



Dipl.-Inform. Sebastian Mies  
Universität Karlsruhe (TH)



# Motivation



- SpoVNet Services

- Built as **overlay** networks upon **heterogeneous** underlays
- **Spontaneously** created – no underlay support needed
- **Adapt** to changing network conditions

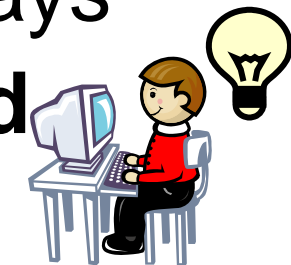
→ How can those overlays be

- created **comfortably**? 
- **secured**? 
- optimized with **cross-layer-information**?

# Our Architectural Contribution



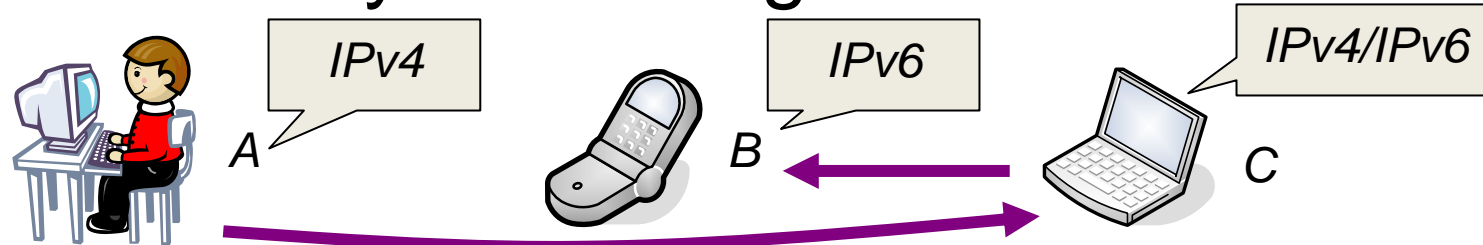
- Divide overlay construction into two parts
  - Provide abstract transport connectivity with Base Communication
  - Provide location independent identifier addressing using the Base Overlay
- Consider security right from the start
  - Integrated security!
- Provide X-layer information for overlays
  - **Support comfortable creation and deployment of new services**



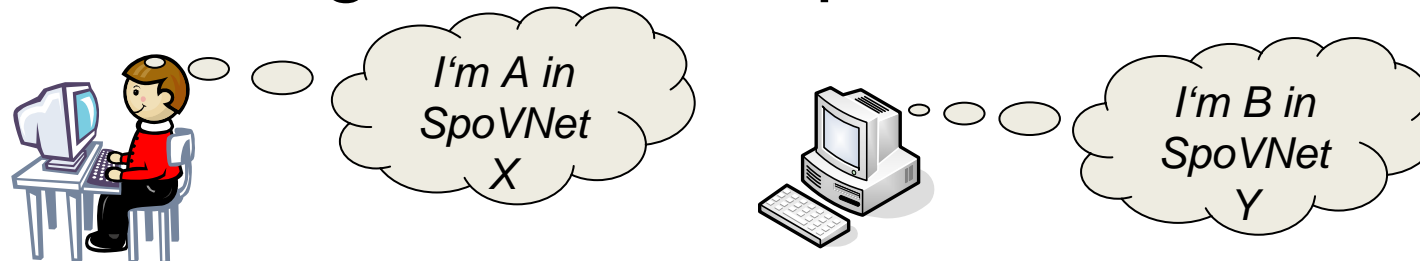
# Selected Contributions



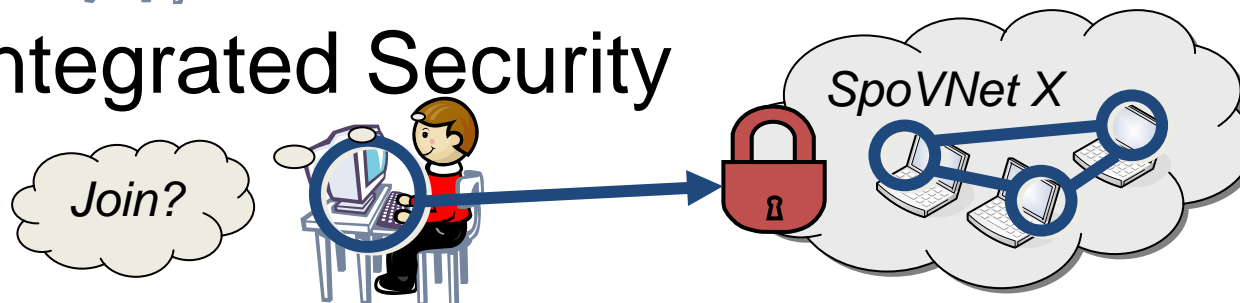
## 1. Connectivity in heterogeneous networks



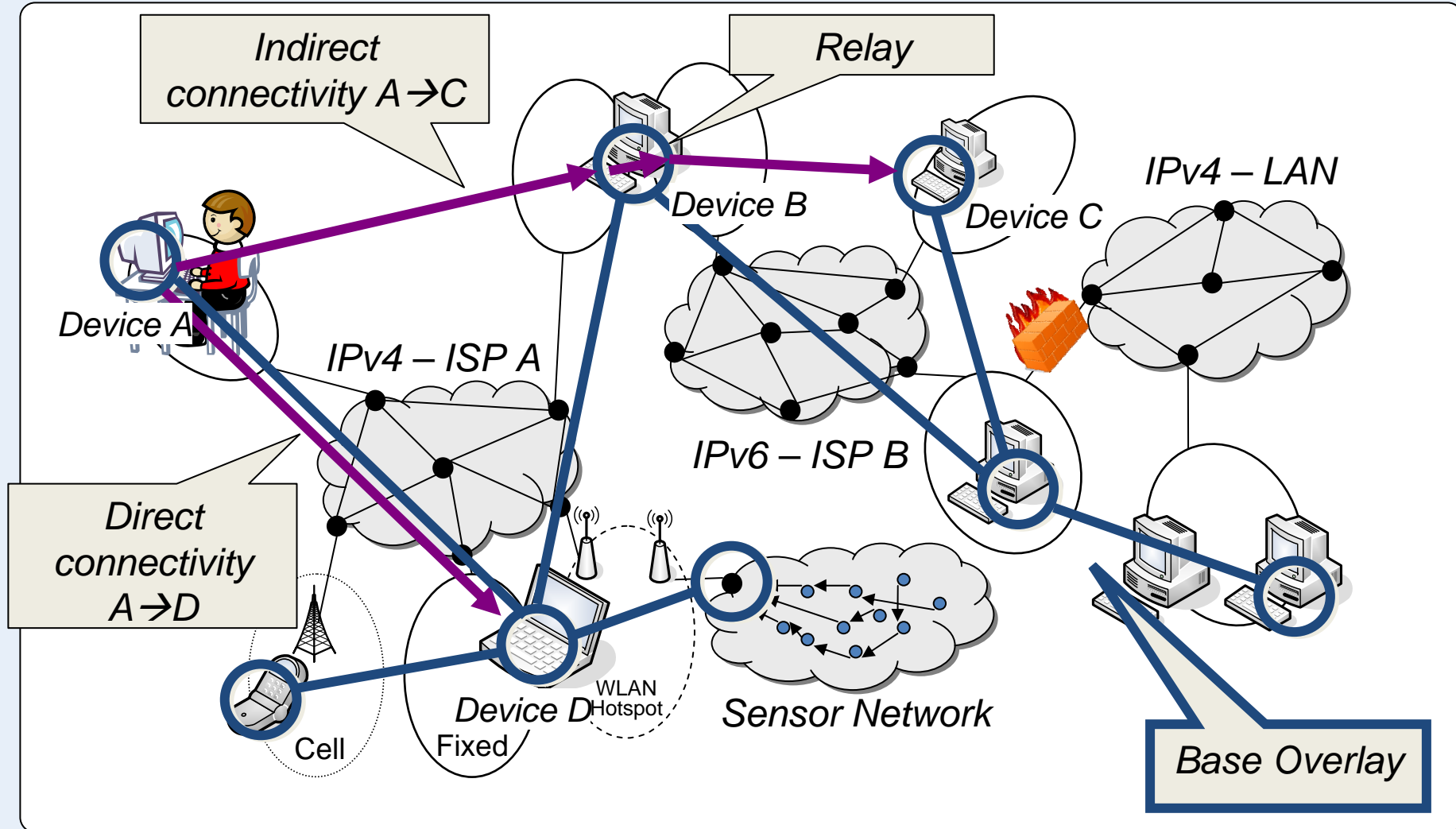
## 2. Addressing and namespaces



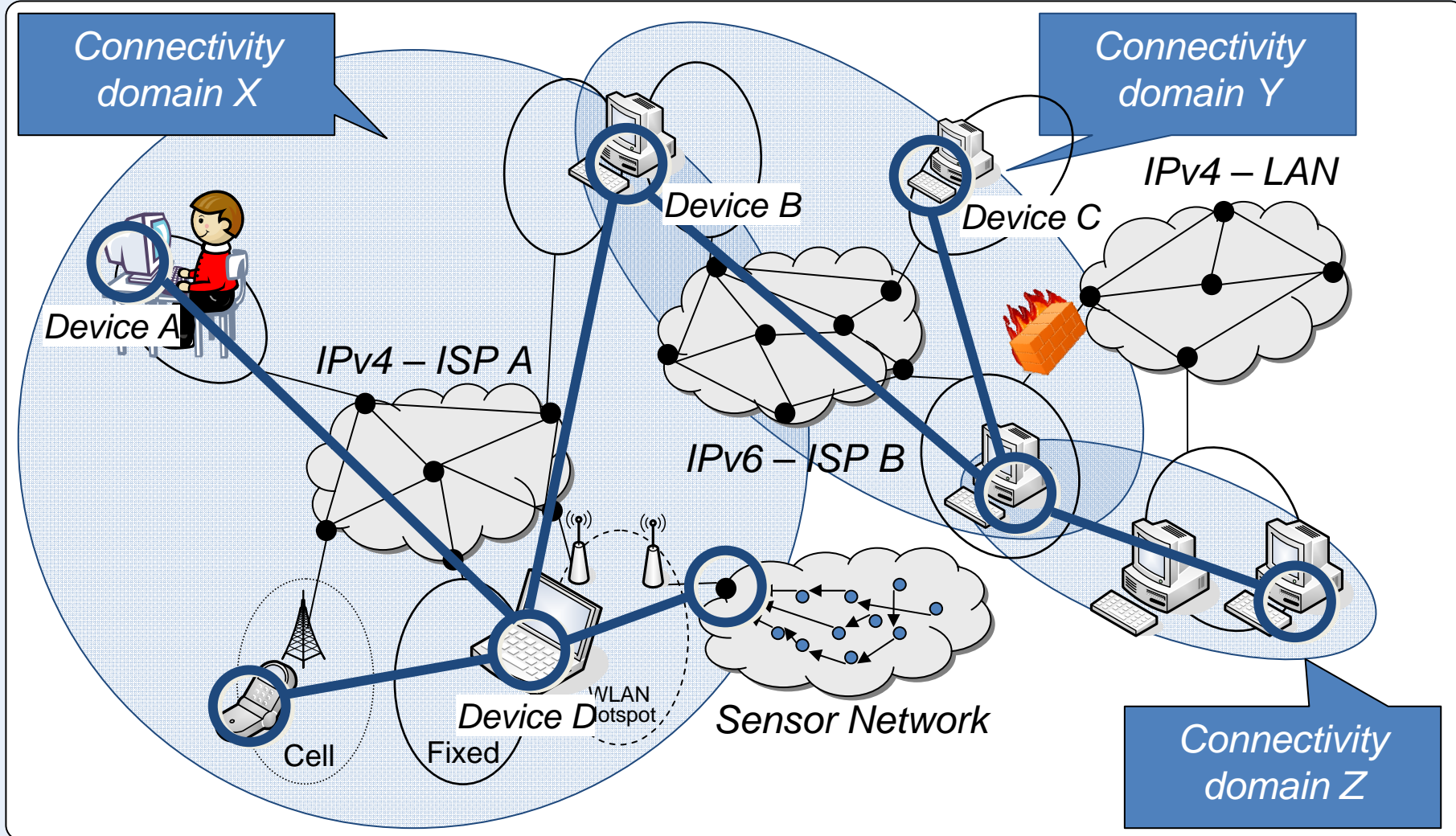
## 3. Integrated Security



# Connectivity



# Connectivity Domains

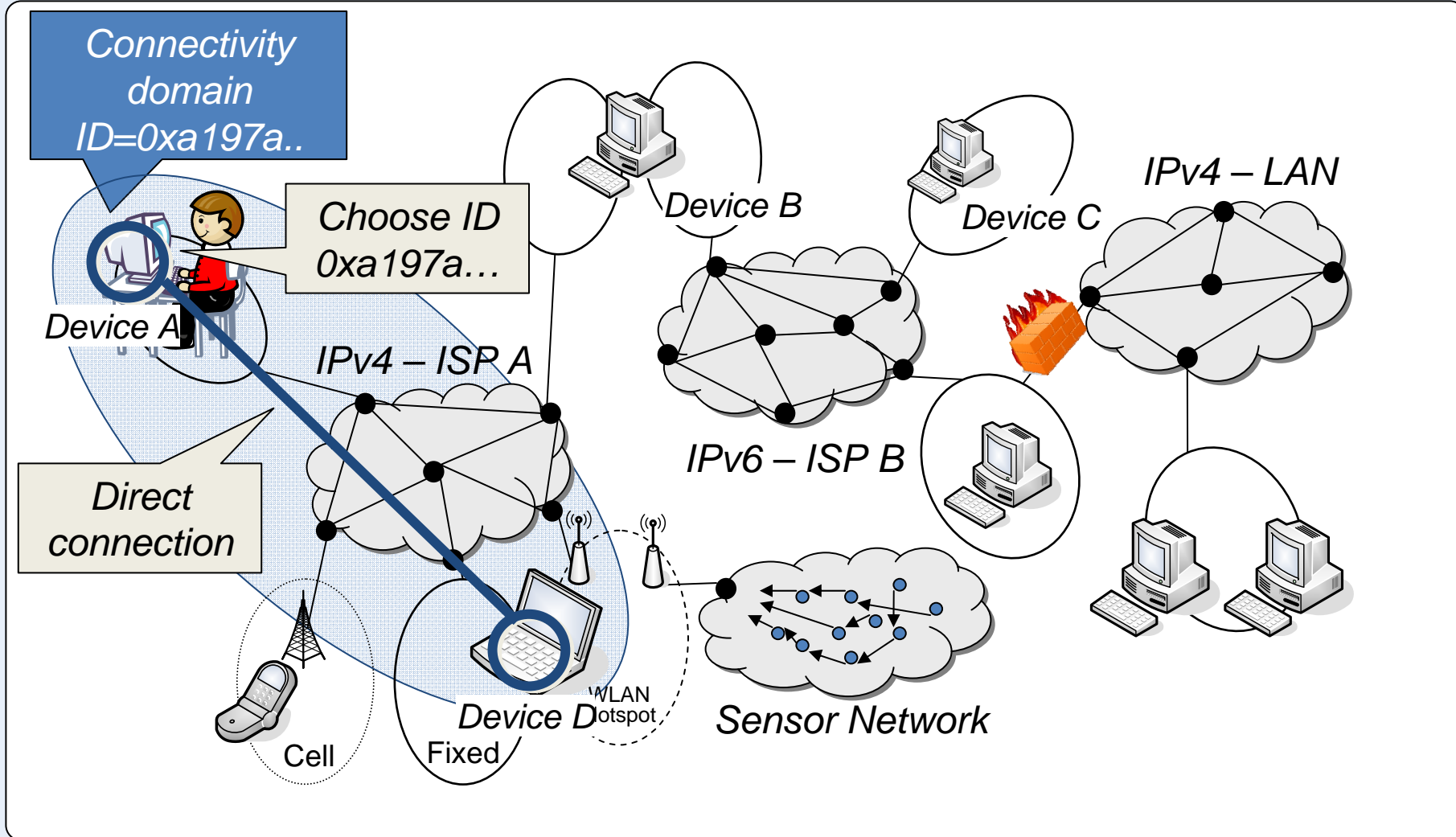


# Connectivity Domains



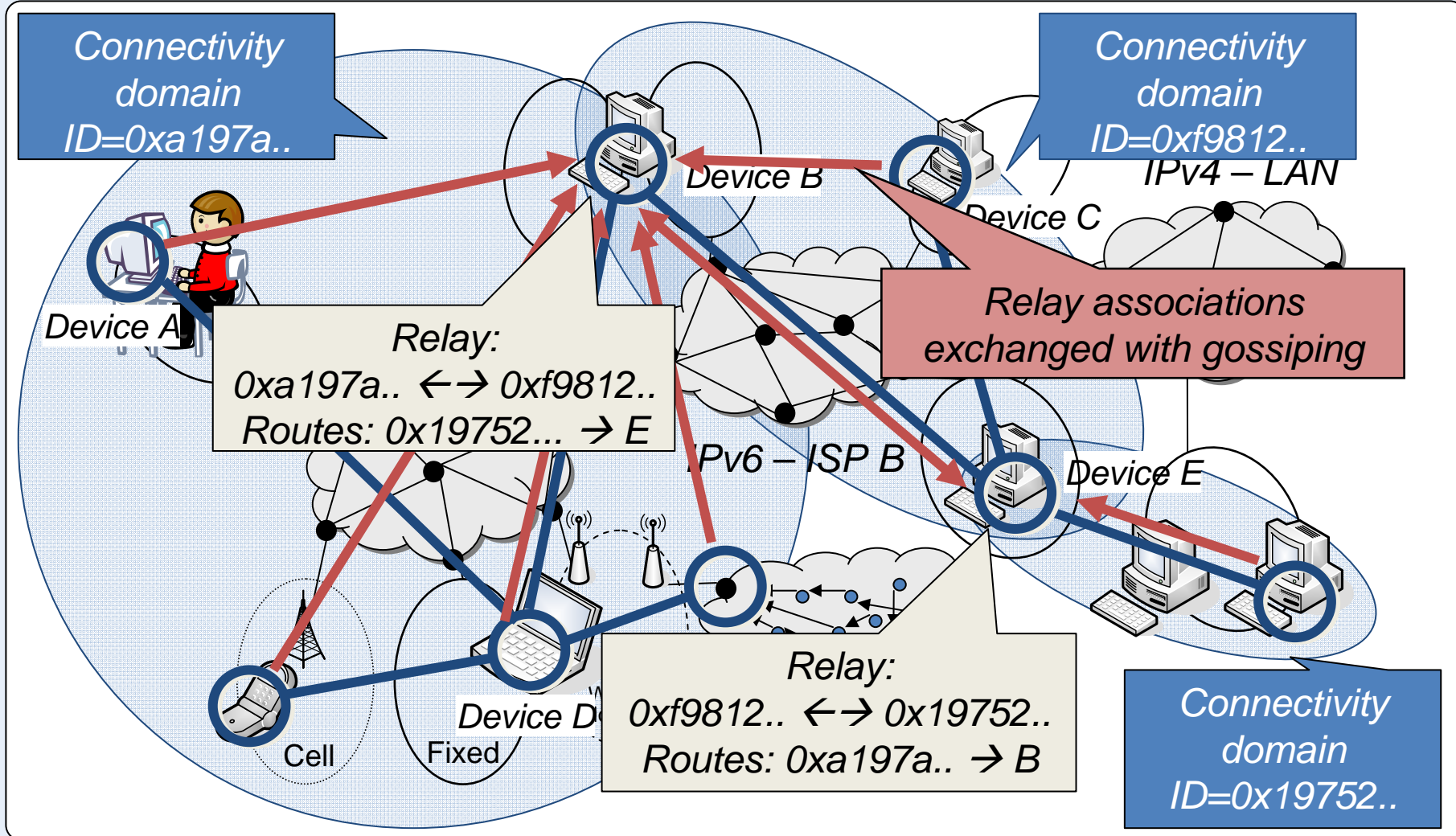
- Problem outline
  - Detect connectivity domains and relays
  - Establish links across connectivity domains
  - Consider partitioning and merging
- Our first solution
  - Identification of connectivity domains with probabilistically unique identifiers
  - Detection of relays
  - Simple link state protocol finds relay paths

# Detection Example





# Detection Example



# Connectivity Domains: Summary



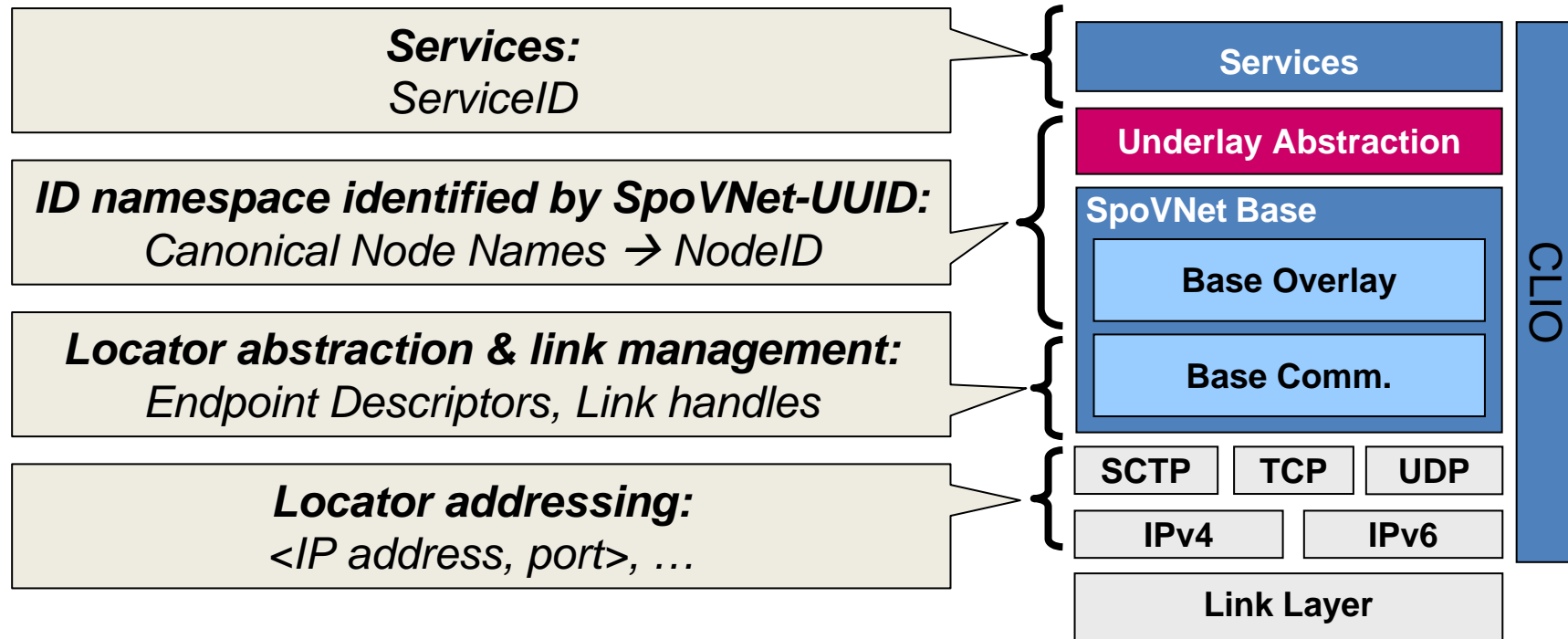
- First **pragmatic** approach allows
  - Distributed **detection** of connectivity domains
  - Provides **relay paths** to each domain
  - ➔ **Provides end-to-end connectivity across heterogeneous networks!**
- Further work
  - Algorithms to handle **partitioning** and **merging**
  - Optimization of relay paths with **virtual coordinates**

# Namespaces and Addressing

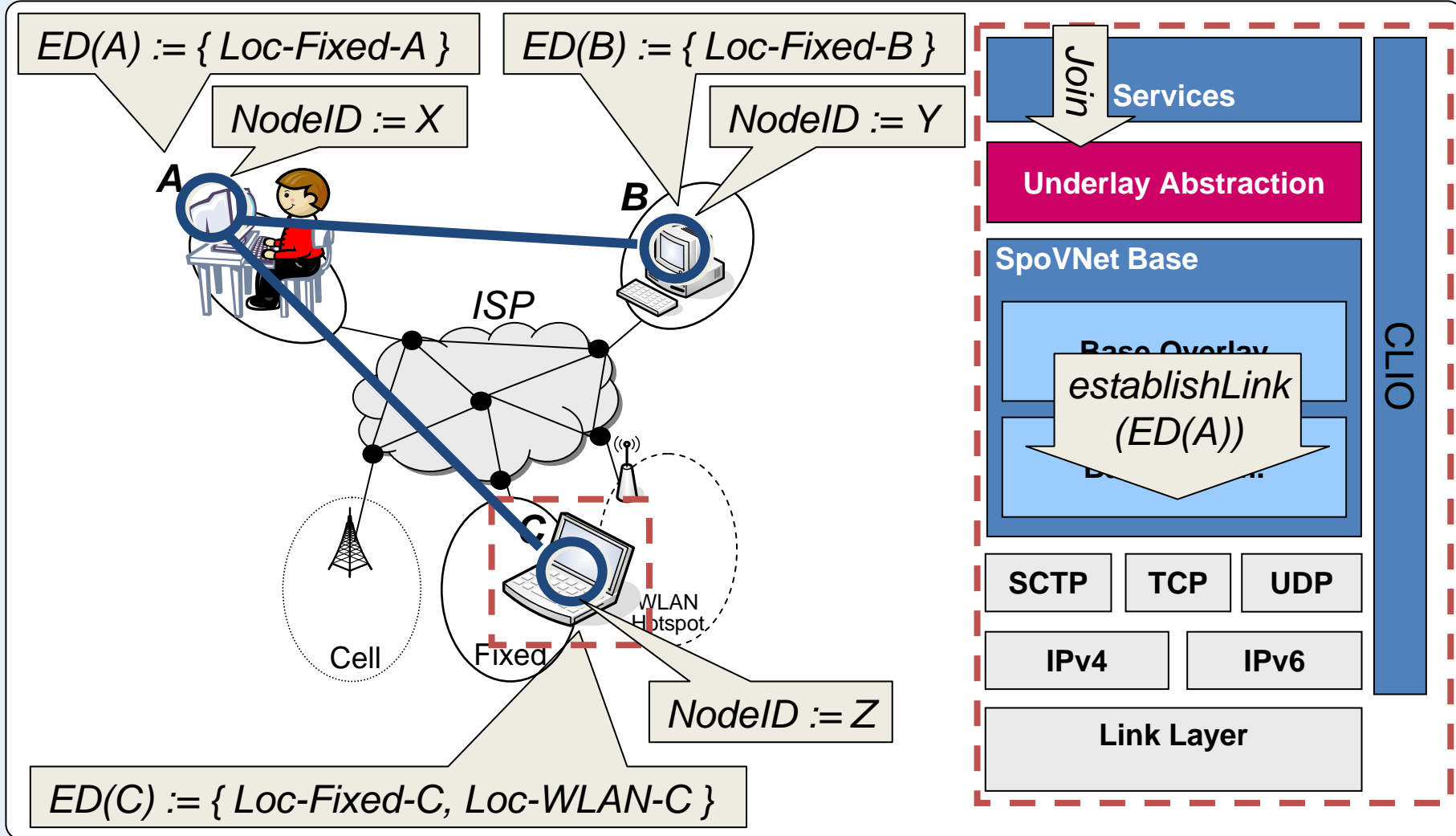


- Base Communication
  - Maintains all links between SpoVNet-Devices
  - Addressing with Endpoint Descriptors
  - Hides underlay addressing from higher layers
- Base Overlay
  - Forms SpoVNet-Instance with its own namespace identified by a SpoVNet-UUID
  - Nodes have Canonical Node Names (CNN)
  - CNNs are hashed to a routable node identifier (NodeID)
- ServiceID
  - Similar to the ports scheme in TCP/UDP
  - Identifies a service in a given node instance

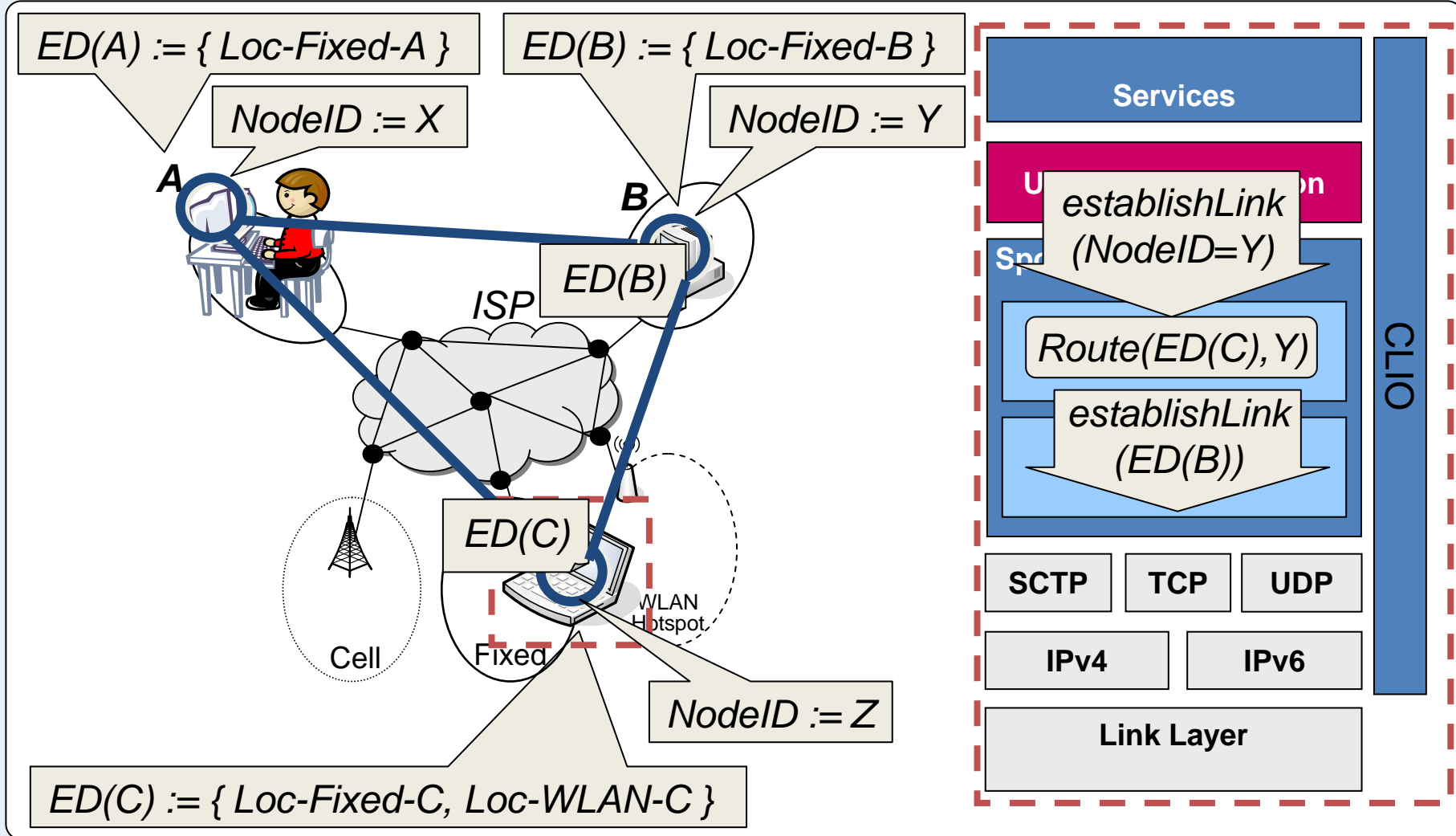
# Namespaces and Addressing



# Link establishment



# Link establishment

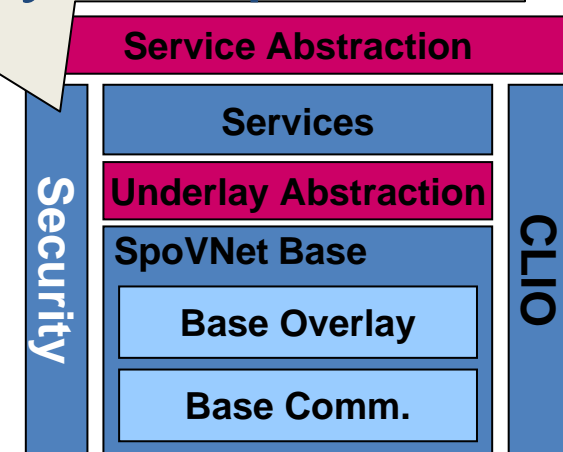


# Integrated Security Strategy

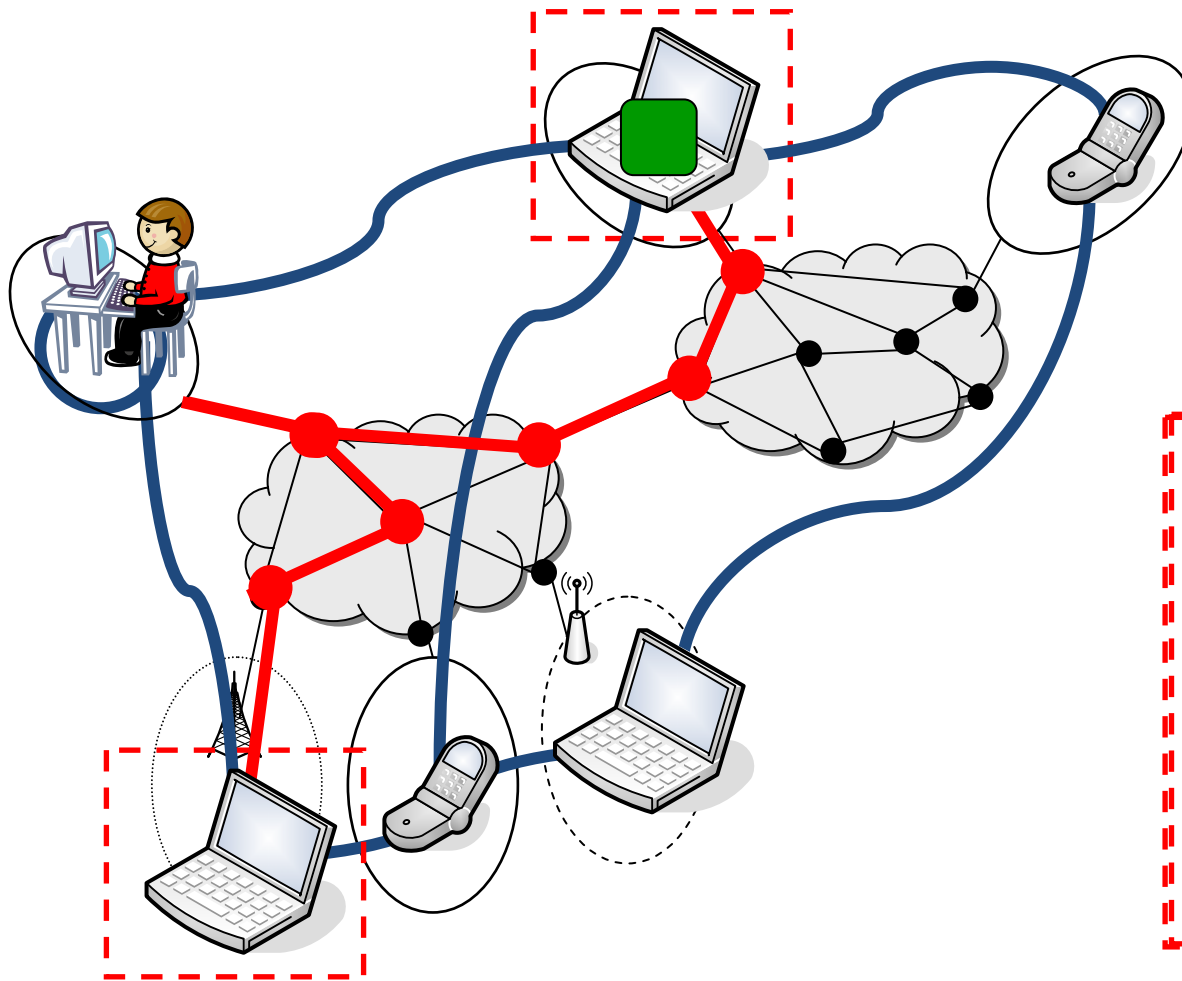


- Consider security as an **integral part** of the SpoVNet architecture
- Identify security sensitive operations **once** for each **service overlay**
- Check operations with **security component**  
→ Enforcement of **policies**

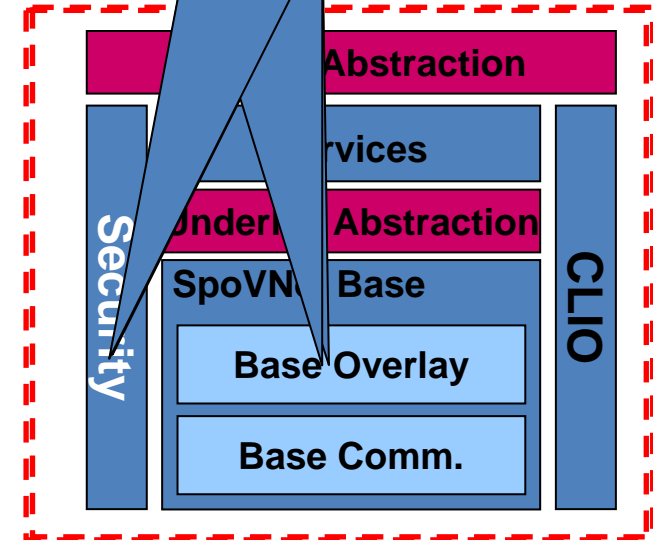
→ **Integrated Security**



# Exemplary Policy: Control Access



Verify the signed credential





# Summary



- SpoVNet's Communication Layers feature
  - Abstraction layer to many different underlays
  - Integrated security
  - Cross-Layer information
- Introduced here
  - Distributed connectivity domain detection
  - Unified location independent addressing and namespaces
  - Integrated Security: Authorization in SpoVNets
- Implementation
  - Currently under heavy development
  - ➔ **First preliminary open-source release end of 2008. Check <http://www.spovnet.de>!**



Thank you!

Questions?