

Towards a richer set of services in Software-Defined Networking

Roberto Bifulco, Ghassan O. Karame

Roberto.Bifulco@neclab.eu, Ghassan.Karame@neclab.eu



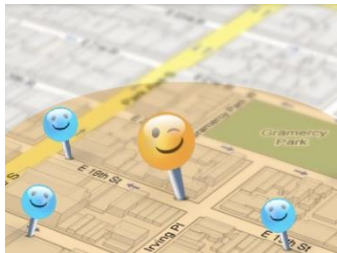
NEC Europe Ltd.,
NEC Laboratories Europe
Heidelberg, Germany

Table of contents

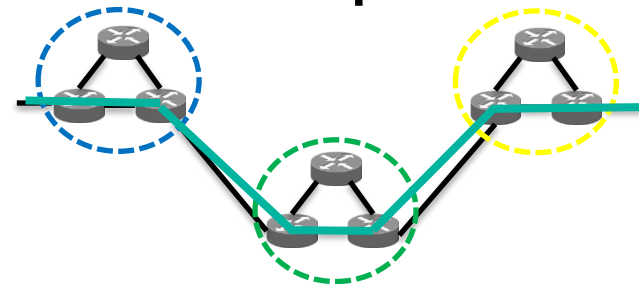
- Brief introduction to **SDN and OpenFlow**
- **Network Location Proof (NPoL)**
- **User-defined path (UdP)**

■ Can we exploit SDN to build network services that are just too complicated to implement in traditional networks?

- **Location proofs**

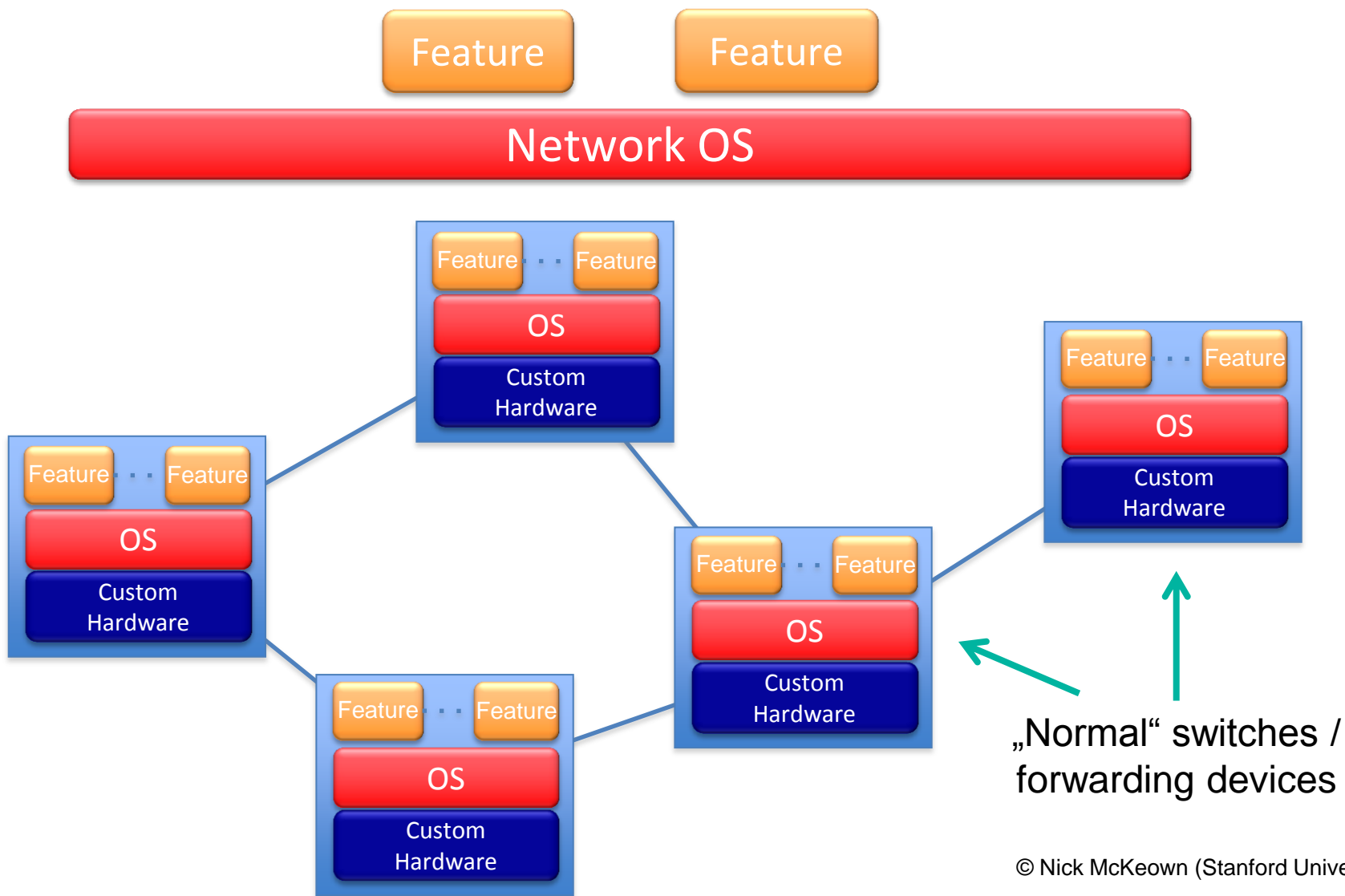


- **User-defined path**



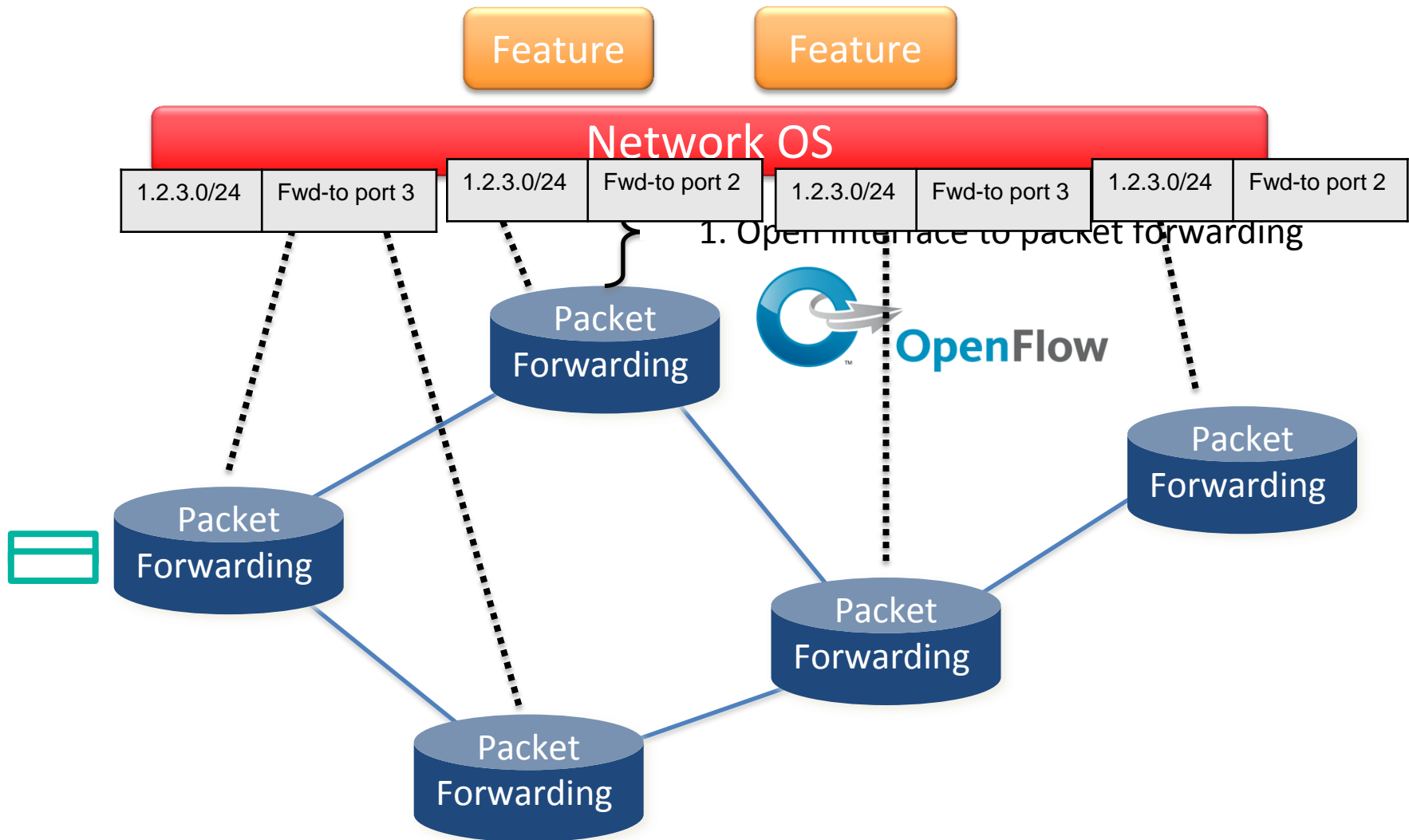
SDN: SOFTWARE-DEFINED NETWORKING

Software Defined Networking



© Nick McKeown (Stanford University)

Software Defined Networking



This is not a future vision. It's here

New industry forum assures interoperability



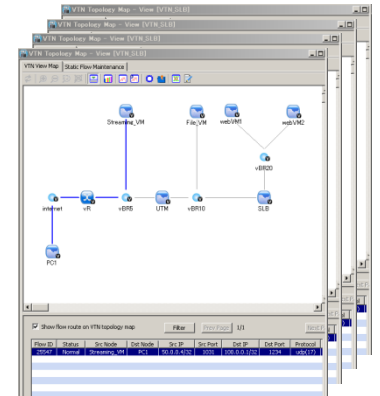
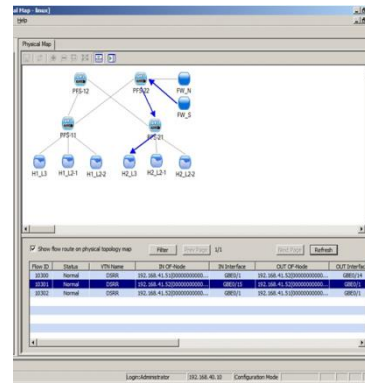
- Define OpenFlow Protocol
- Promote **Software-Defined Networking (SDN)**
- 7 board members, > 70 regular members

Board Members



SDN in the Data Center:

NEC's ProgrammableFlow



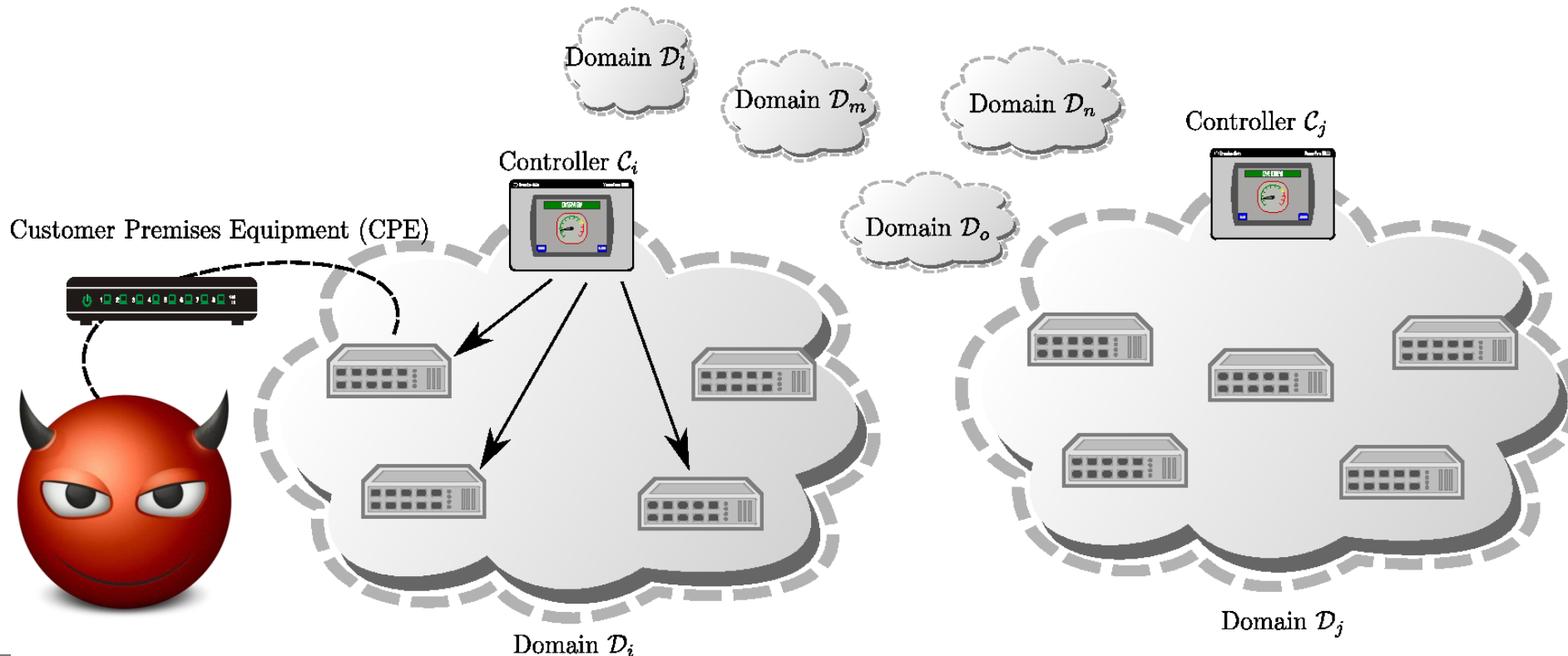
SDN in the backbone:

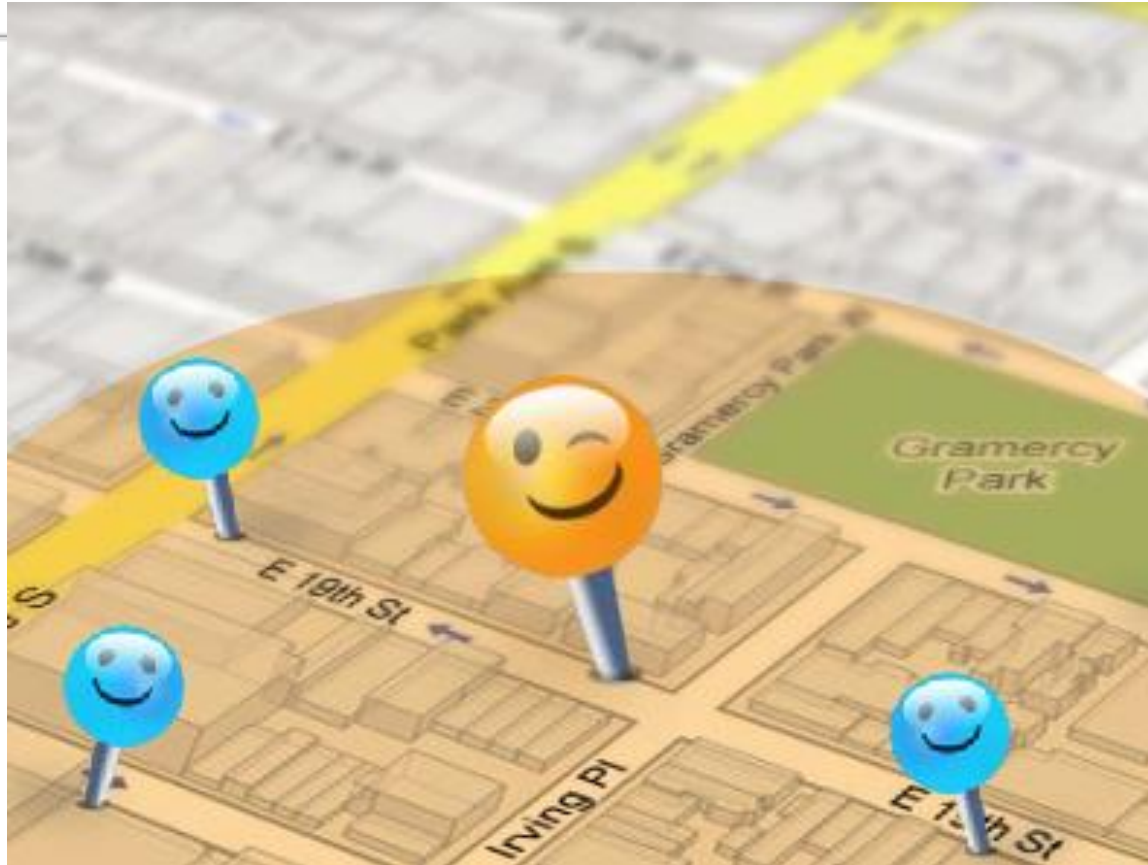
Google's OpenFlow WAN



System and attacker model

- Domain D_i is **Controlled** by Controller C_i ;
- Controller C_i is equipped with public/private **key pair**
- U_j belonging to D_i is equipped with public/private **key pair**
- The network Controller and **network components are trusted**
- Users want of course to **acquire** new services without being entitled to 😊

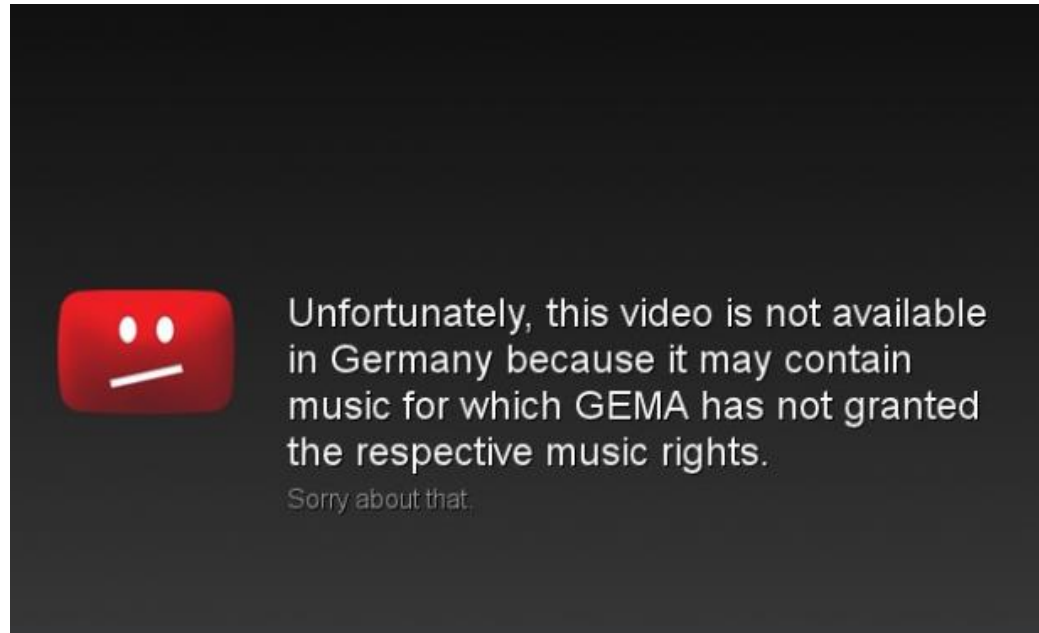




Location proof

“Location proofs” consist of a certificate that certifies the presence of a given entity at a certain location at some point in time.

Why location proofs?



Many services rely on **location information**

- Maybe many more will come...

Audio/video streaming, banking, voting, etc.

Current solutions to acquire location proofs are either **unreliable** (e.g., IP Geolocation) or require **ad hoc changes** to the network

Exploit SDN to provide location proofs

We provide location proof by:

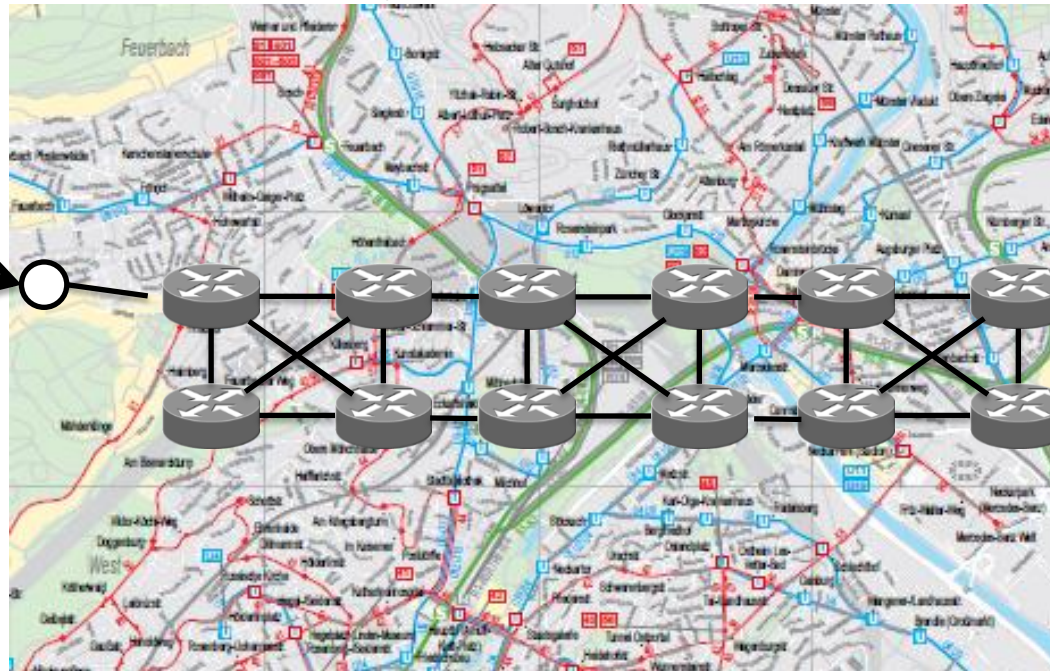
- guaranteeing that a given **IP address is present at a given location**;
- linking an **identity** to the IP address.

Required steps

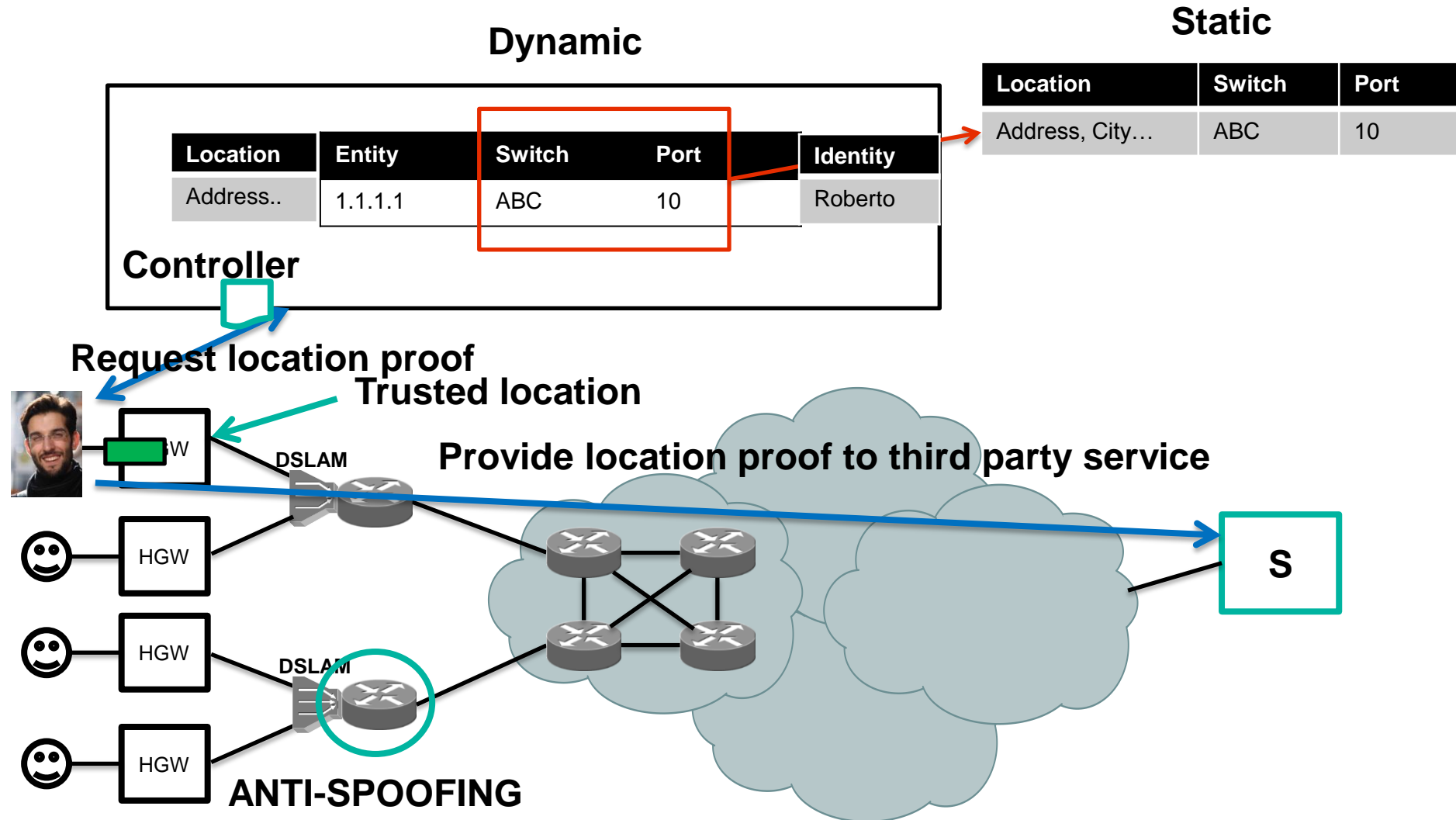
- Discover network location
- Relate network location to physical location
- Relate network flows to user identity



Roberto



NPoL: overview



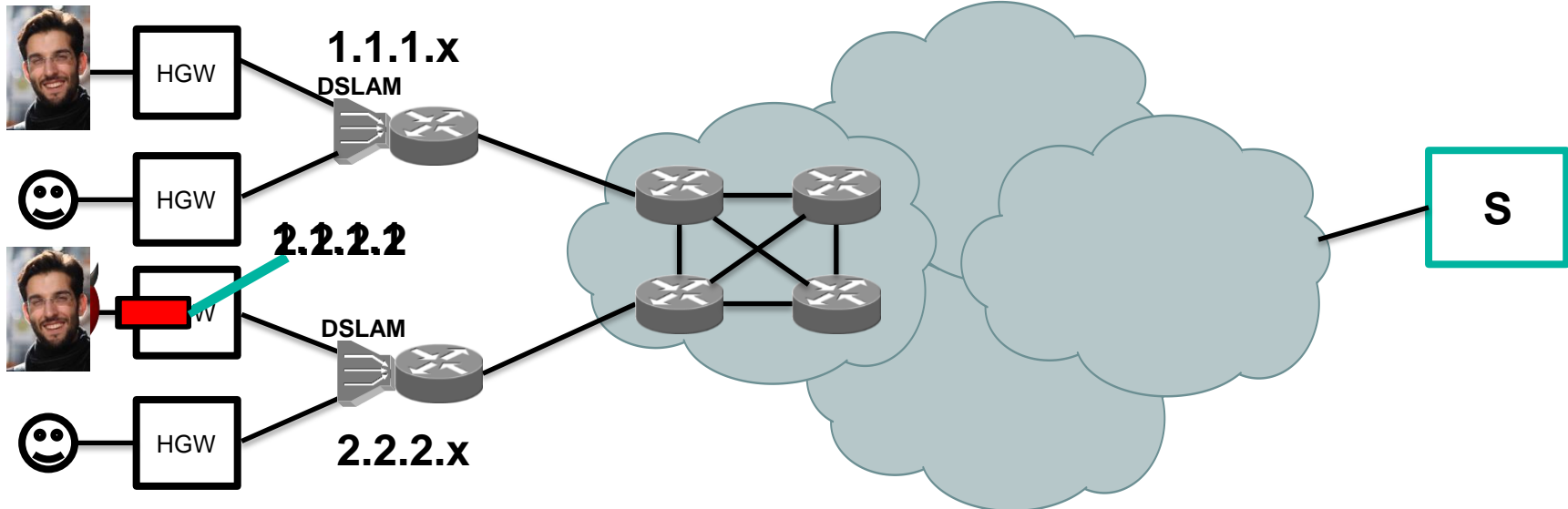
NPoL: attacks

Controller

| Location | Entity | Switch | Port | Identity |
|----------|---------|--------|------|----------|
| A | 1.1.1.1 | ABC | 10 | Roberto |

Roberto moved to location B

is it possible?

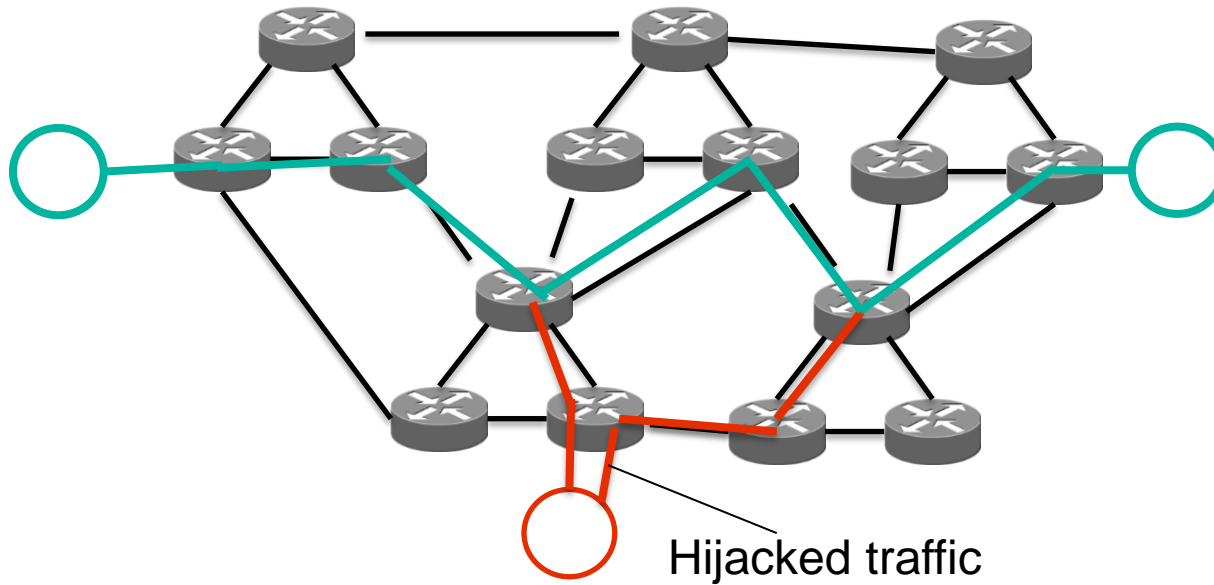




User-defined Path

A network path which obeys to user specific constraints

Why UdpP?



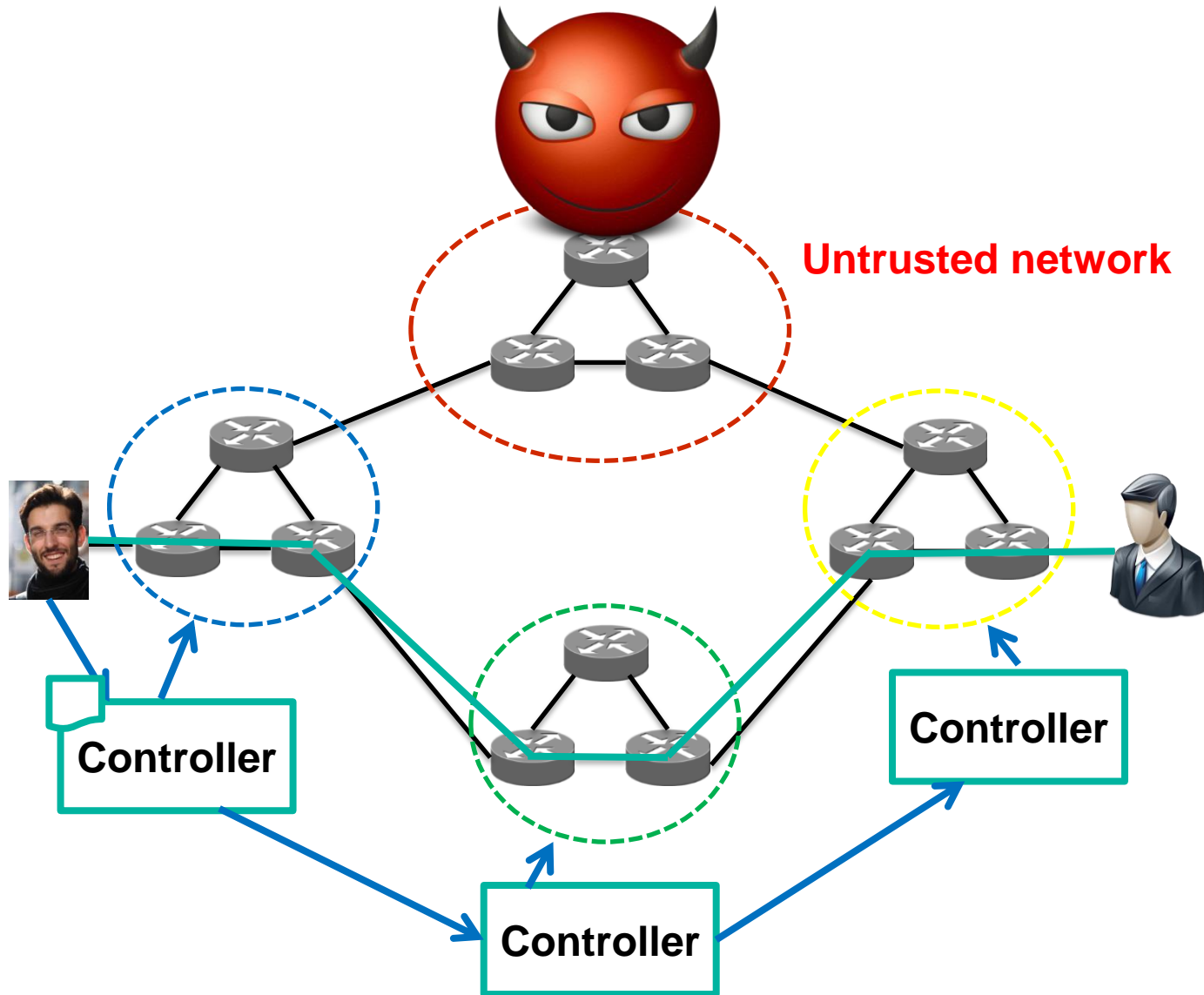
Untrusted ISPs

- Some authoritarian countries hijacking traffic

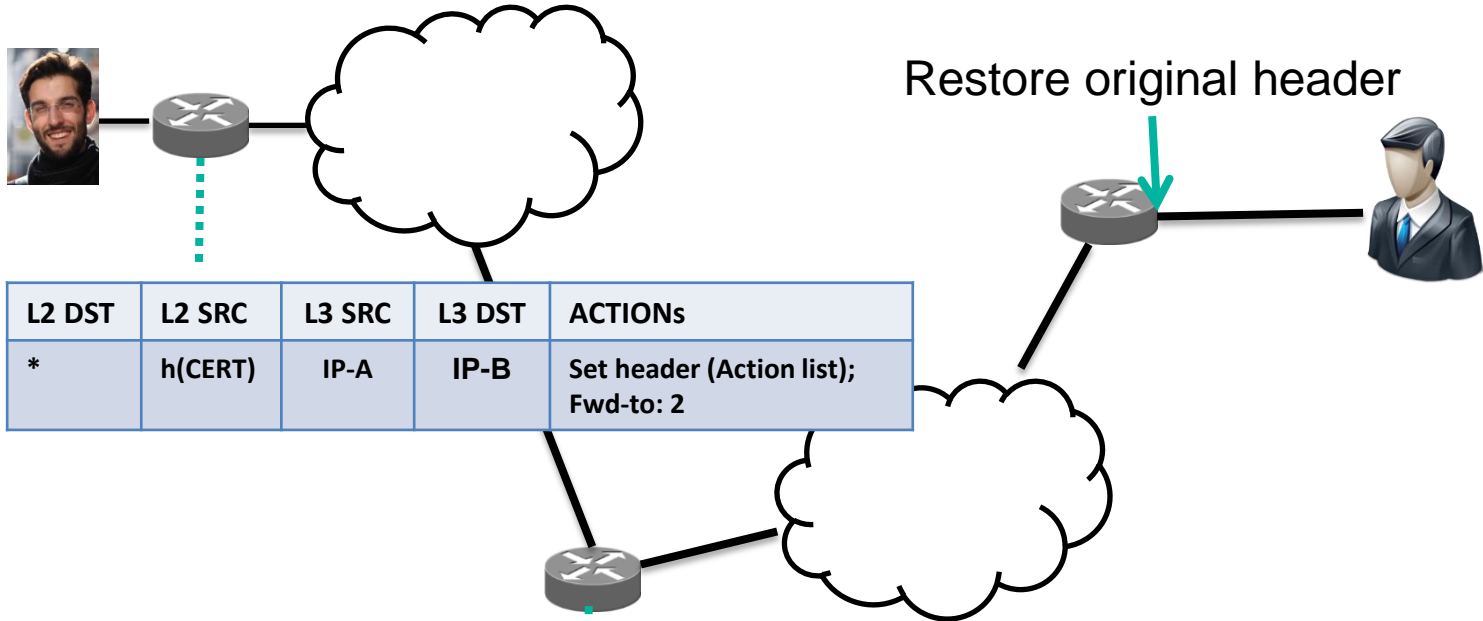
Improved QoS/dependability required by some applications

- E.g., telemedicine

UdP: overview



UdP: packet forwarding

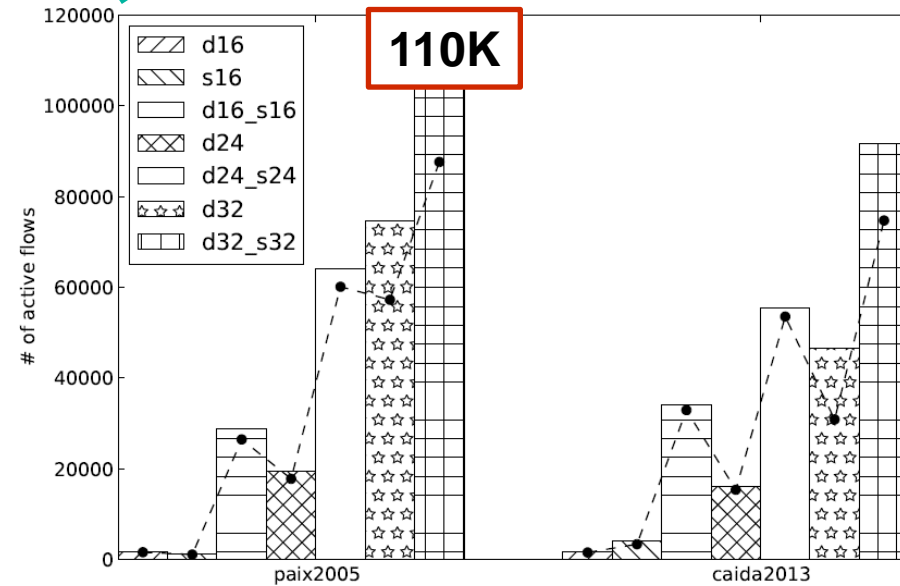
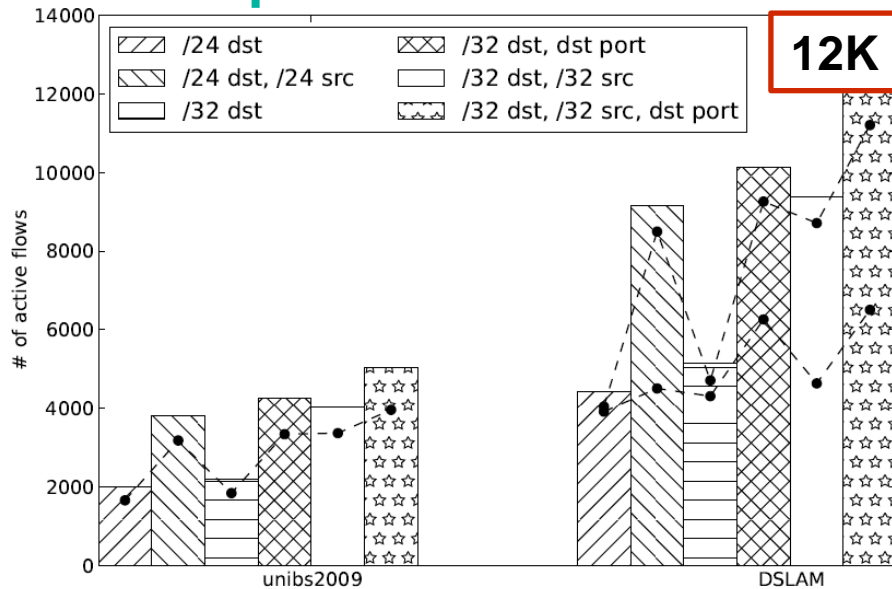
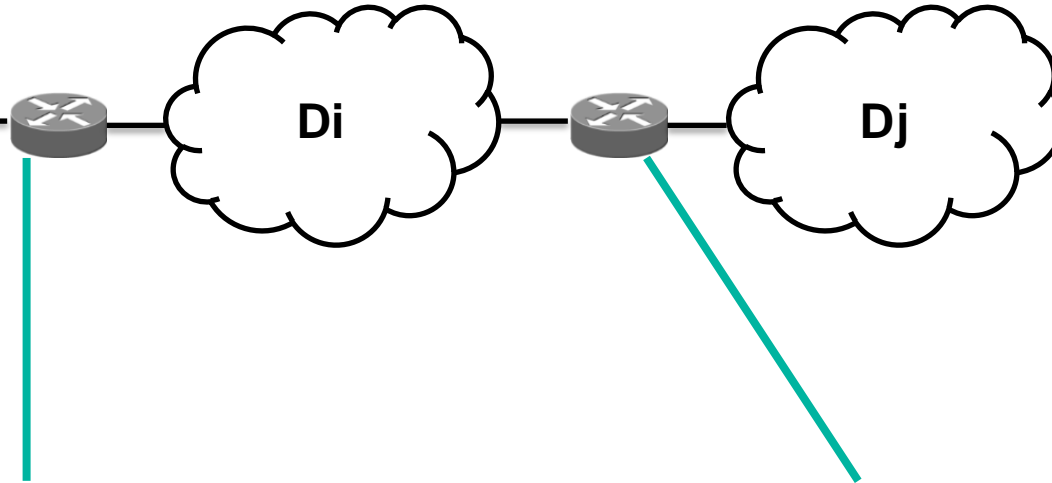


| L2 DST | L2 SRC | L3 SRC | L3 DST | ACTIONS |
|--------|---------|--------|--------|--|
| * | h(CERT) | IP-A | IP-B | Set header (Action list); Fwd-to: 2 |

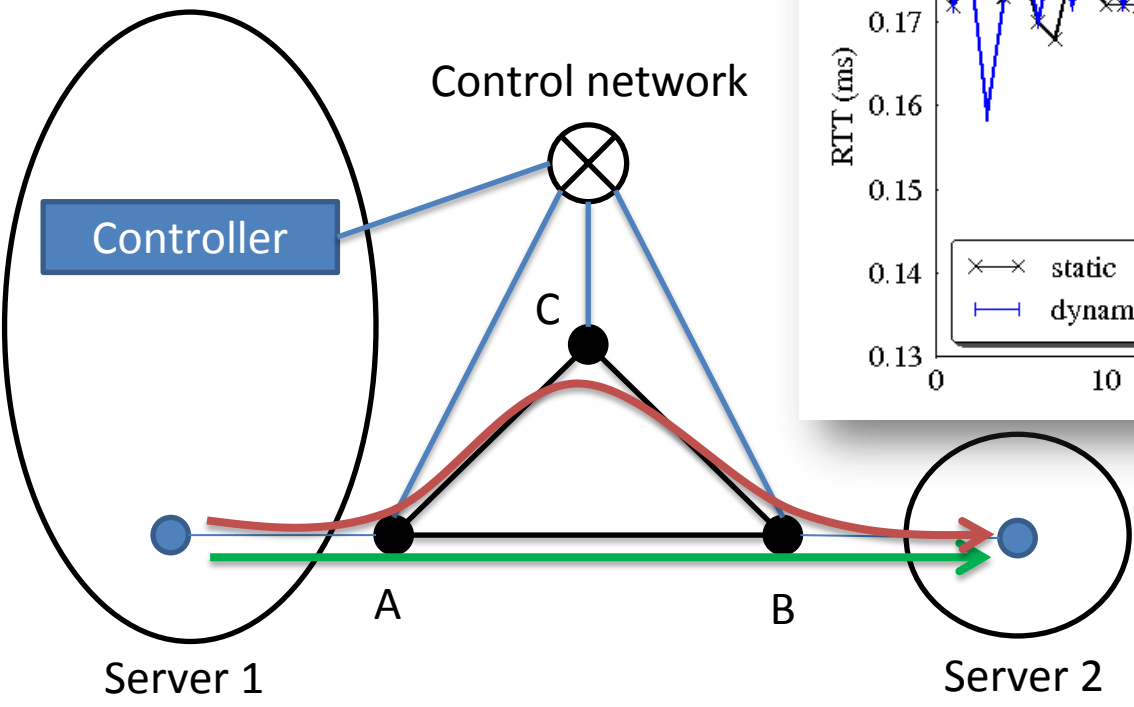
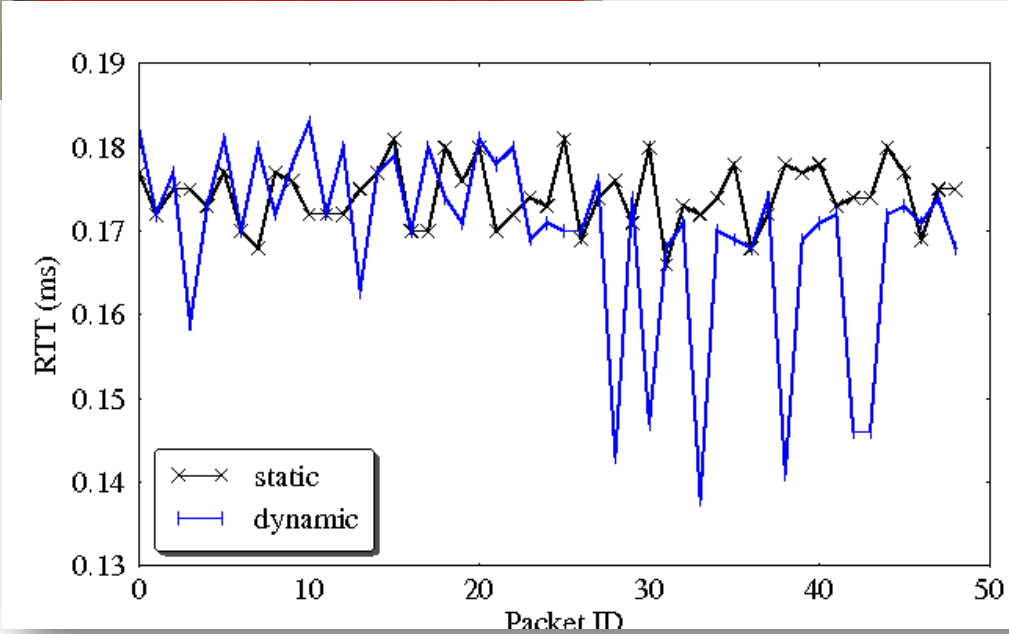
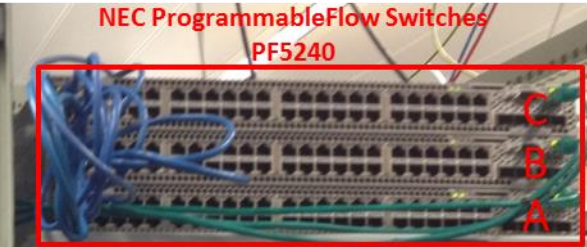
| Action list | | | Action pointer | ACTIONS |
|-------------|---|---|----------------|---|
| 3 | 1 | 4 | 2 | Increment pointer; Based on pointer; |

| Code | Action |
|------|------------|
| 1 | Fwd-to: 11 |
| 2 | Fwd-to: 5 |
| ... | ... |

UdP: Scalability



Implementation and evaluation



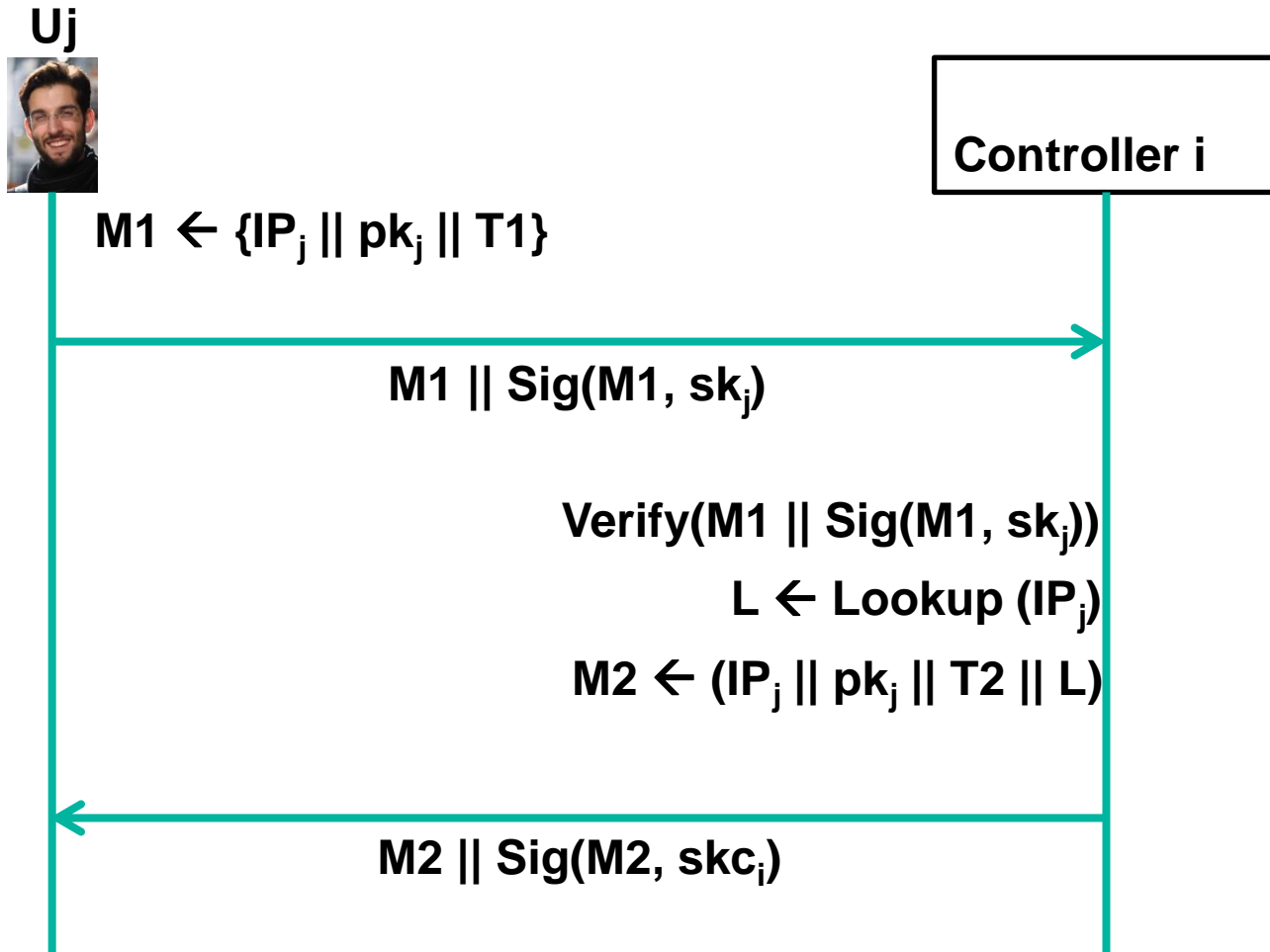
Conclusions

- SDN enables the creation of new services by exploiting the already deployed network infrastructure;
 - We implemented and evaluated two new network services: **NPoL** and **UdP**;
- Both services were implemented on a **SDN testbed** composed of hardware switches (OpenFlow-based)
- The solutions scalability has been validated using **real traffic traces** from both **access** and **core** networks
- NPoL** and **UdP** are two examples, what's next?
 - The network is not just a cloud (anymore)!

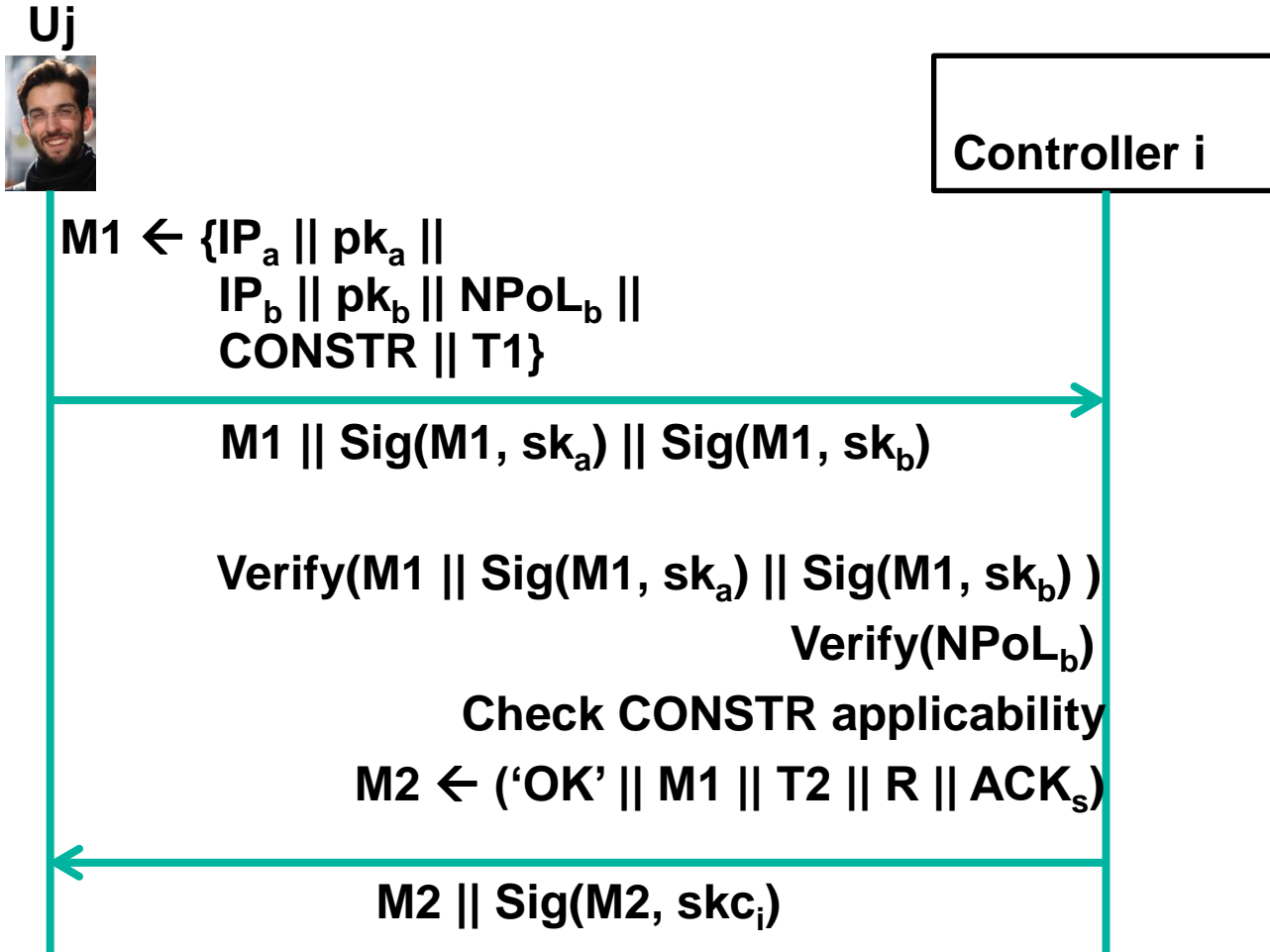
Empowered by Innovation

NEC

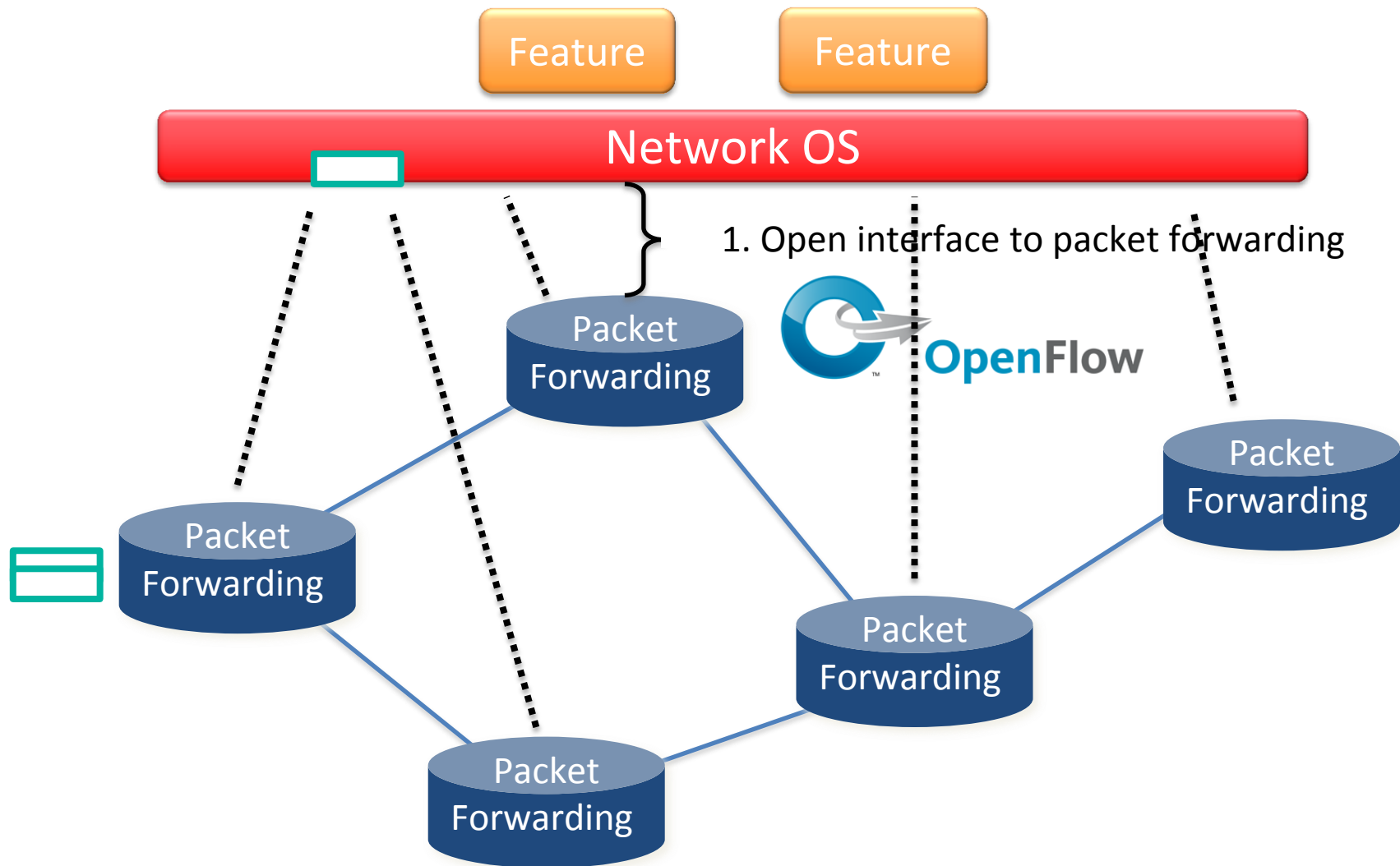
Asking for location proof



Asking for UdP



Software Defined Networking



© Nick McKeown (Stanford University)