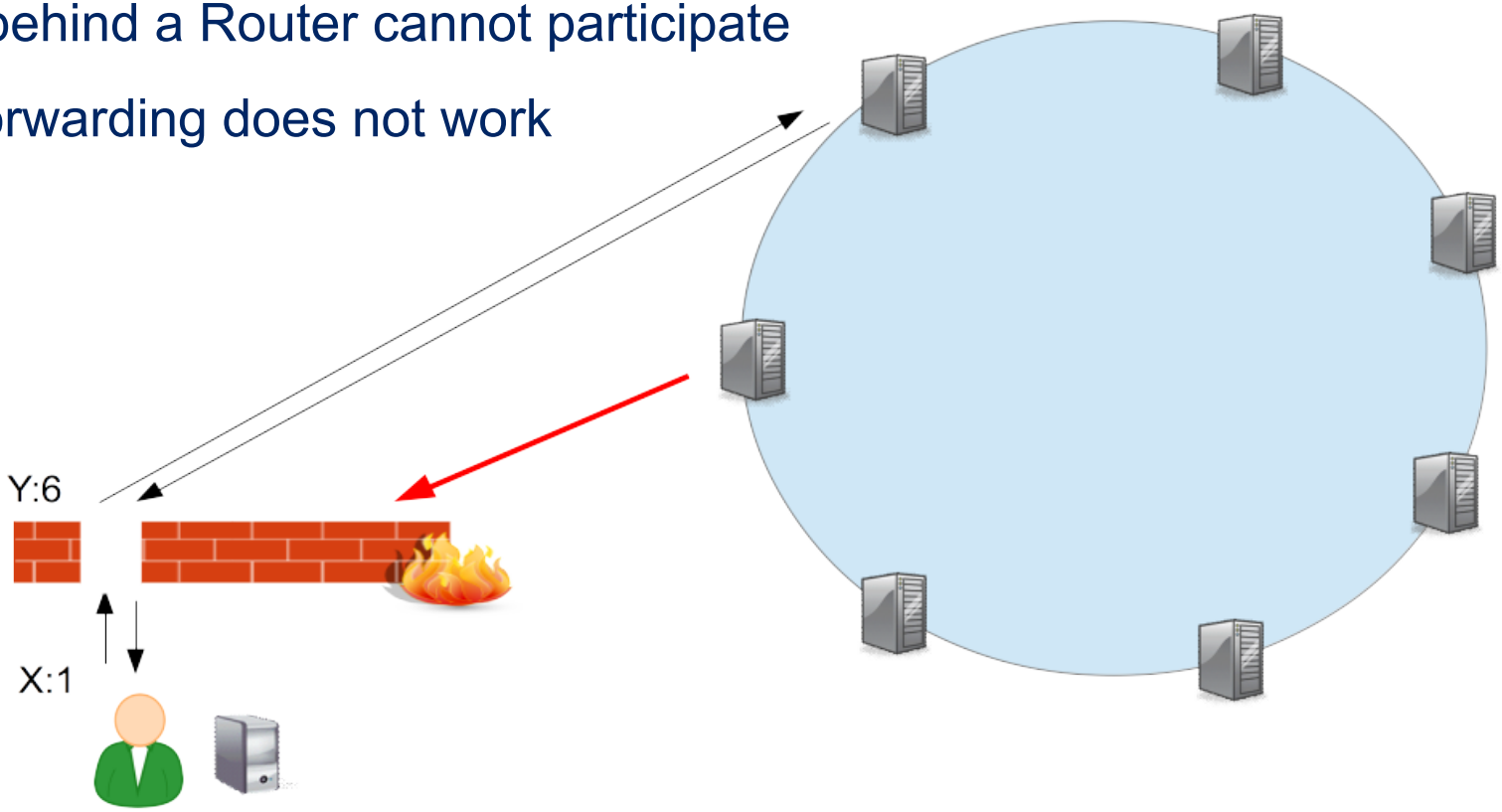
- stores discovered Rings
- Caches addresses of online nodes

discover()
checkMessageHeader()

Overlay - NAT

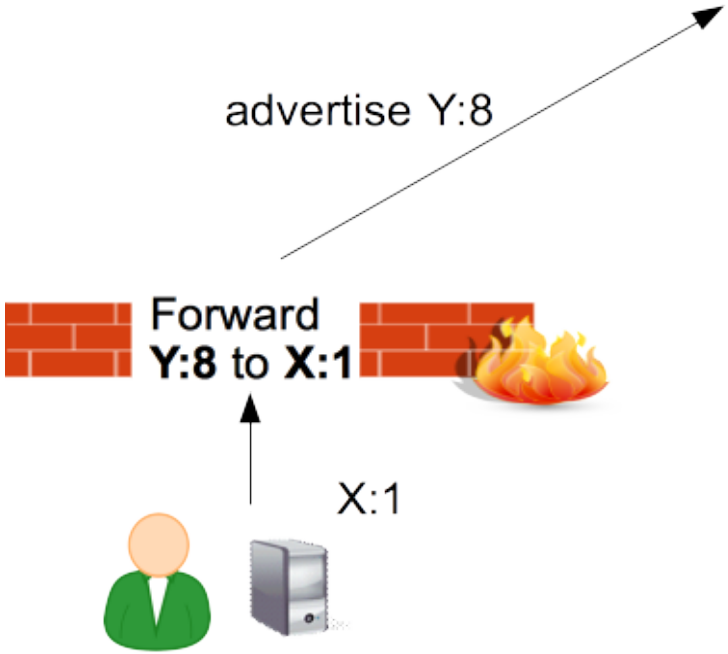
Issues so far:

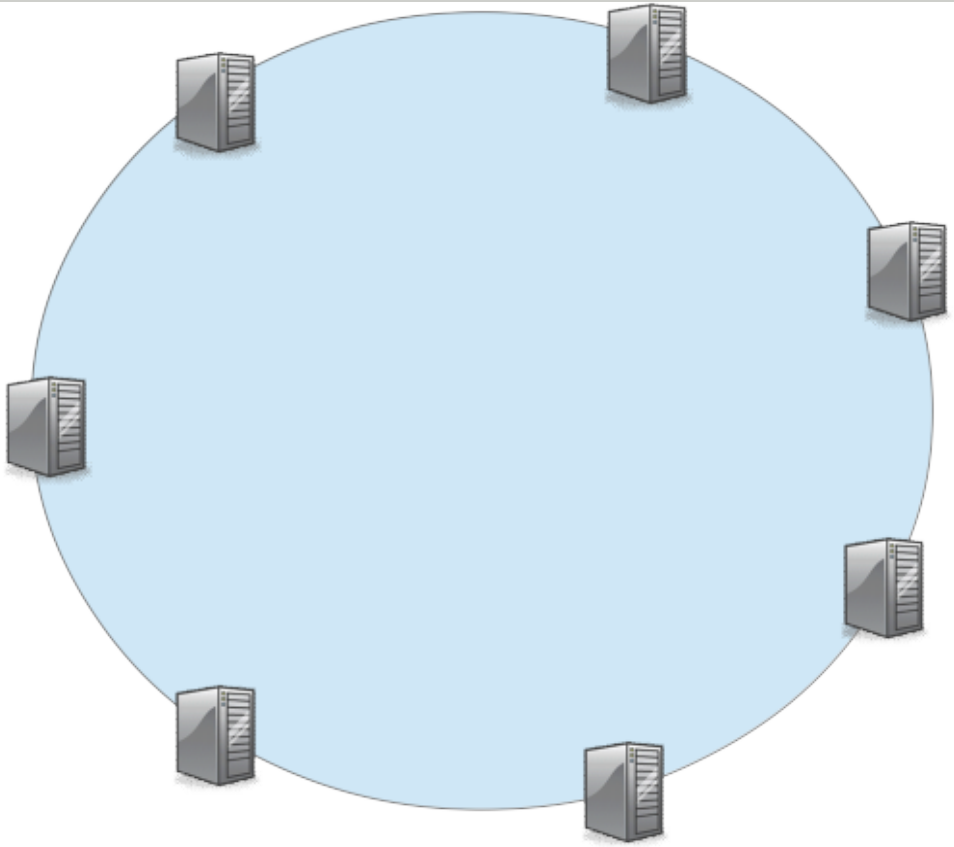
- Hosts behind a Router cannot participate
- Port Forwarding does not work



Overlay - NAT

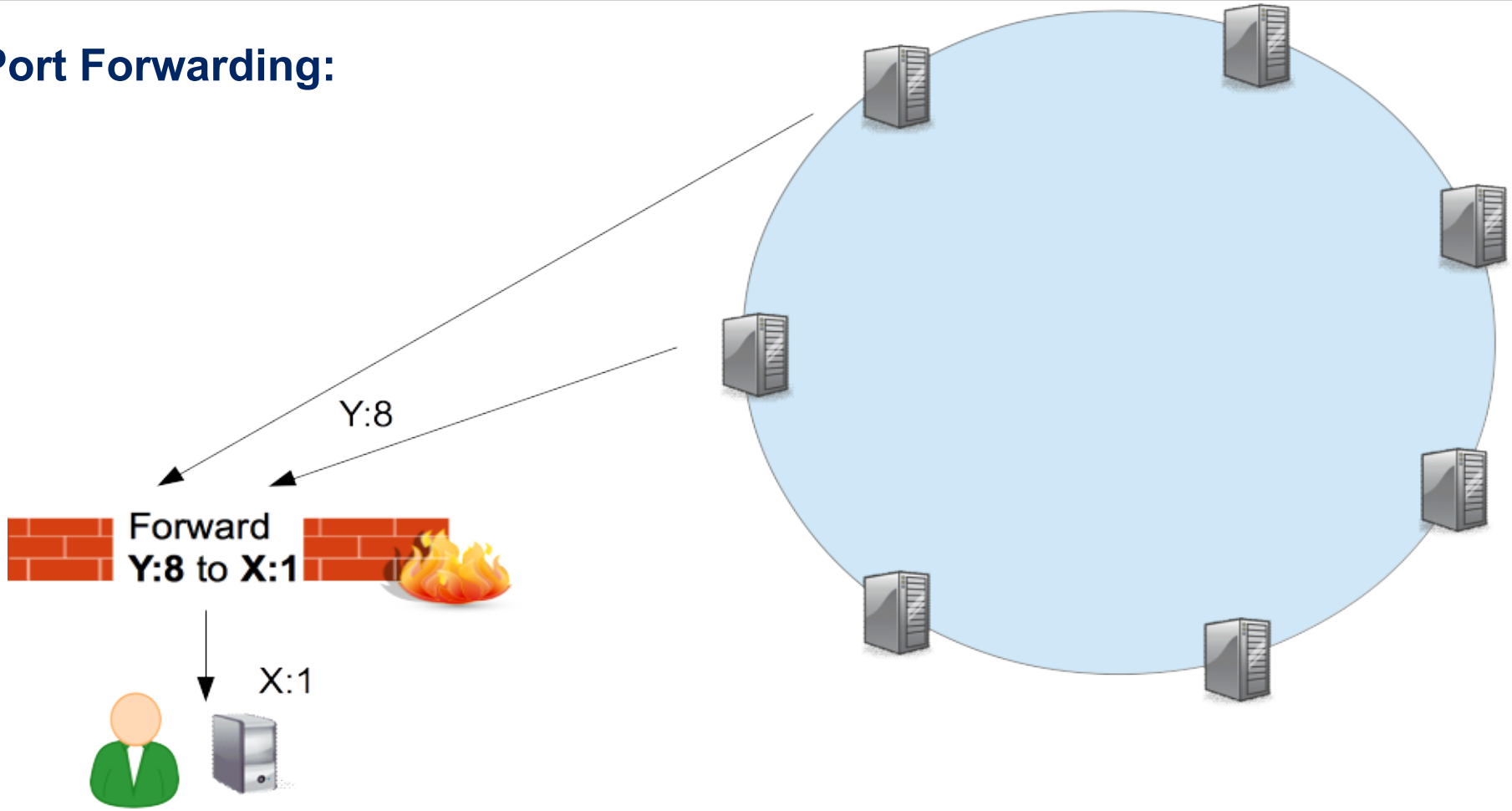
Port Forwarding:





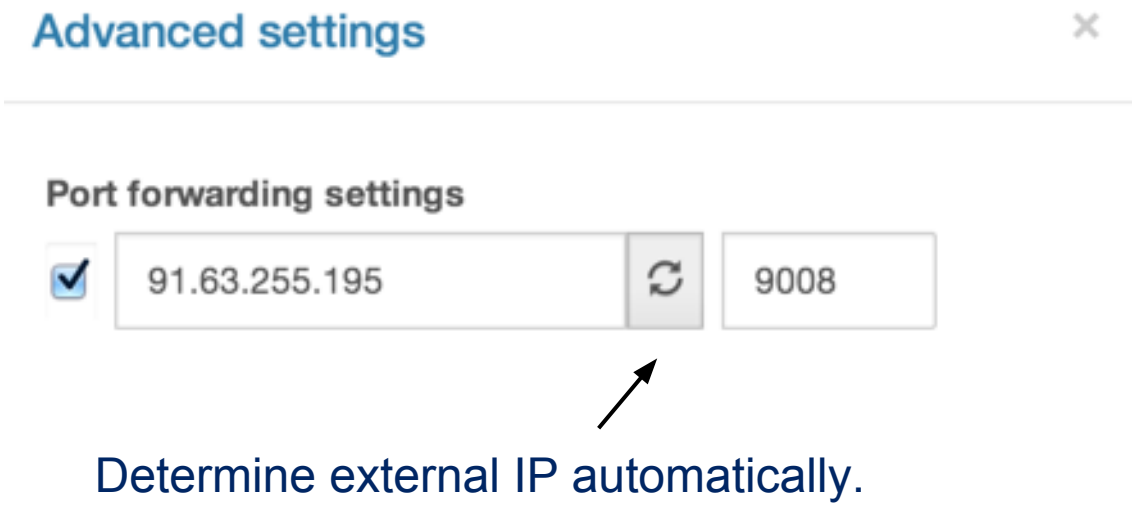
Overlay - NAT

Port Forwarding:



Overlay - NAT

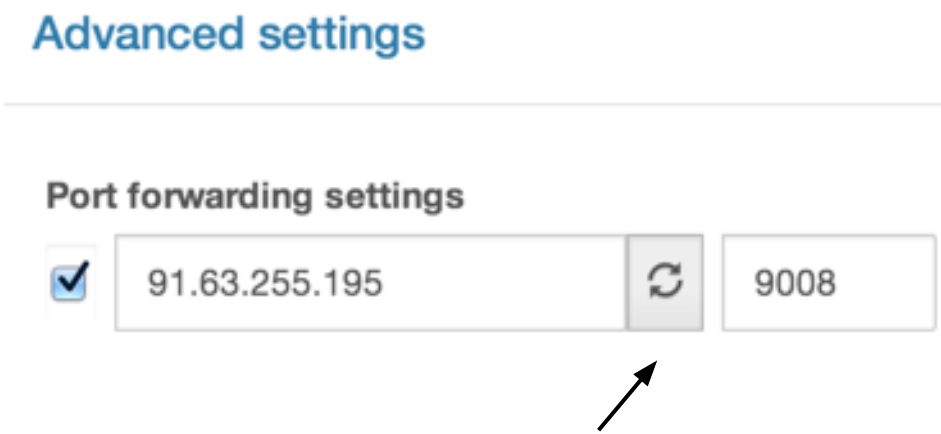
Port Forwarding:



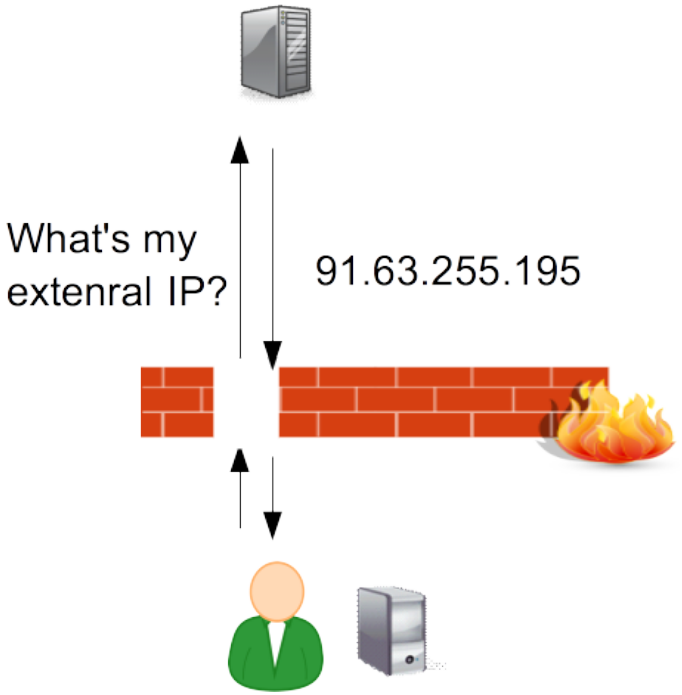
Determine external IP automatically.

Overlay - NAT

Port Forwarding:

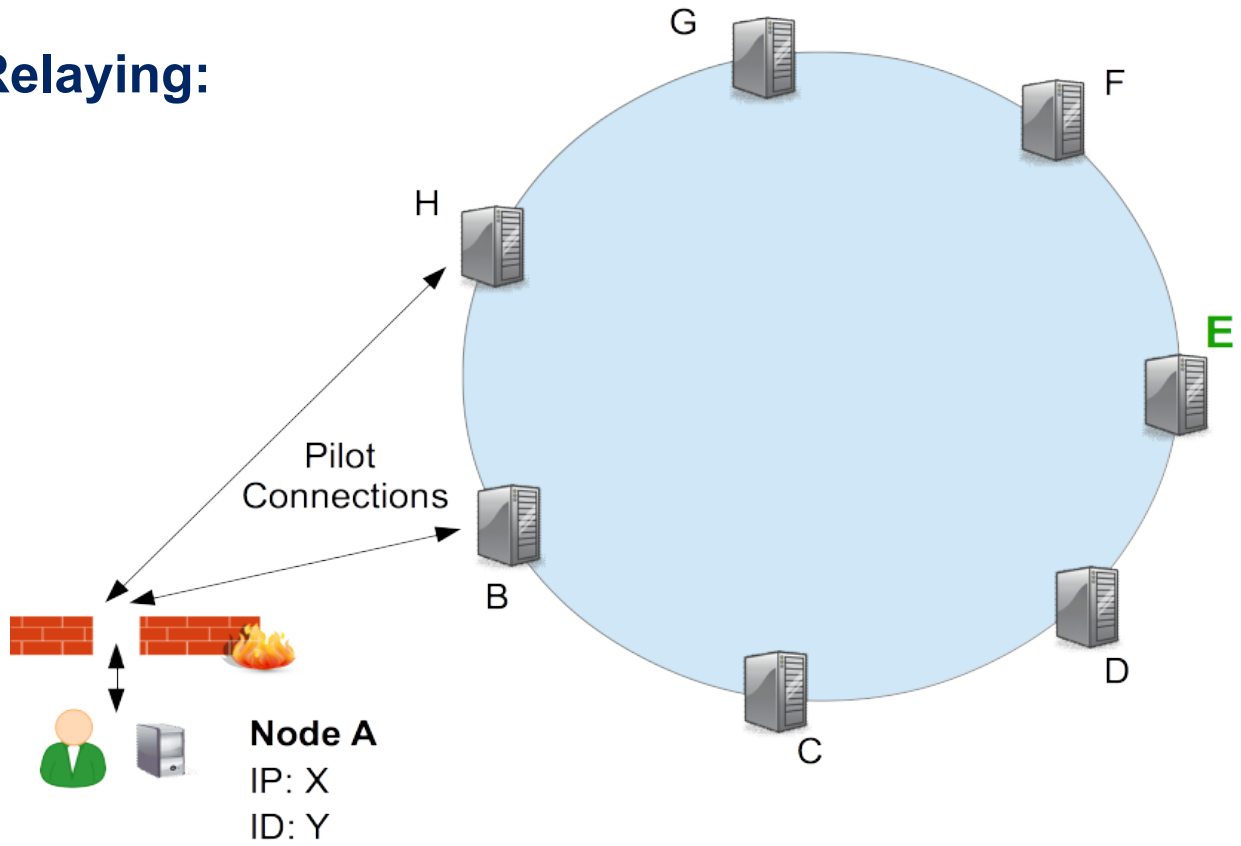


Determine external IP automatically.



Overlay - NAT

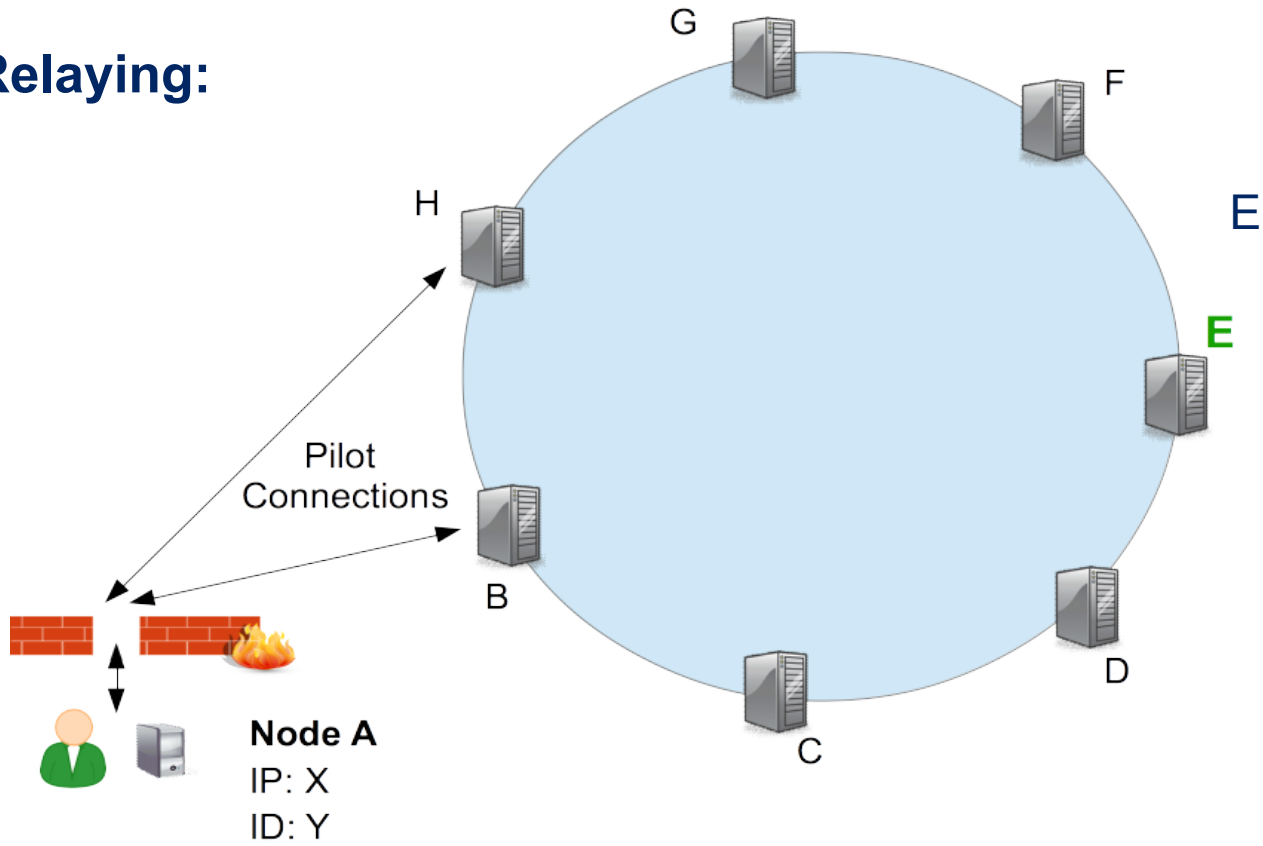
Relaying:



A establishes Pilot connections to **public** leafs...

Overlay - NAT

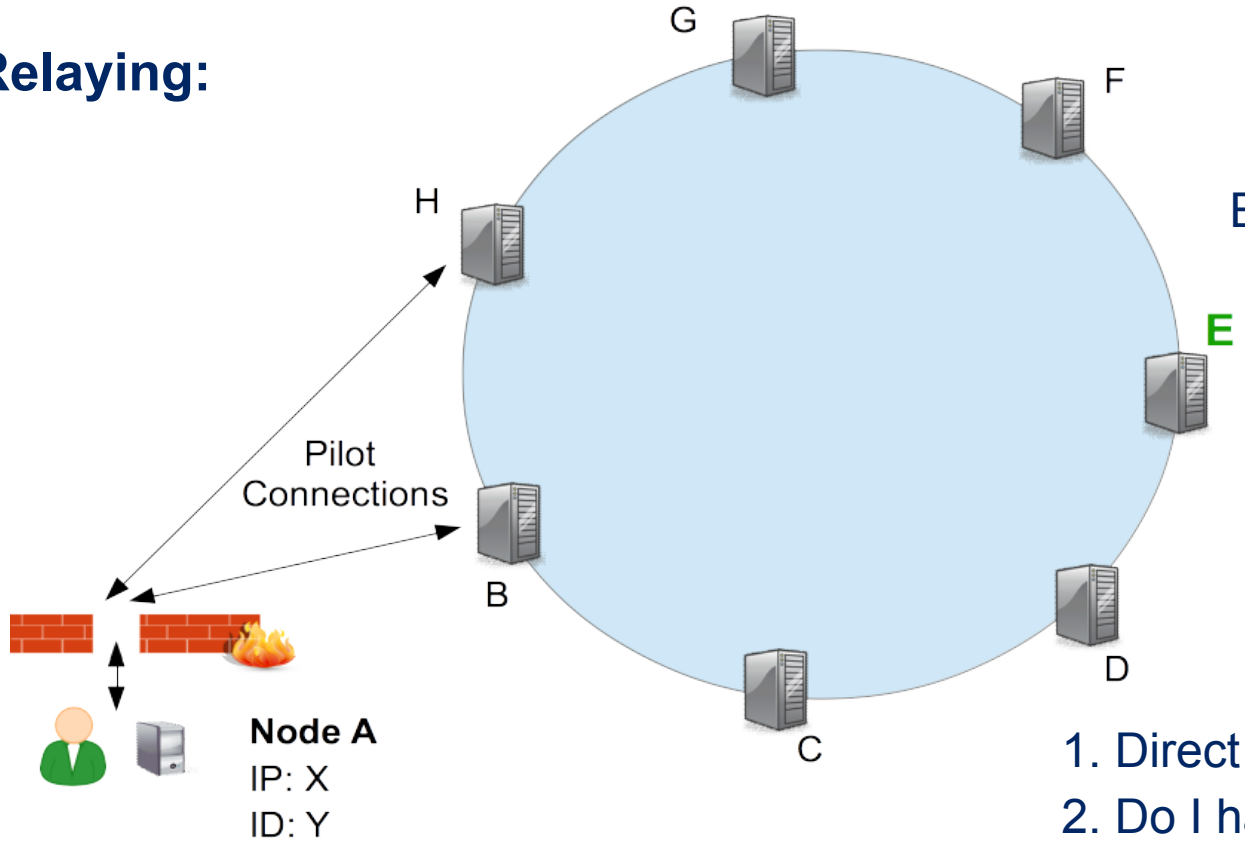
Relaying:



E wants to connect to A....

Overlay - NAT

Relaying:

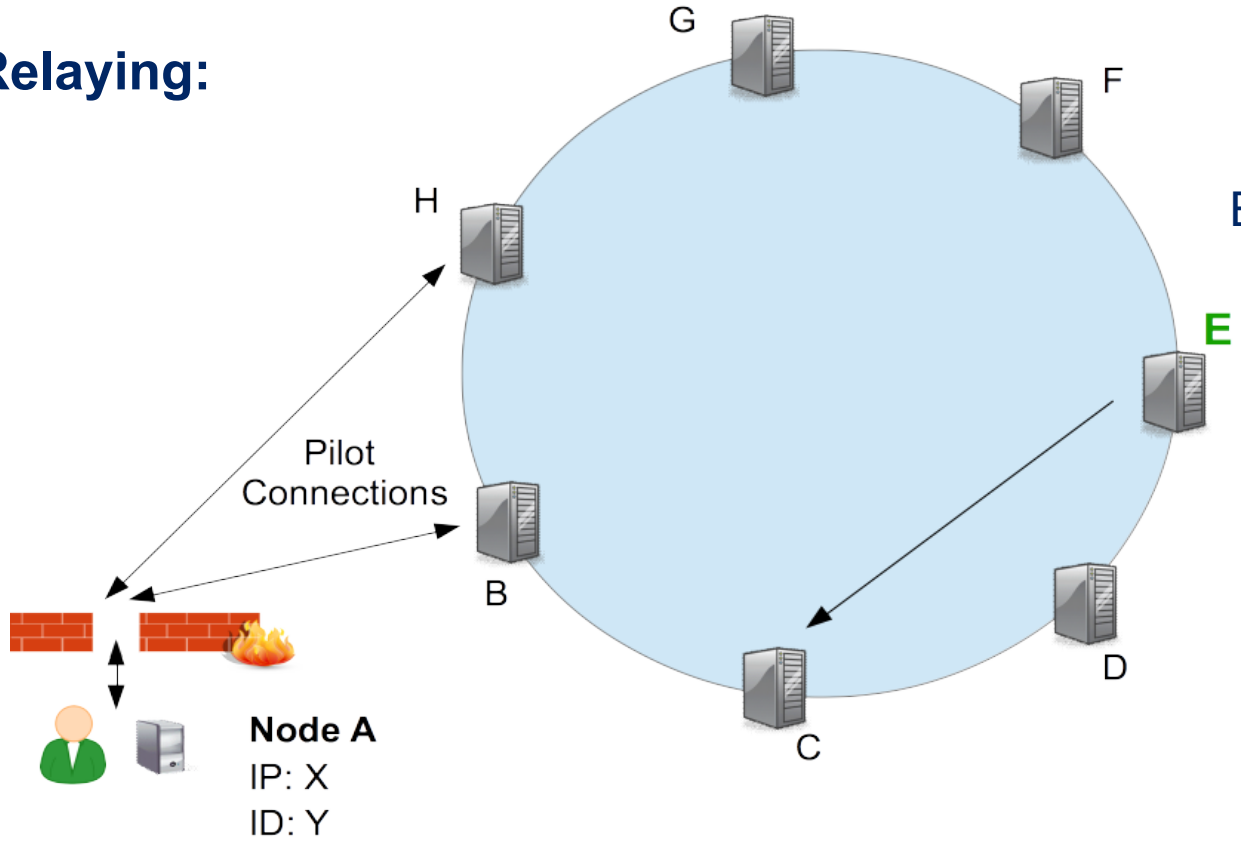


E wants to connect to A....

1. Direct connection possible?
2. Do I have a Pilot to A?
3. Has a leaf of mine a Pilot to A?
4. **Use Pastry Routing to ID Y**

Overlay - NAT

Relaying:

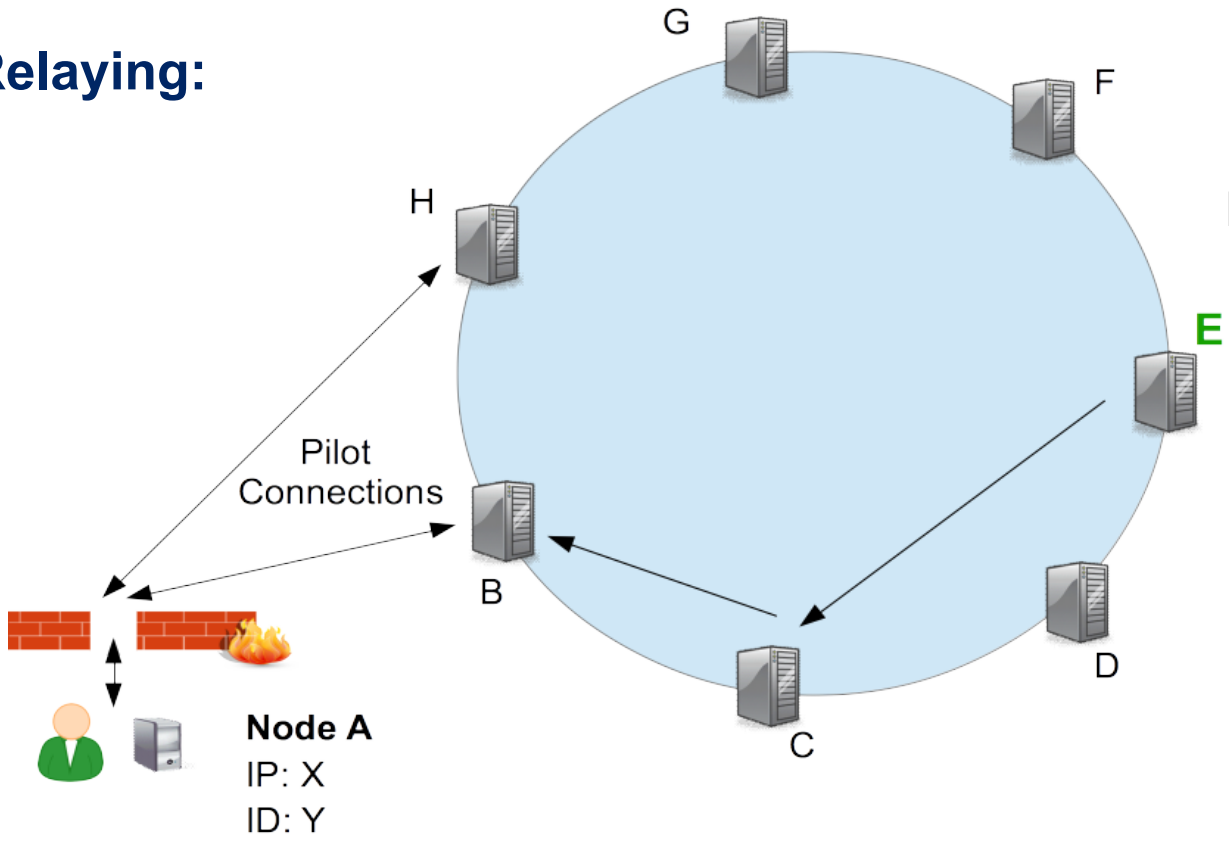


E wants to connect to A....

Non-reachable nodes skipped when routing...

Overlay - NAT

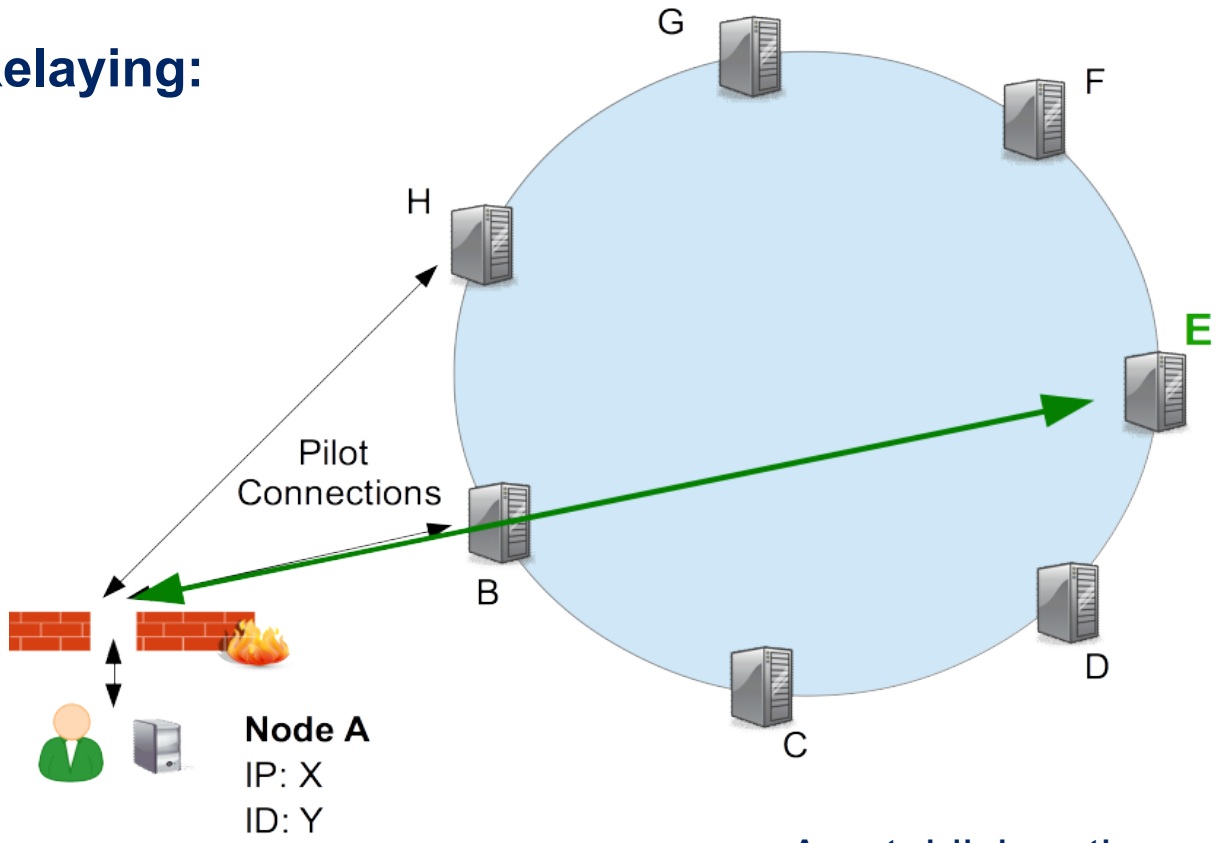
Relaying:



E wants to connect to A....

Overlay - NAT

Relaying:

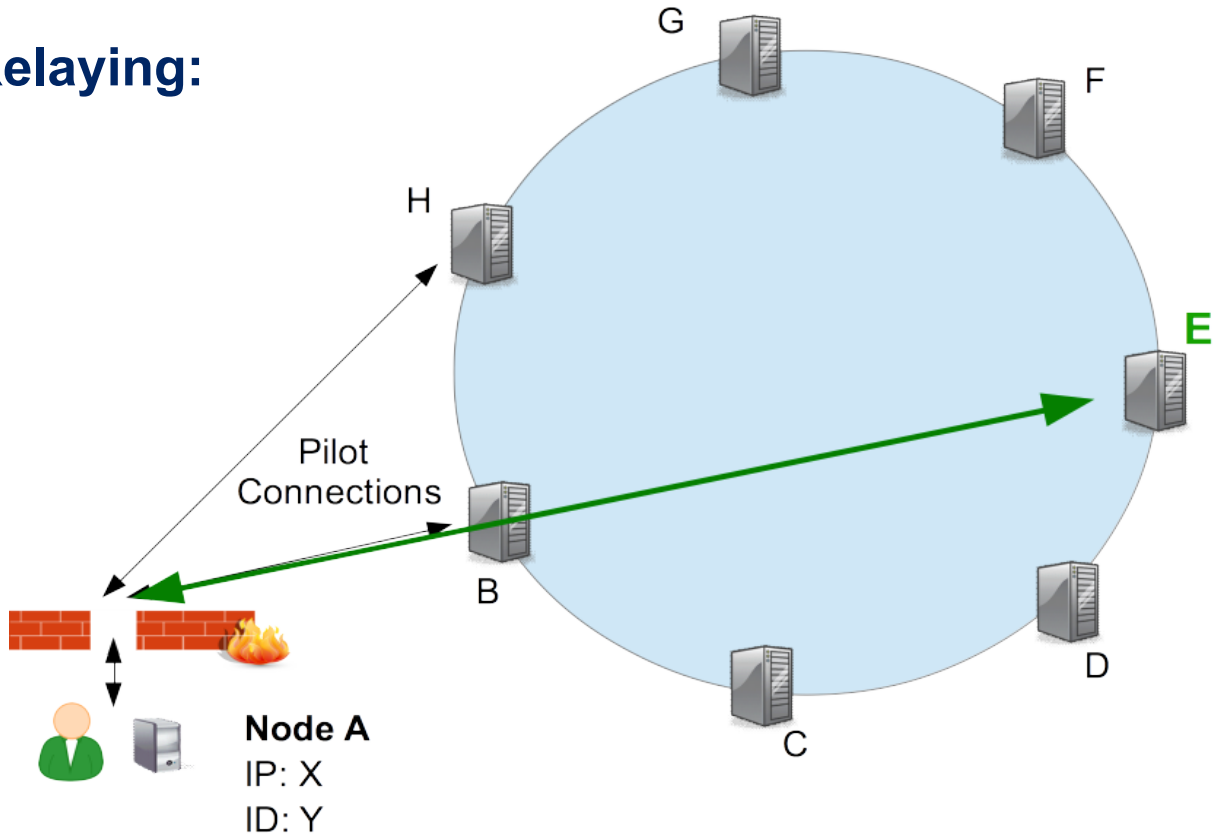


E wants to connect to A....

A establishes the connection to E...

Overlay - NAT

Relaying:

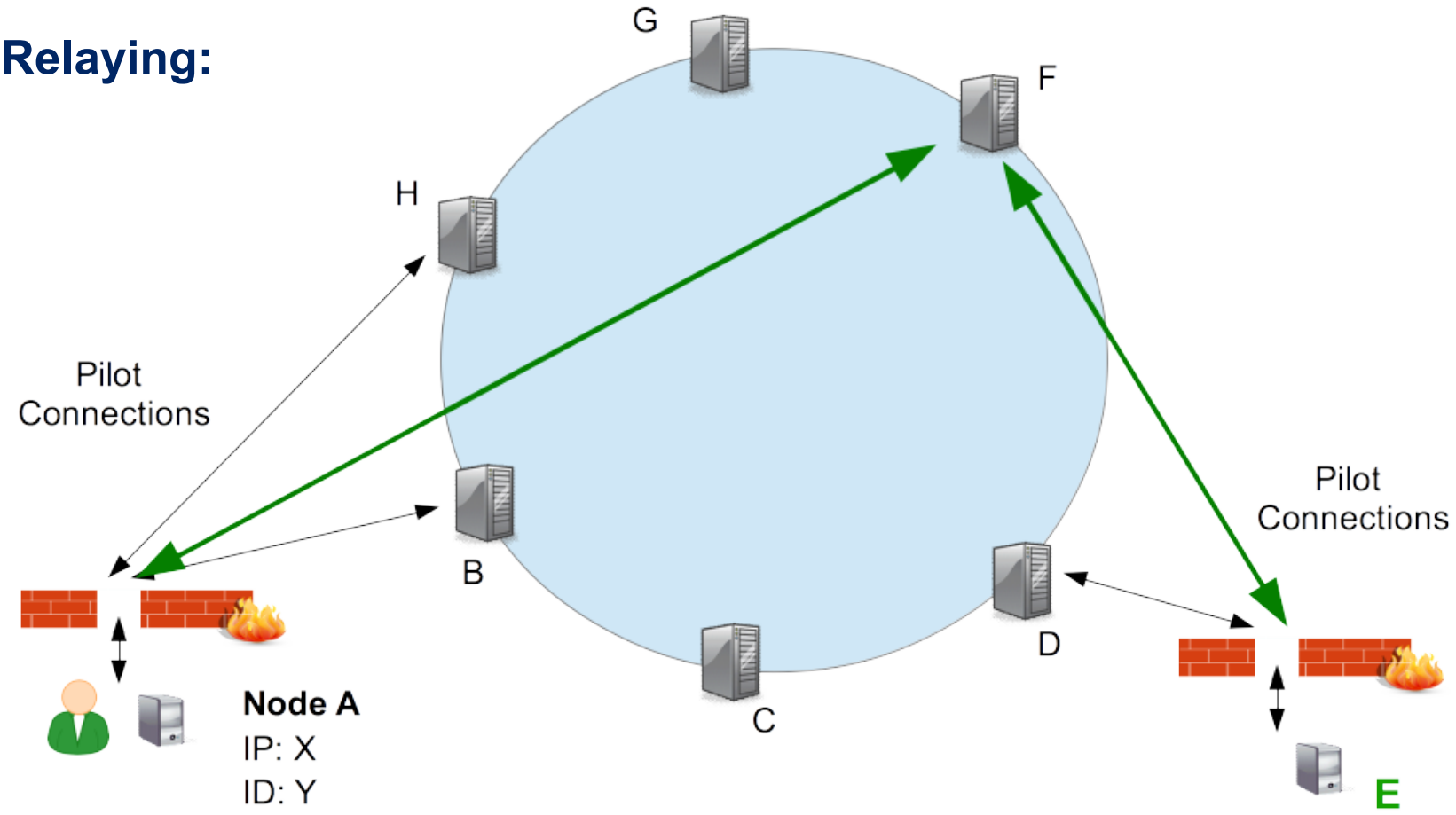


E wants to connect to A....

But what happens, when E is behind a router, as well?

Overlay - NAT

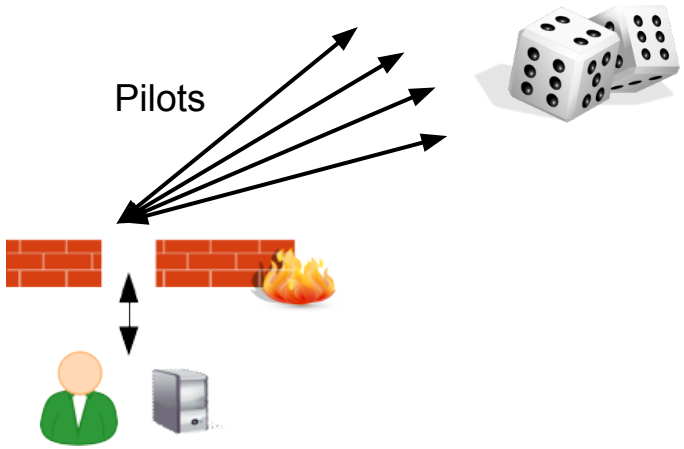
Relaying:



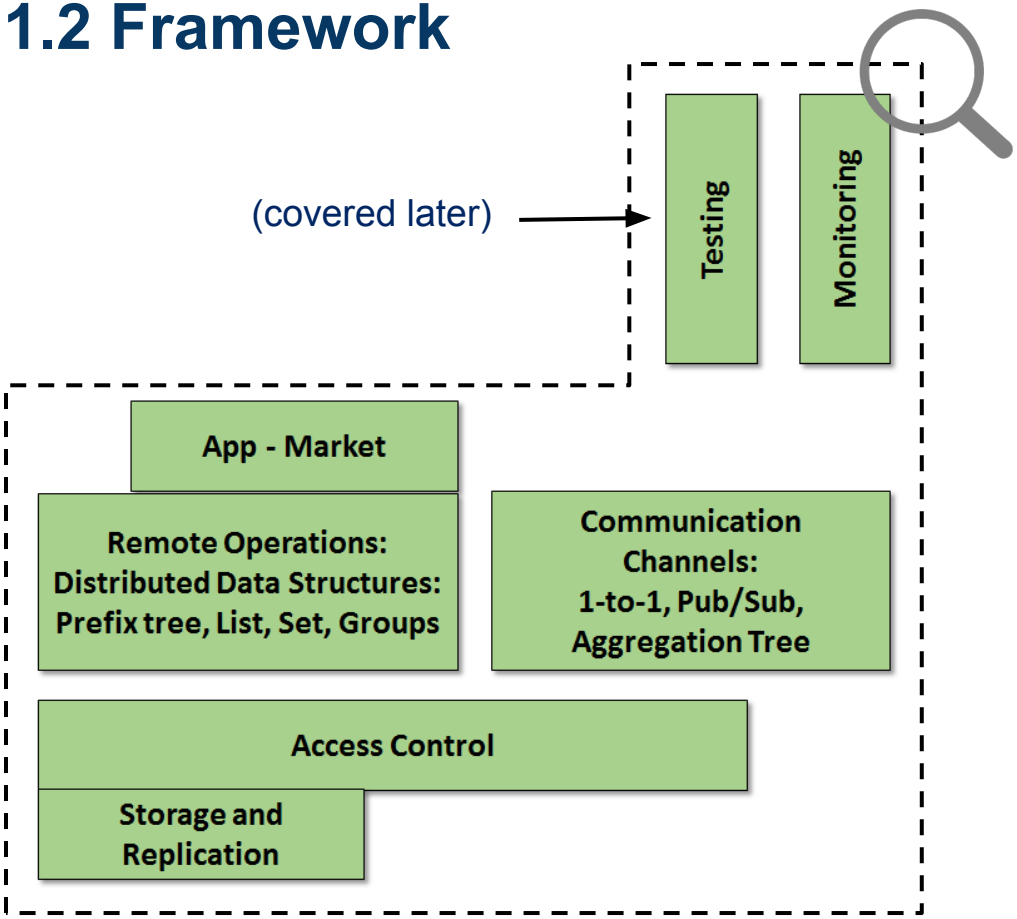
Overlay - NAT

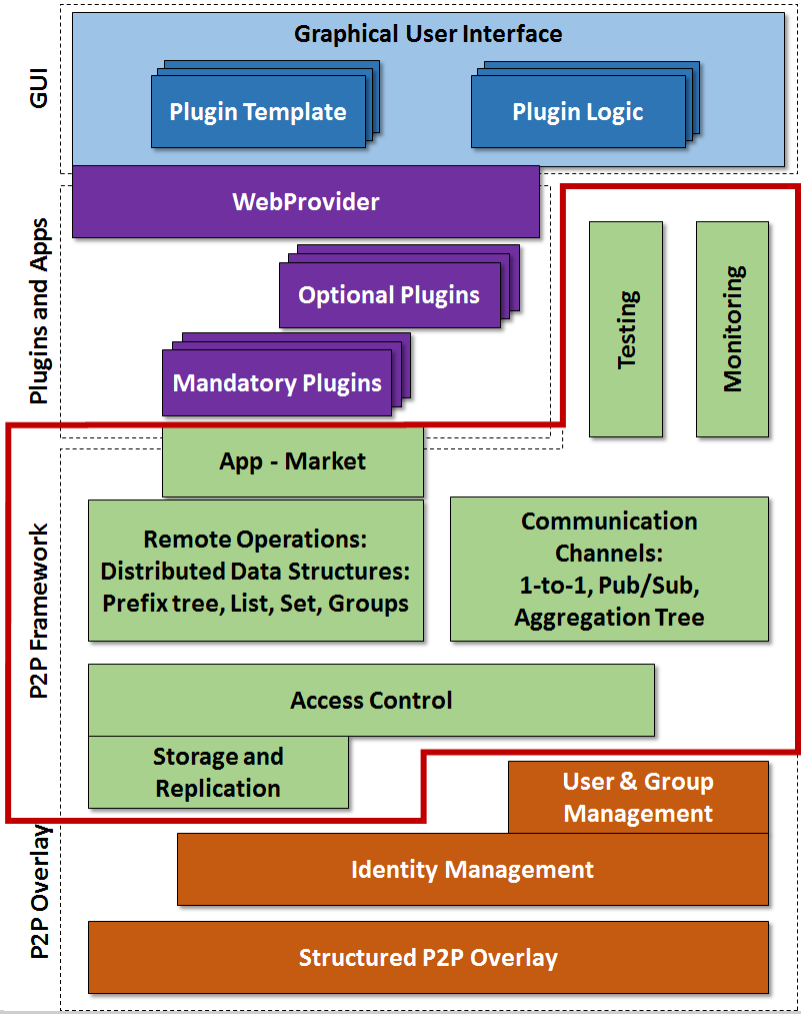
Constraints and Implications:

- At least one leaf of a private (NATed) node has to be public
- Public nodes can become bottlenecks
  - However, NATed nodes choose outgoing pilots at random



1.2 Framework

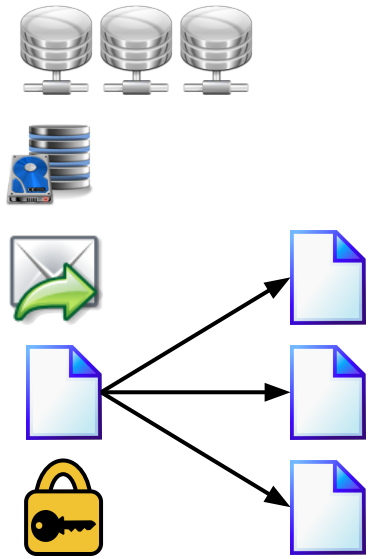




The Framework

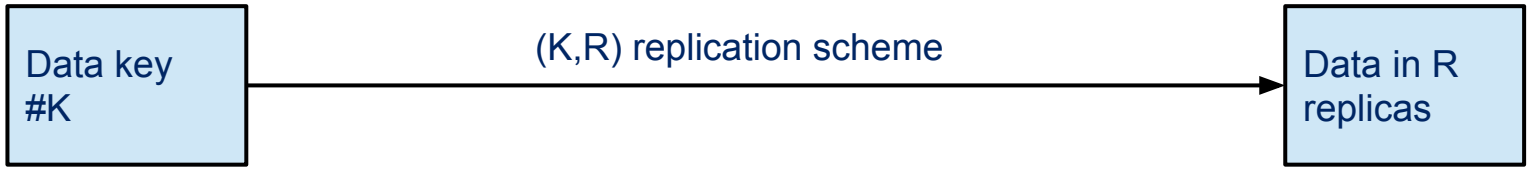
Core functionalities:

- **Distributed Data structures**
- **Storage**
- **Message dispatcher**
- **Replication**
- **Access controls**



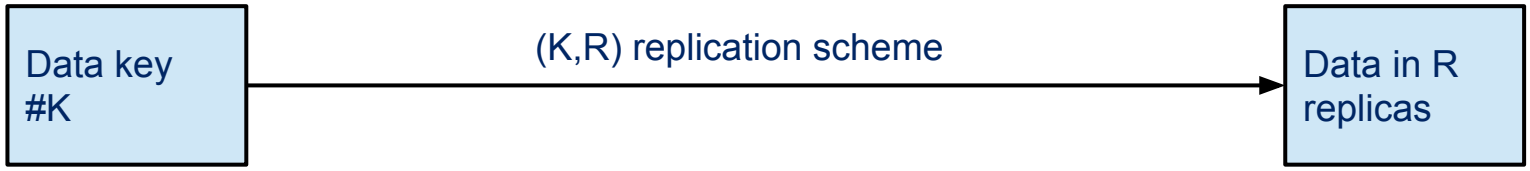
Replication

Key based replication



Replication Bug

Key based replication

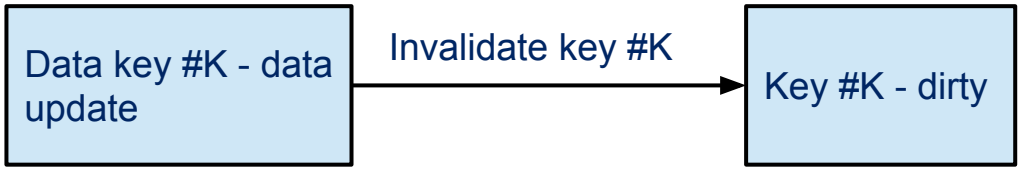


Problem ?

- **Data update for key #K**
  - The replicas still have the data for key #K
  - Replicas checks only for key #K, not the data content
  - Data becomes inconsistent

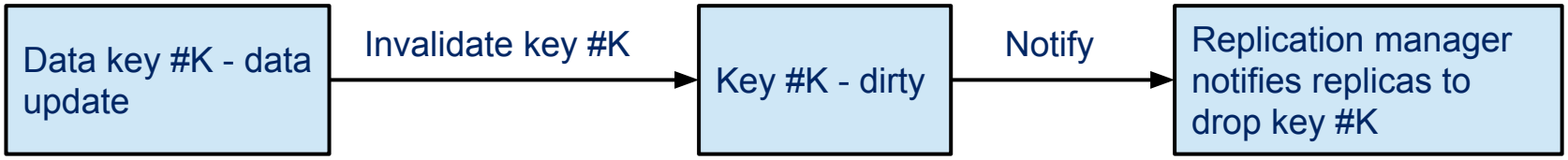
Replication Fix

Key based replication solution



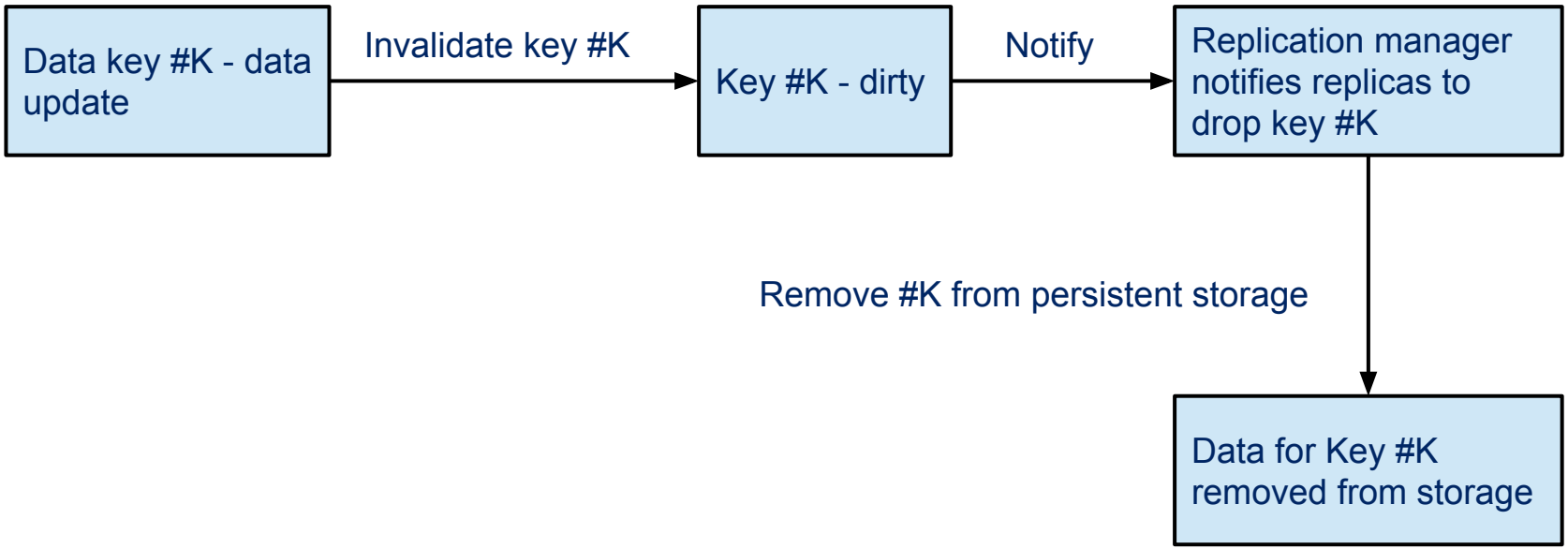
Replication Fix

Key based replication solution



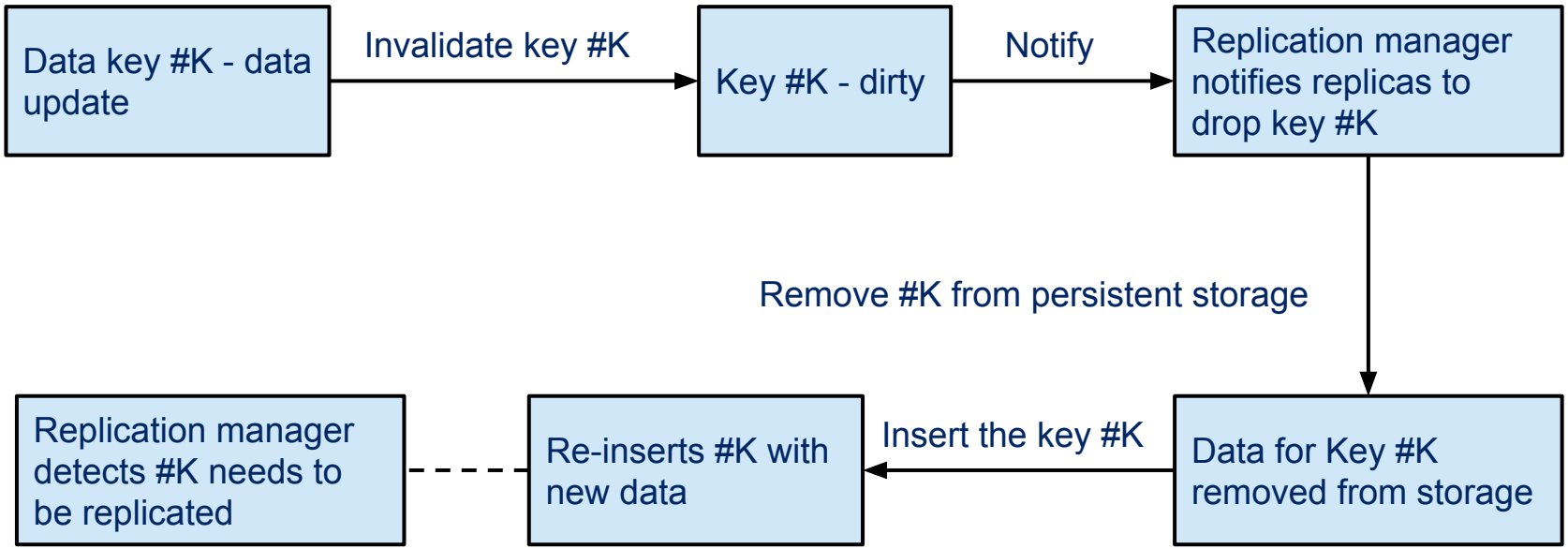
Replication Fix

Key based replication solution



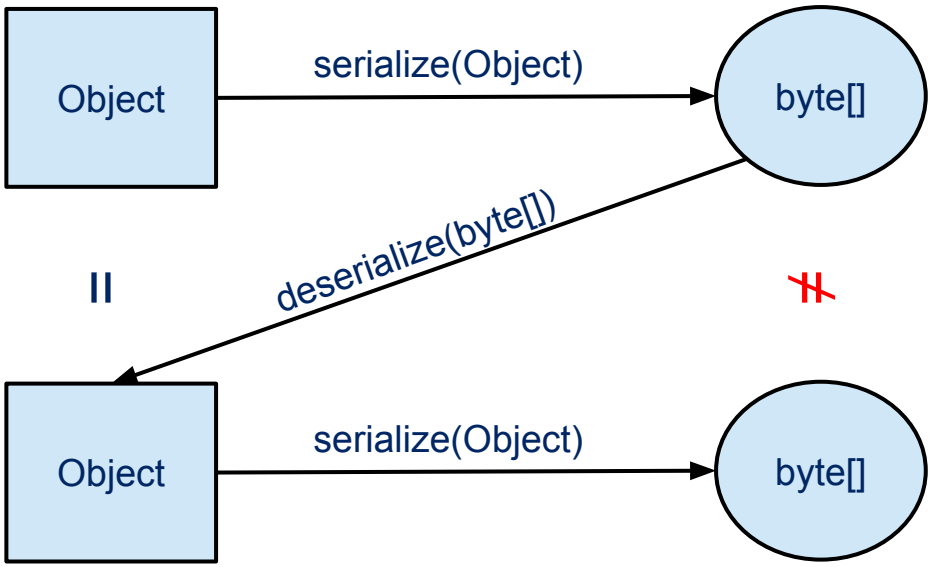
Replication Fix

Key based replication solution



Signing Bug

Java Serialization

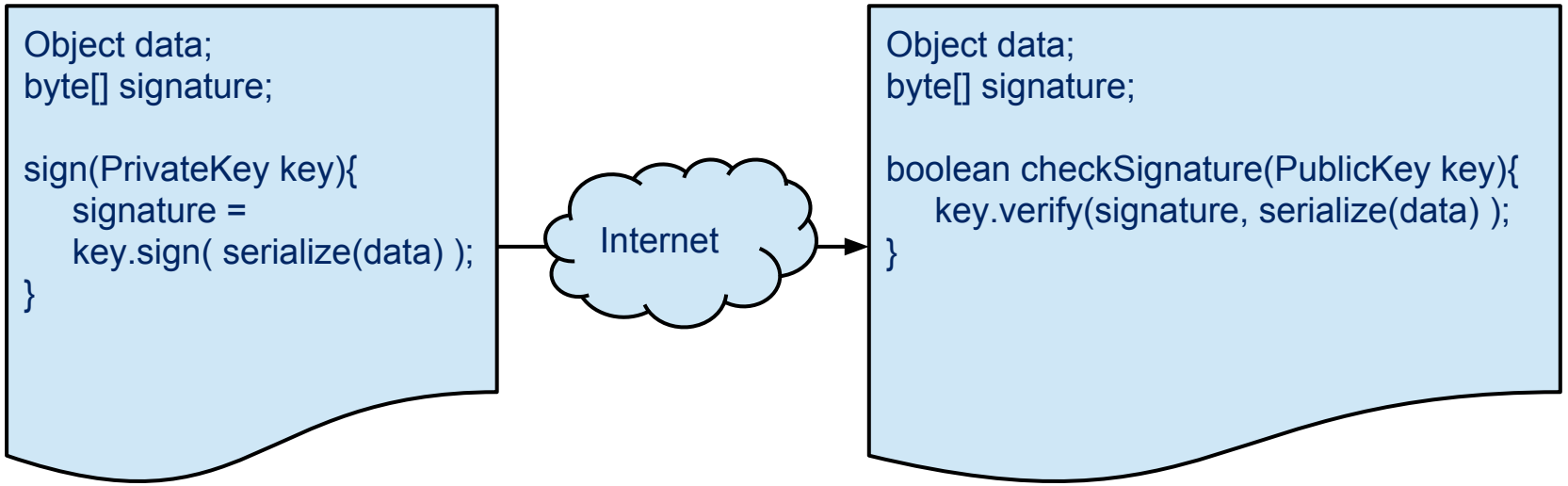


Signing Bug

```
Object data;
byte[] signature;

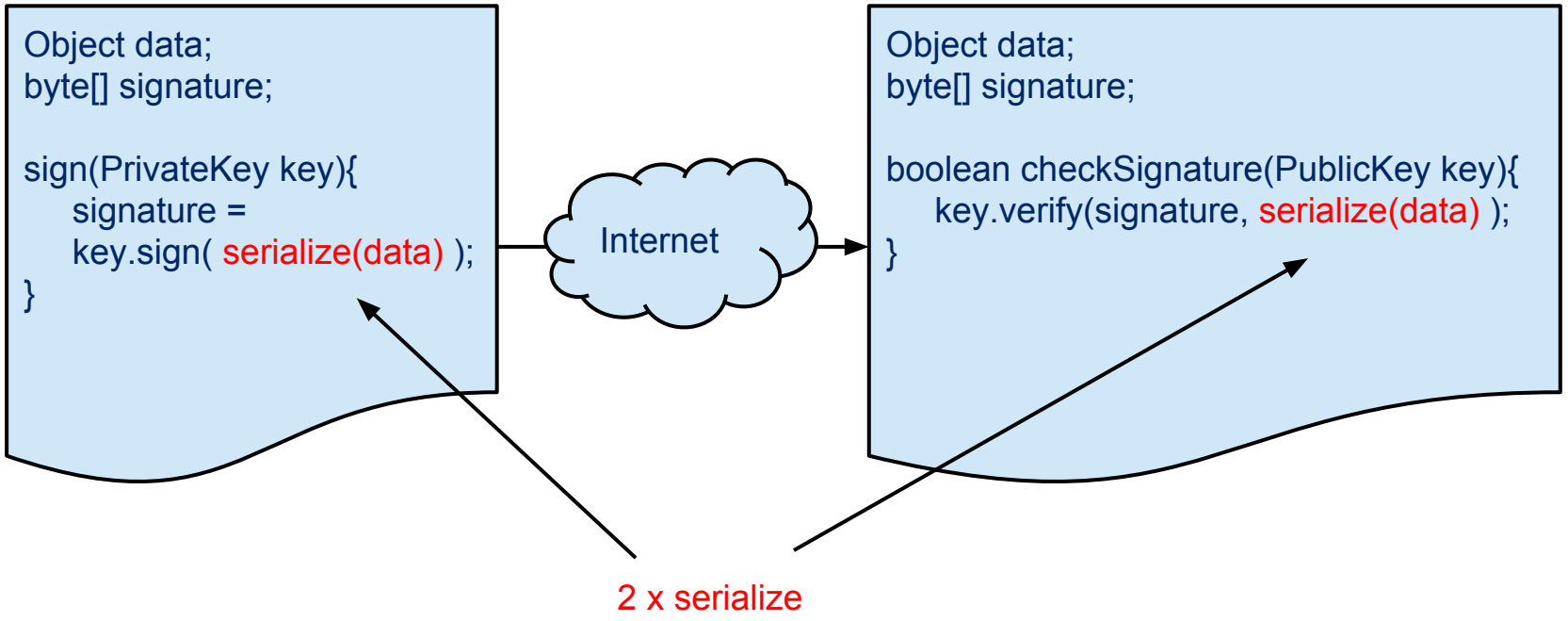
sign(PrivateKey key){
    signature =
    key.sign( serialize(data) );
}
```

Signing Bug


Object data;
byte[] signature;
sign(PrivateKey key){
signature =
key.sign(serialize(data));
}
Internet
Object data;
byte[] signature;
boolean checkSignature(PublicKey key){
key.verify(signature, serialize(data));
}

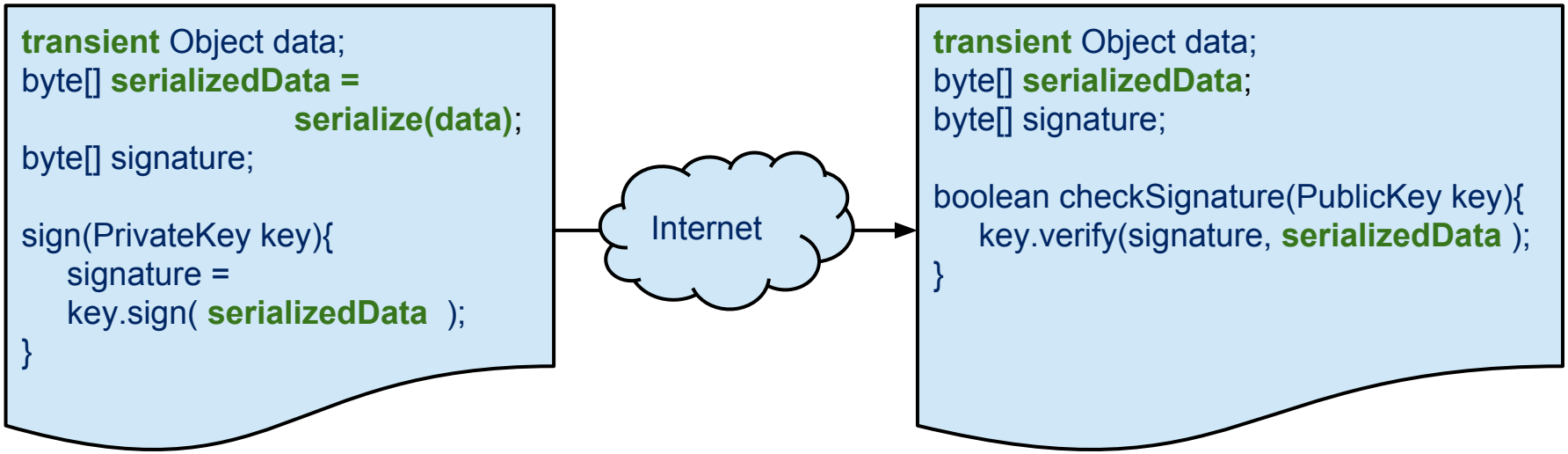
Signing Bug

Values of a serialized Object may differ

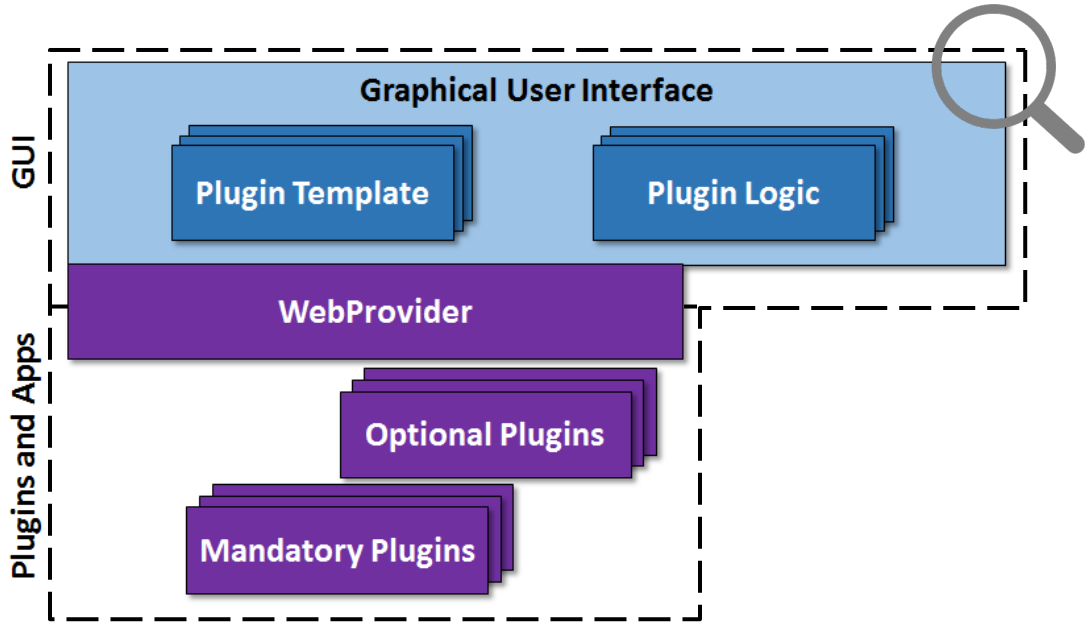


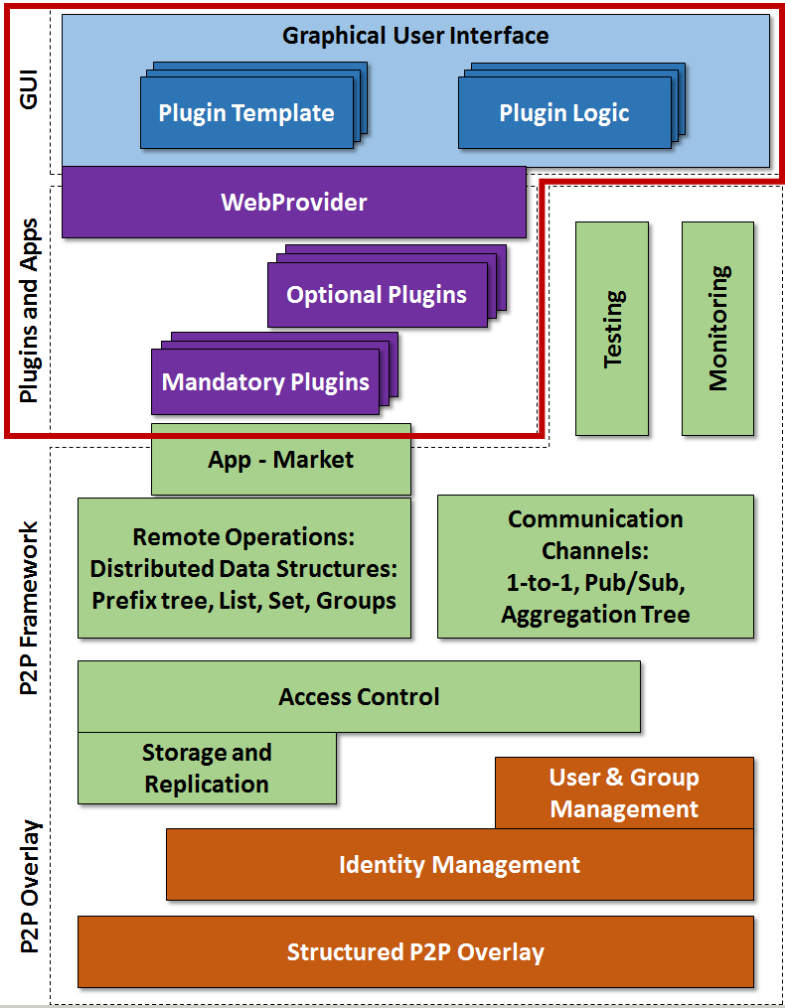
Signing Fix

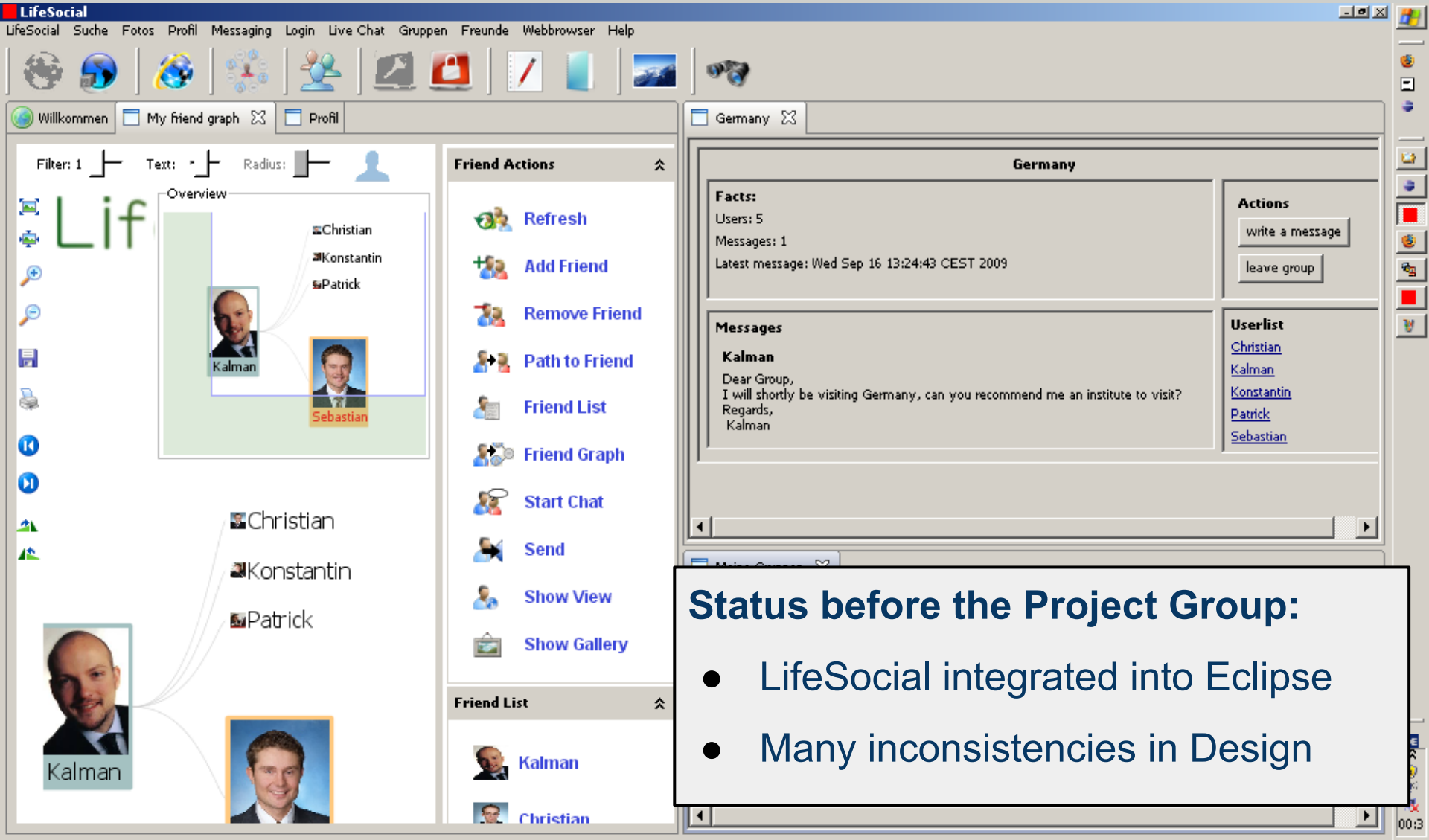
Transfer serialized Data



1.3 Plugins and GUI







Status before the Project Group:

- LifeSocial integrated into Eclipse
- Many inconsistencies in Design

GUI

Results of the Project Group:

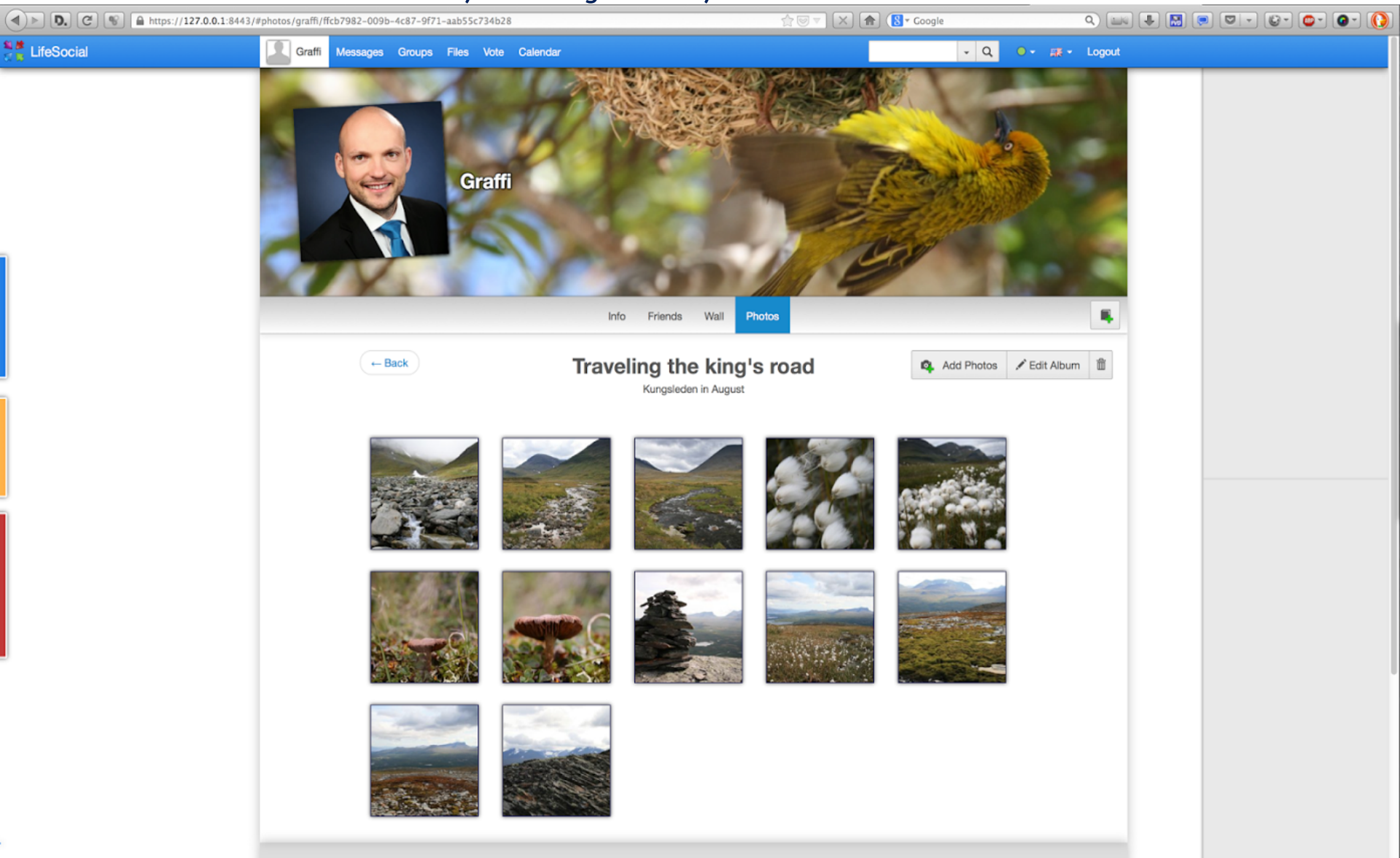


- GUI decoupled from Eclipse
  - application acts as a “Backend”
  - actual GUI is opened in a browser
- Use of standard Web Technologies:
  - HTML5
  - AJAX
  - jQuery
  - Bootstrap
  - Knockback.js

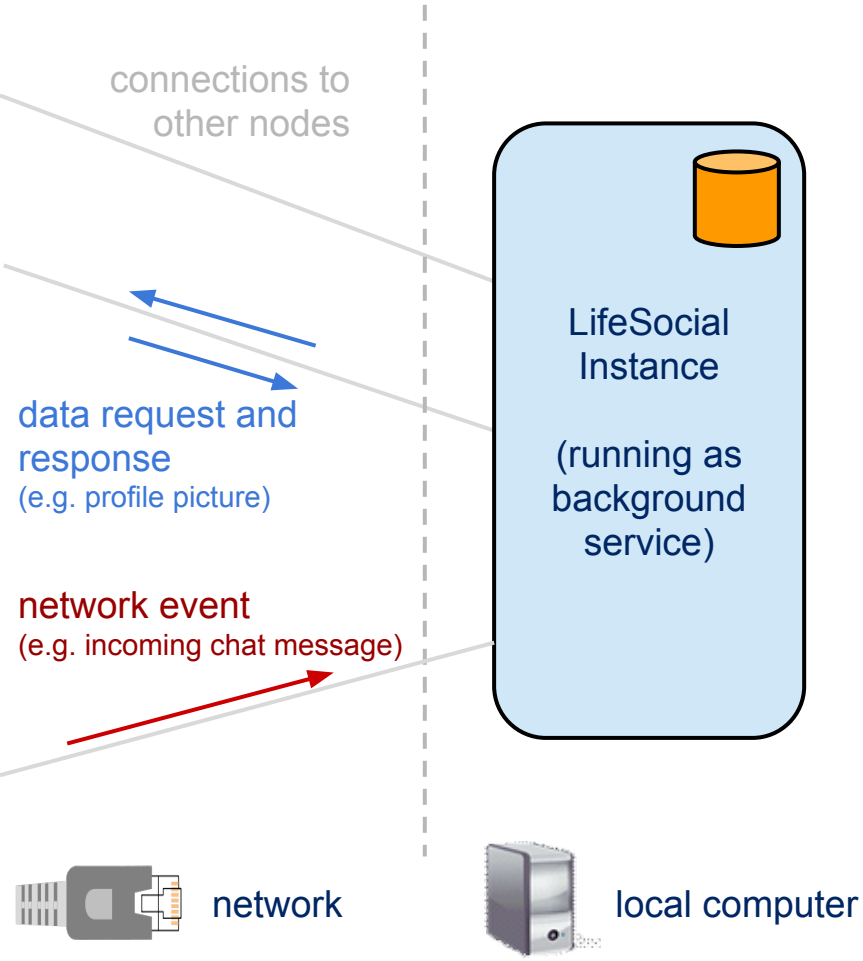
GUI Design decisions / goals



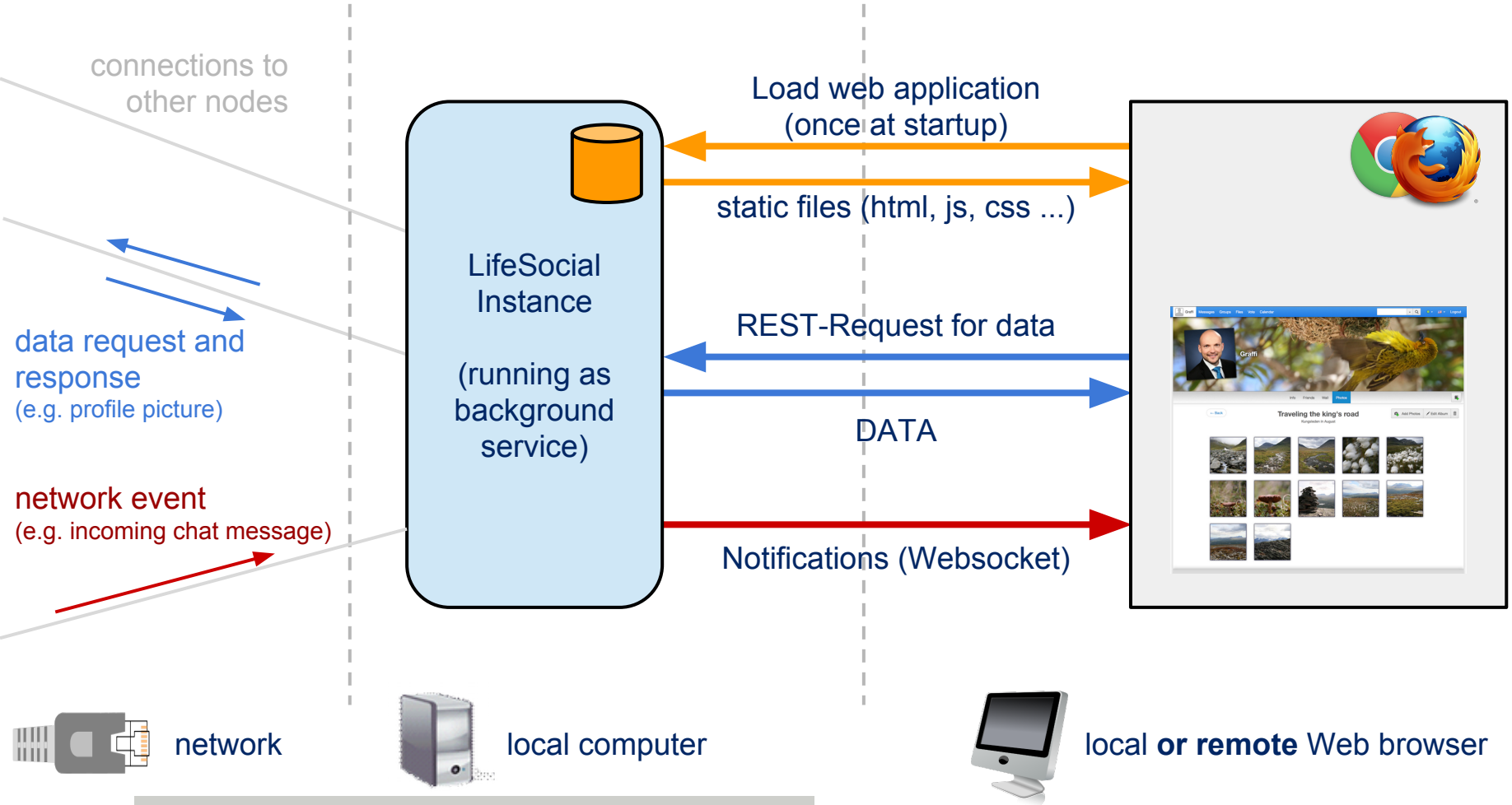
- Javascript single page web application
  - Browser generates Pages (contrary to html pages generated by the backend)
  - only parts of the page are changed when navigating
  - floating windows stay open (e.g. chat)
  - only relevant data is requested from the backend
- Consequent multi-language support
- Support for mobile devices (Responsive web design)


https://127.0.0.1:8443/#photos/graffi/ffcb7982-009b-4c87-9f71-aab55c734b28
Google
LifeSocial
Graffi
Messages
Groups
Files
Vote
Calendar
Logout
Graffi
Info
Friends
Wall
Photos
← Back
Traveling the king's road
Kungsleden in August
Add Photos
Edit Album

HTML Architecture

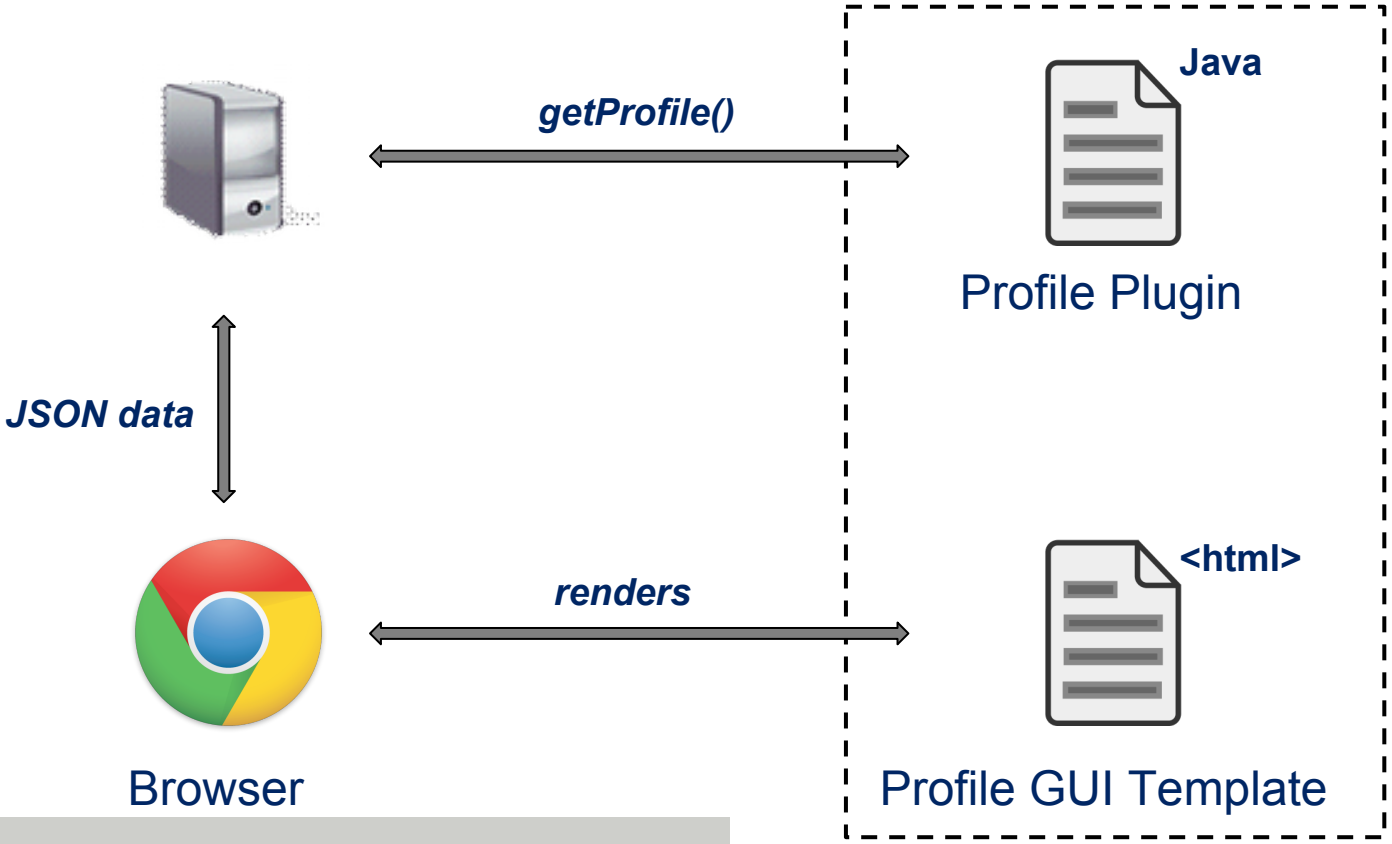


HTML Architecture



Plugins and GUI

Each plugin is completely separated from the plugin GUI:



Plugins

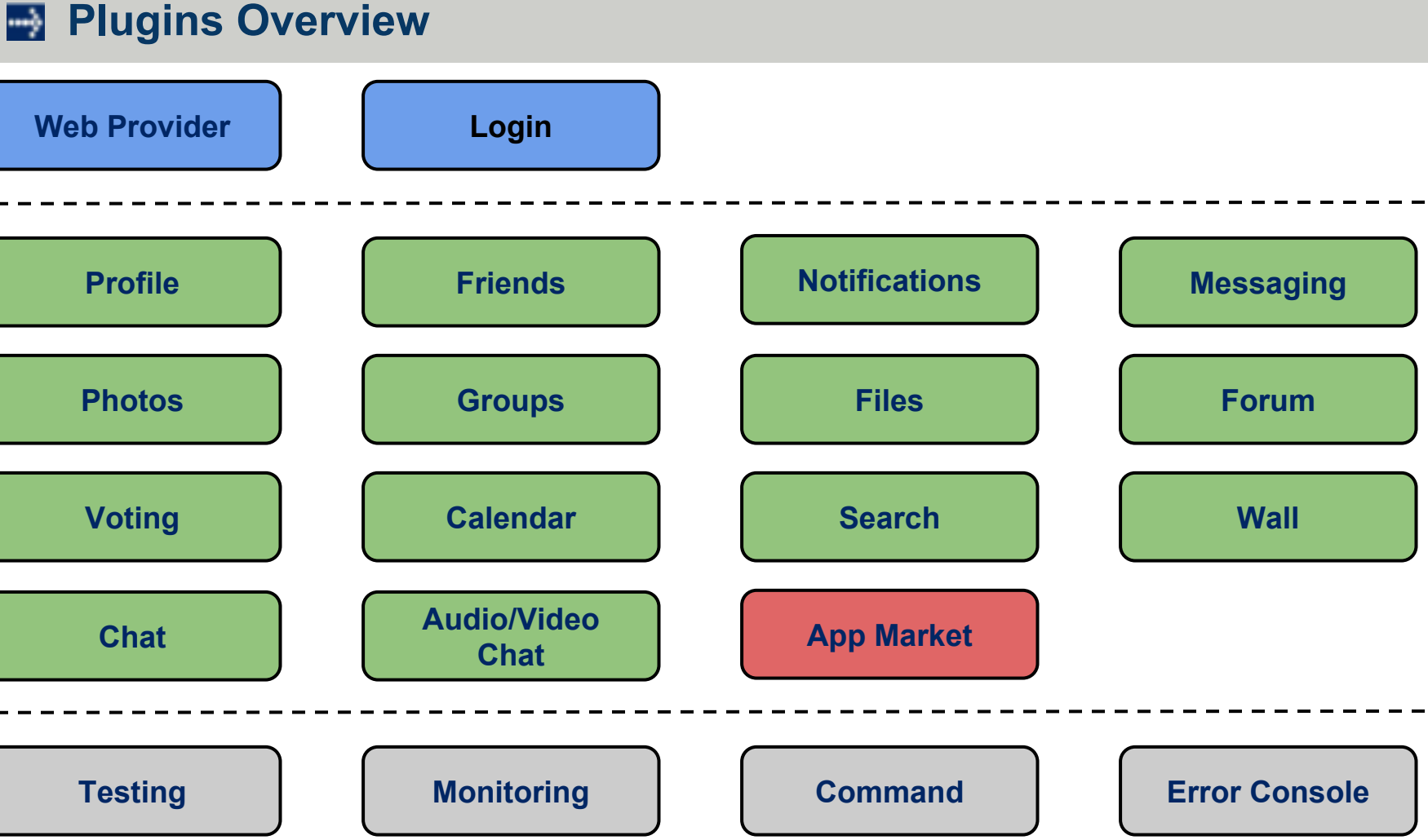
Issues before the Project Group:

- Often, data was not encrypted - no privacy
- Not using the P2P Framework in a consistent way

⇒ Most Plugins completely rewritten

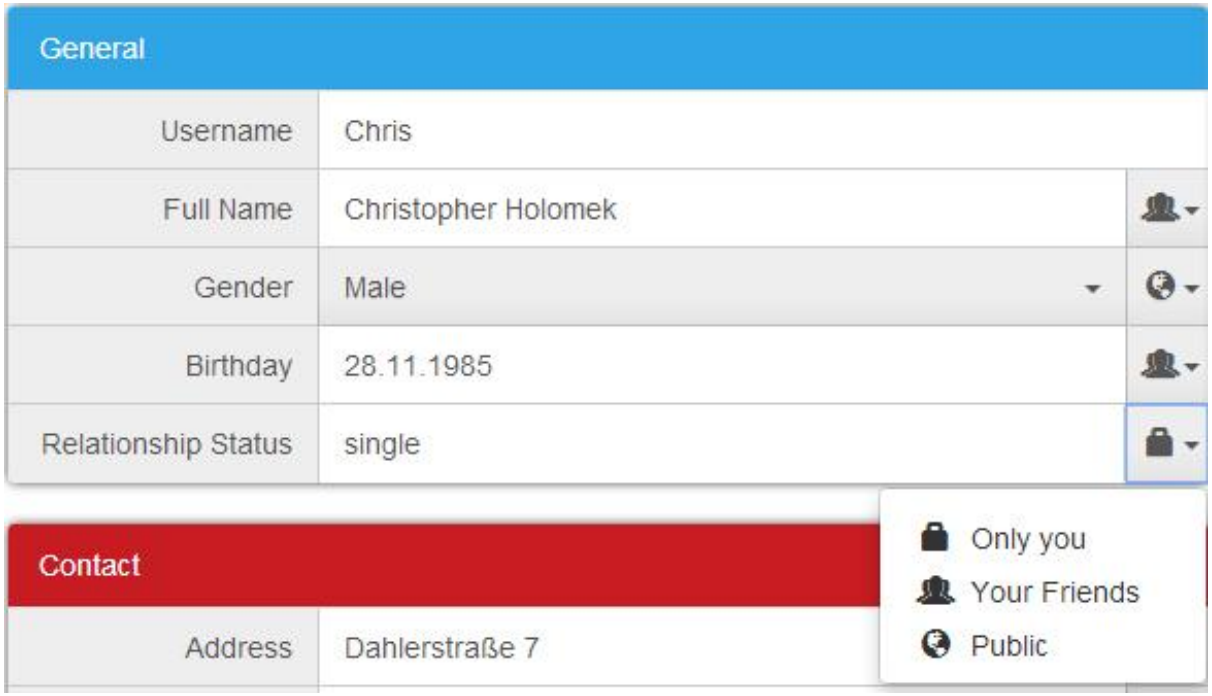
...and extended with a new HTML GUI

Plugins Overview



Profile Plugin

- Rewritten completely
- Privacy for each field





Wall Plugin

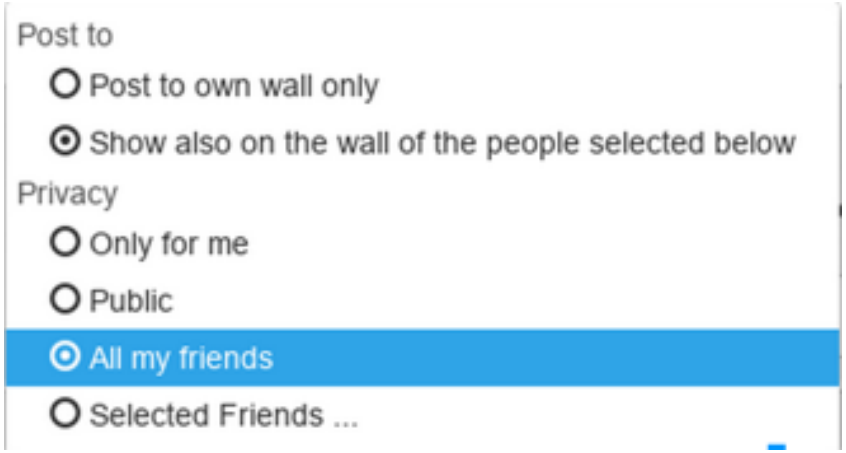
Before the Project Group:

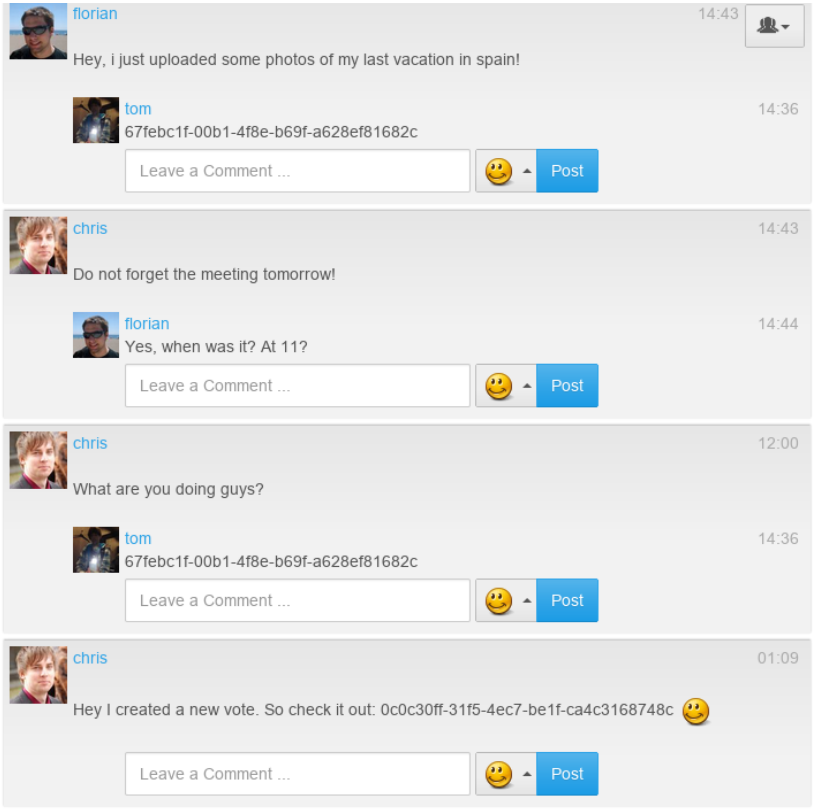
- each user has an own wall with entries (like a “guest book”)
- everyone could post on this wall
- wall had to be “visited” to see the entries
- **entries were completely unencrypted**

Wall Plugin (Now)

- Entries are encrypted
- Privacy selection
- Auto-Publish to the wall of others

⟹ **behaves more like a news stream**





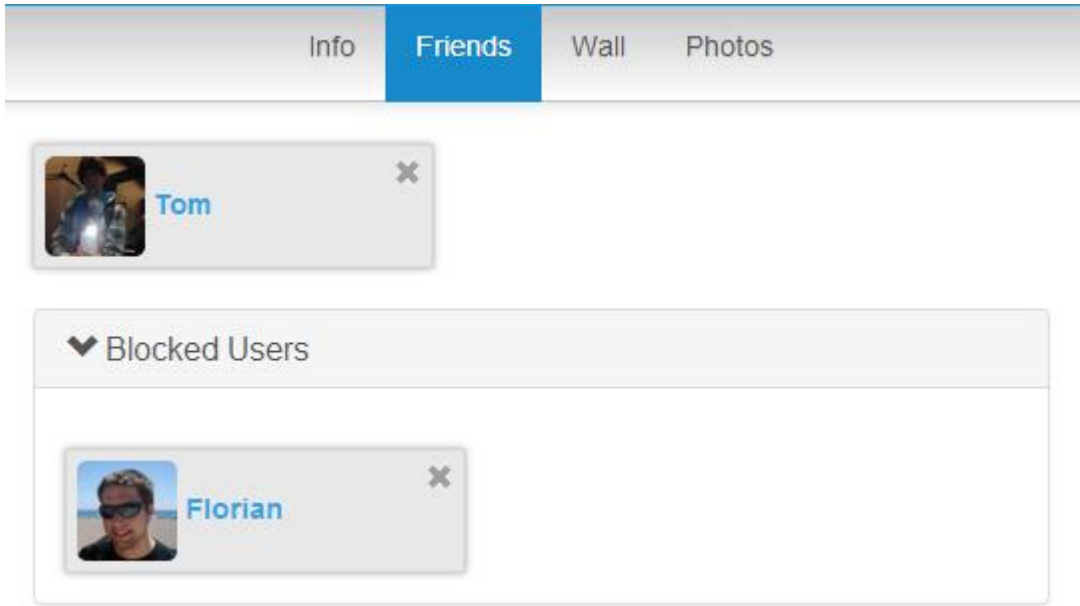
Notification Plugin

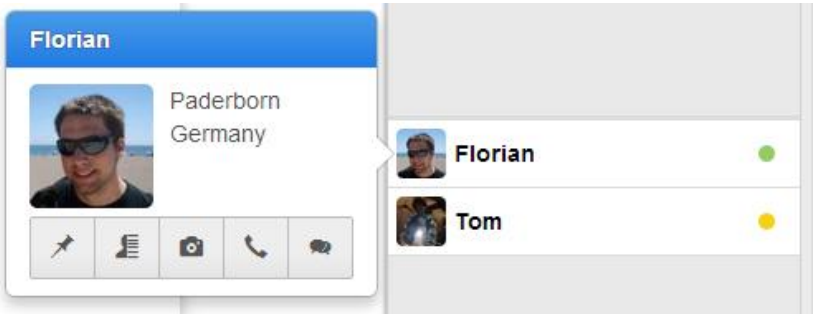
- Send notifications
- Notifications stored when user is offline
- Drop or replace notifications
- Send custom data in notification
- Soundeffect
- Define templates for GUI
- Plugins can register for Notifications



Friends Plugin

- Friendship request via Notification Plugin
- Login status of friends
- Friend & Blocklist (right)
- Sidebar (left)





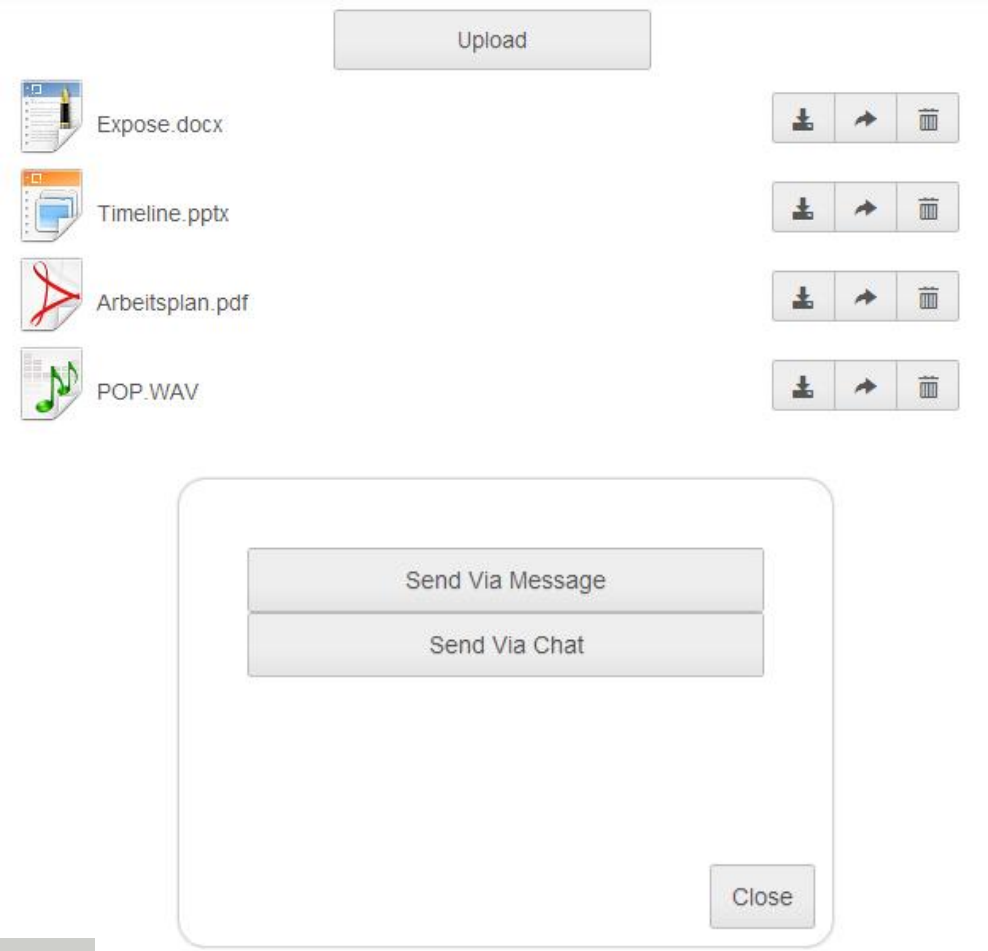
Messaging Plugin

- Rewritten completely
- Inbox & Outbox
- Write, reply and forward messages
- Badges show unseen messages
- Labels
- Attachments



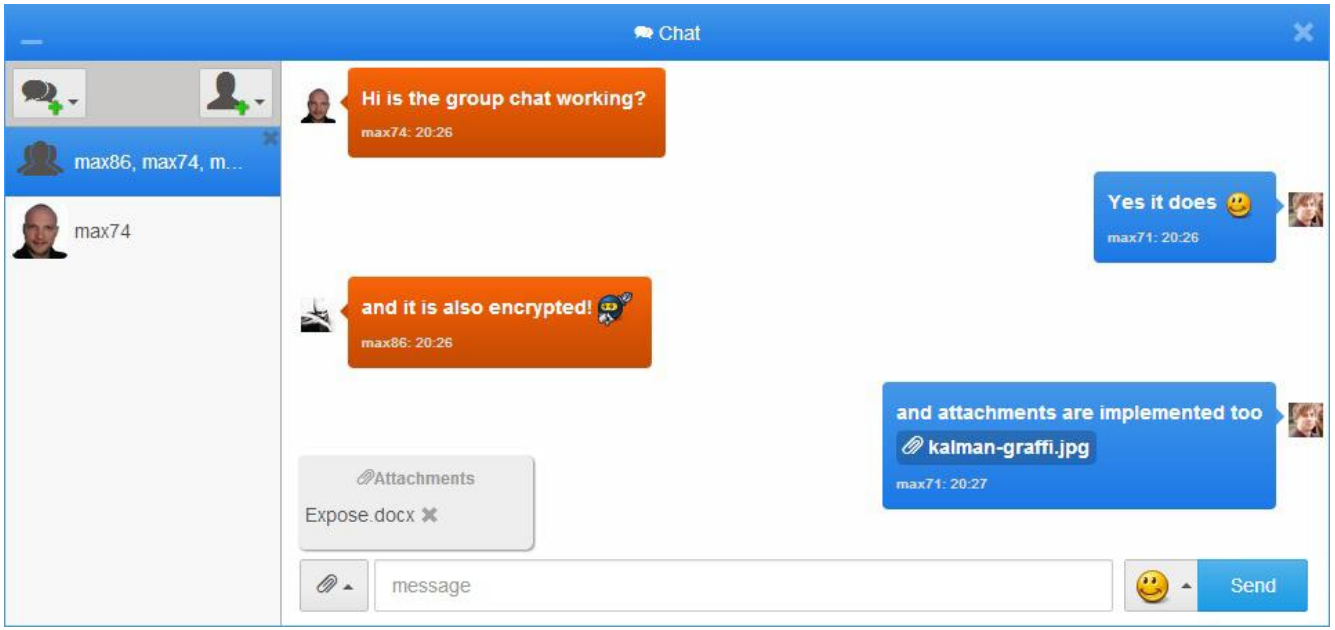
Files Plugin

- Up- and download files
- Deletion of files
- Share files
  - Via Message
  - Via Chat
  - … extendable



Chat Plugin

- Rewritten completely
- One to one
- Many to many
- Soundeffect
- Attachments







Institute of Computer Science
Research Group – Theory of Distributed Systems

Audio/Video Chat Plugin

- One to one
- Uses WebRTC
- Signalling
  - information exchange
  - over our network





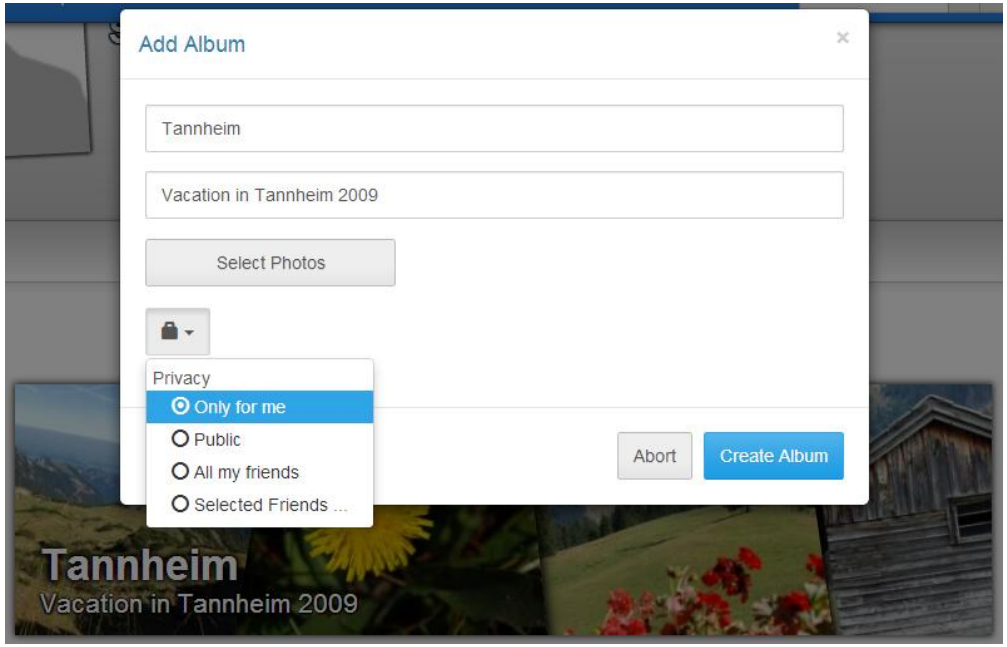






Photos Plugin

- Rewritten completely
- Album with title and description
- Photos with caption and comments
- Privacy for albums
- Encryption of photos





Search Plugin

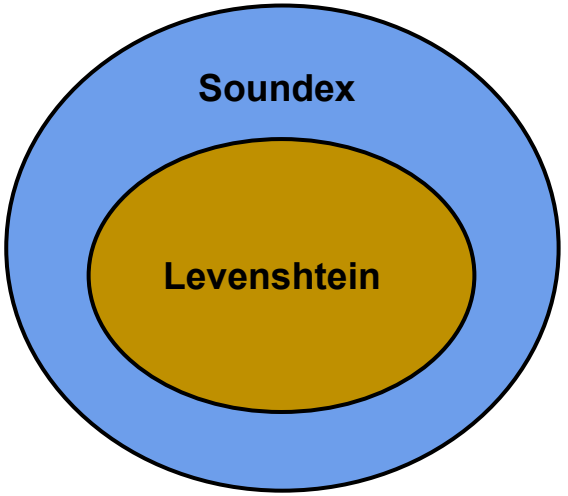
1. Pre-Filter using Soundex

Britney ⇨ B635

bewährten ⇨ B635

2. Post-Filter using Levenshtein distance

- compare two strings
- min # operations to make both strings equal



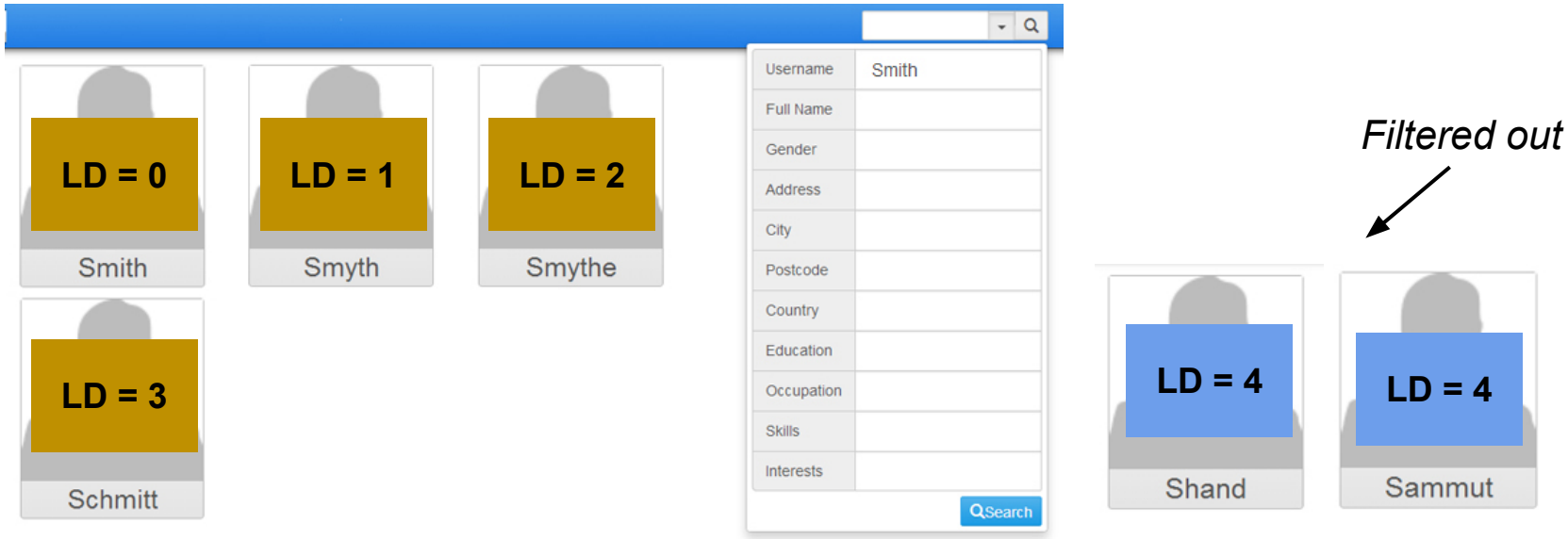
Search Plugin

Search for “Smith”

1. Soundex:

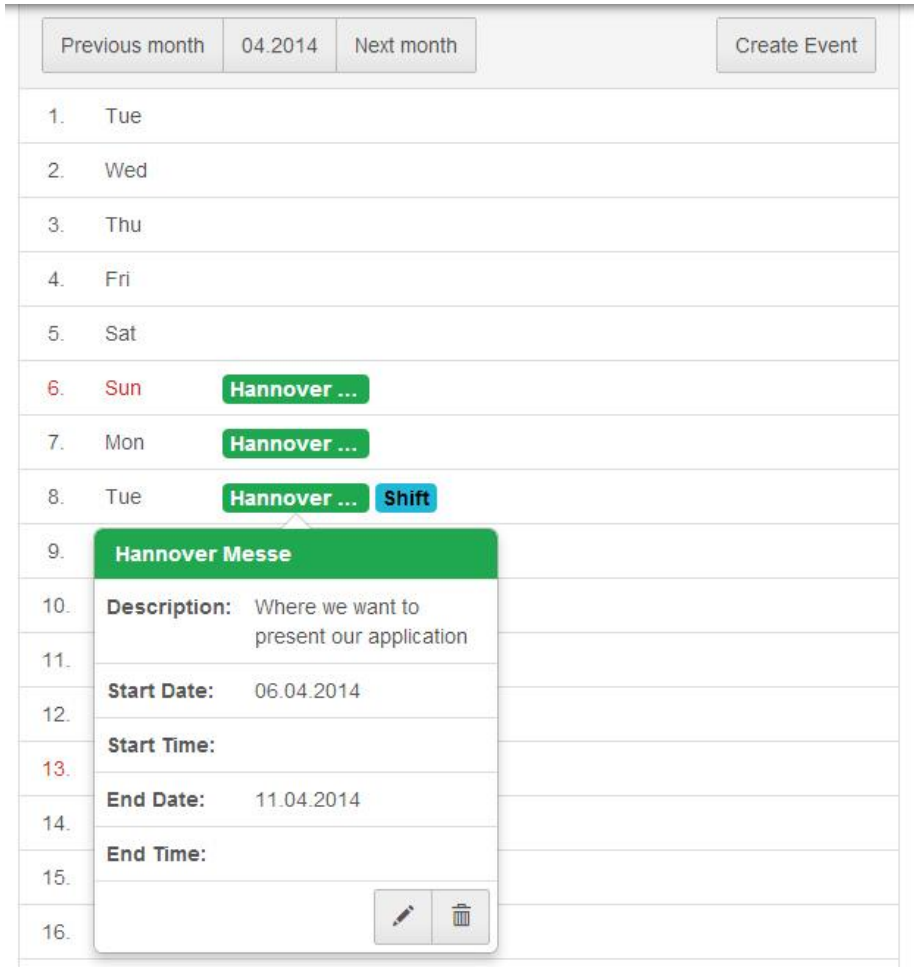
Schmitt, Shand, Smith, Smyth, Smythe, Sammut

2. Levenshtein distance:



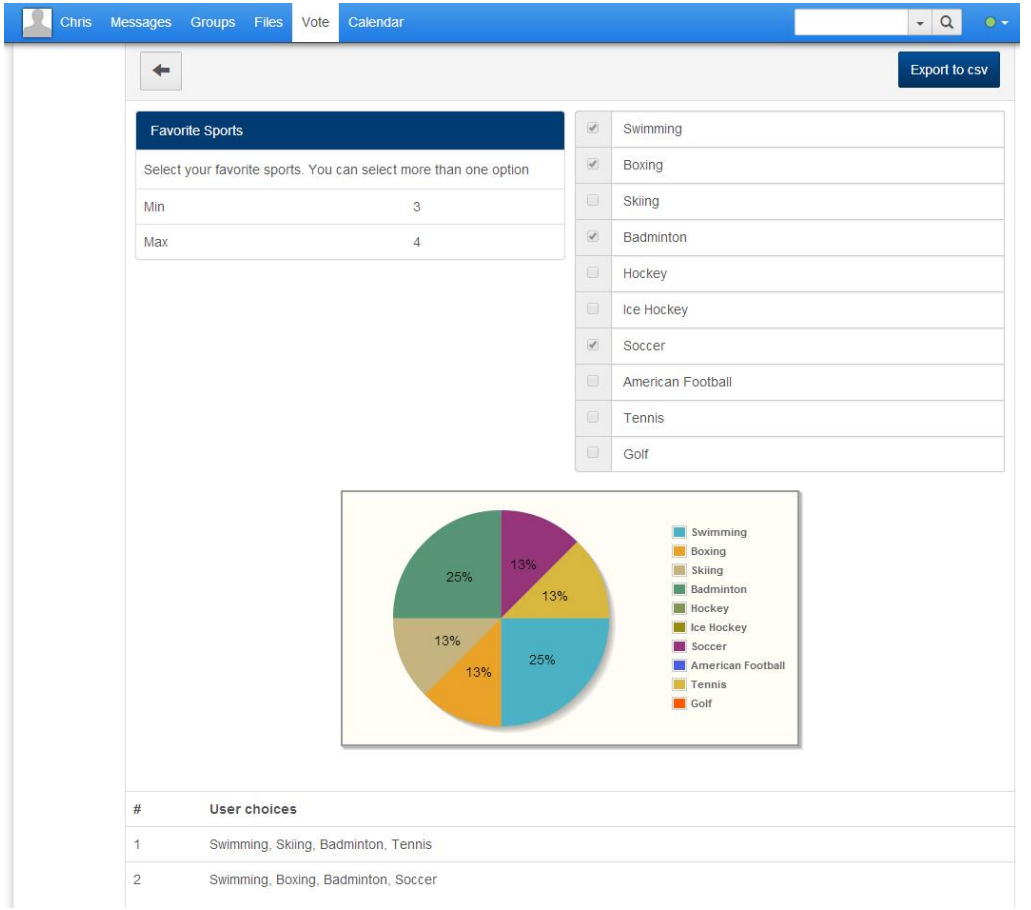
Calendar Plugin

- Month view
- Create, modify and delete appointments
- Multi-day appointments
- Reminder via notification



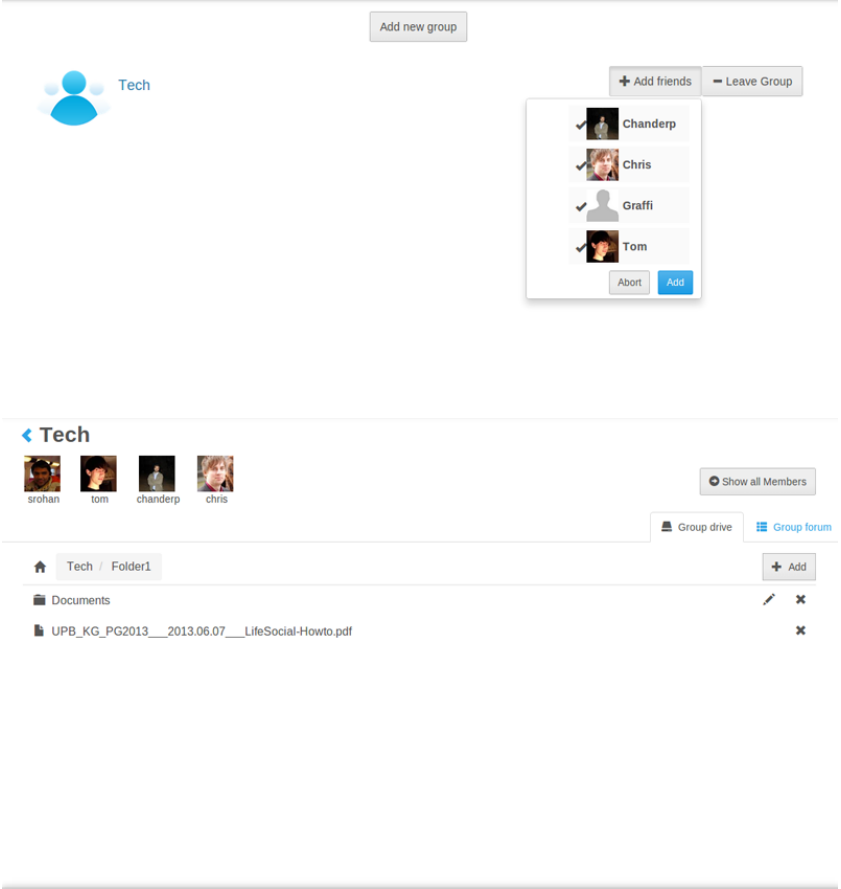
Voting Plugin

- Rewritten completely
- Create and delete votings
- Privacy
  - Private
  - Public
- Pie Chart
- Export results to csv



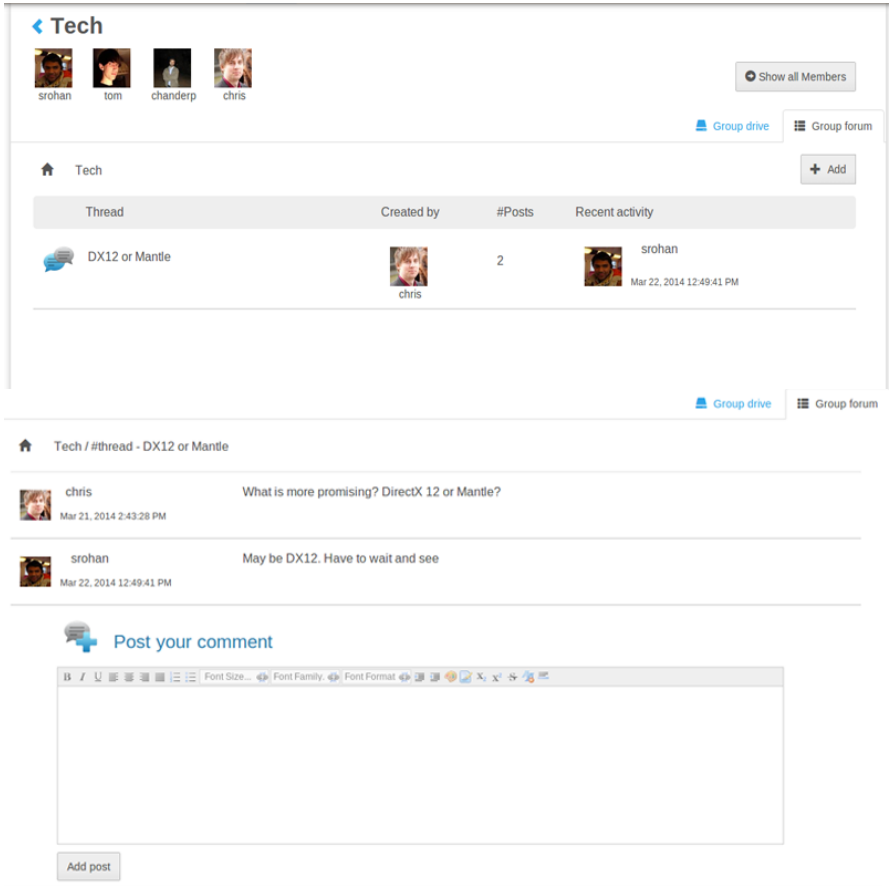
Groups Plugin

- Privacy mode: public
- Members add their friends to a group
- User notified when added to a group
- Provided functionalities
  - shared drive
  - forum
- Security using user key signing for folders and files in the shared drive



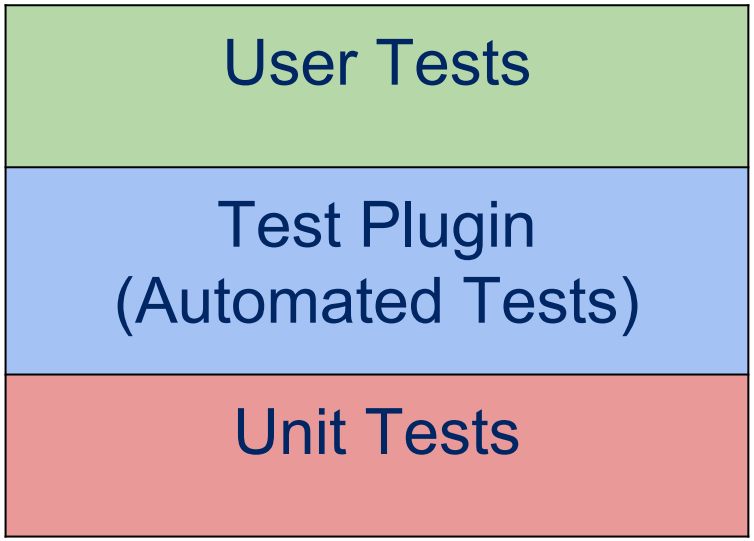
Forum Plugin

- Forum provided for a group
- One forum for each group
- WYSIWYG support
- Posts and threads cannot be modified or deleted
- Security using user key signing for the threads and the posts



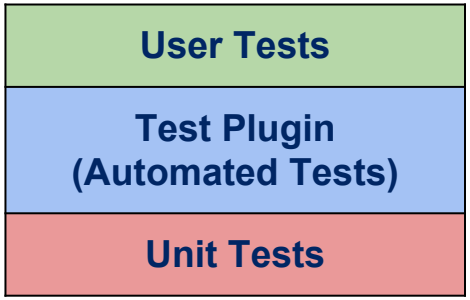
Testing

- To check functionality, performance, reliability etc.
- Three blocks:
  1. Unit Tests
  2. Test Plugin Tests
  3. User Tests



Testing

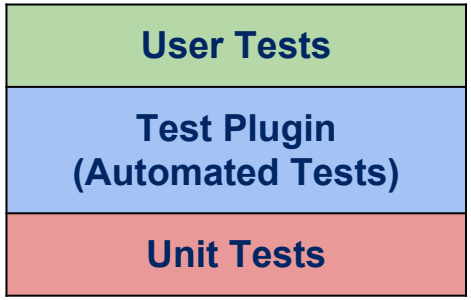
1. **Unit Tests**
   - Testing single components
   - Testing with several simulated nodes on the local machine
   - No GUI interaction involved



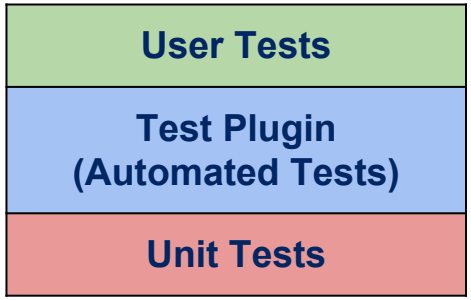
Testing

2. Test Plugin

- Testing the system as a whole
- Performed distributed on 20 machines
- Roles: Master, Slave
- Automated execution of test plan

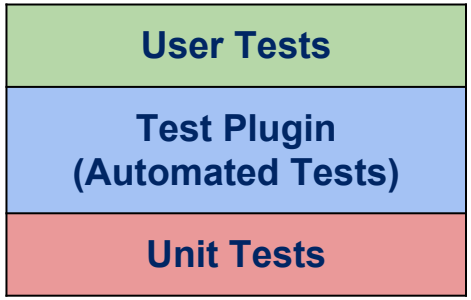


Testing



2. **Test Plugin**
   - **New**
     - Created “sendFriendRequestInOrder” to avoid from potential problem
   - **Further work**
     - Modify and create new test cases

Testing



3. User Tests

- Internal team test done
- Users connected from at home (NAT)
- Two public always-on nodes in the ring
- Tested for several weeks

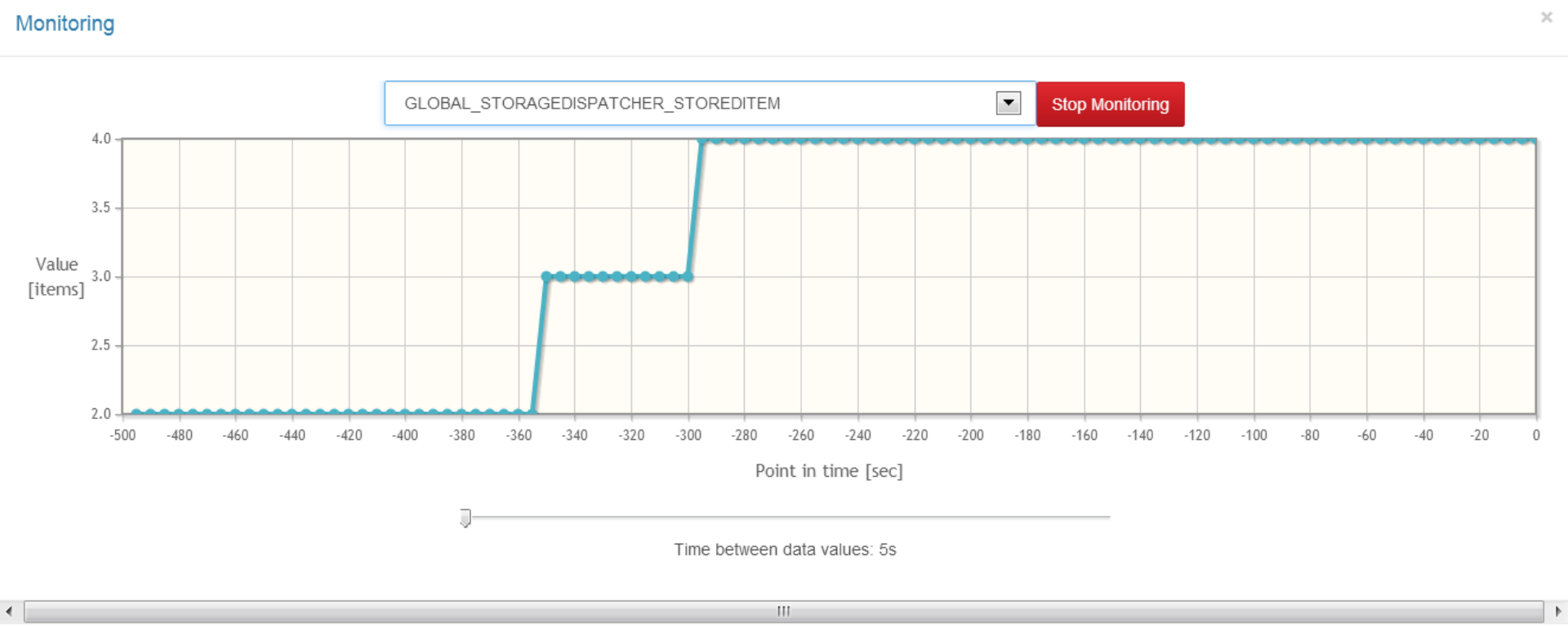
- **next:** Invite external users for an Alpha Test

Monitoring

- Monitoring global statistics of the system
- For improving quality of service
- Evaluating through various metrics

Monitoring

Monitored data



Conclusion

- **P2P Framework**
  - Solid
  - Secure
  - Works in real environments
- **Prototype LifeSocial**
  - Standard Web Technologies
  - Secure
  - Privacy opt-in





Further Steps

- Public alpha test - starts soon...
- Refrain from Eclipse RCP
- Improve plugins
- Further plugins
  - App Store
  - Video Streaming
  - BitTorrent
- Further NAT strategies
- Optimizing

Institute of Computer Science
Research Group – Theory of Distributed Systems

Thank you for listening

And have fun during the demonstration

Interested?

Visit our Website: http://p2pframework.com

Download and try it out by yourself...

Passwort: LS2014alpha