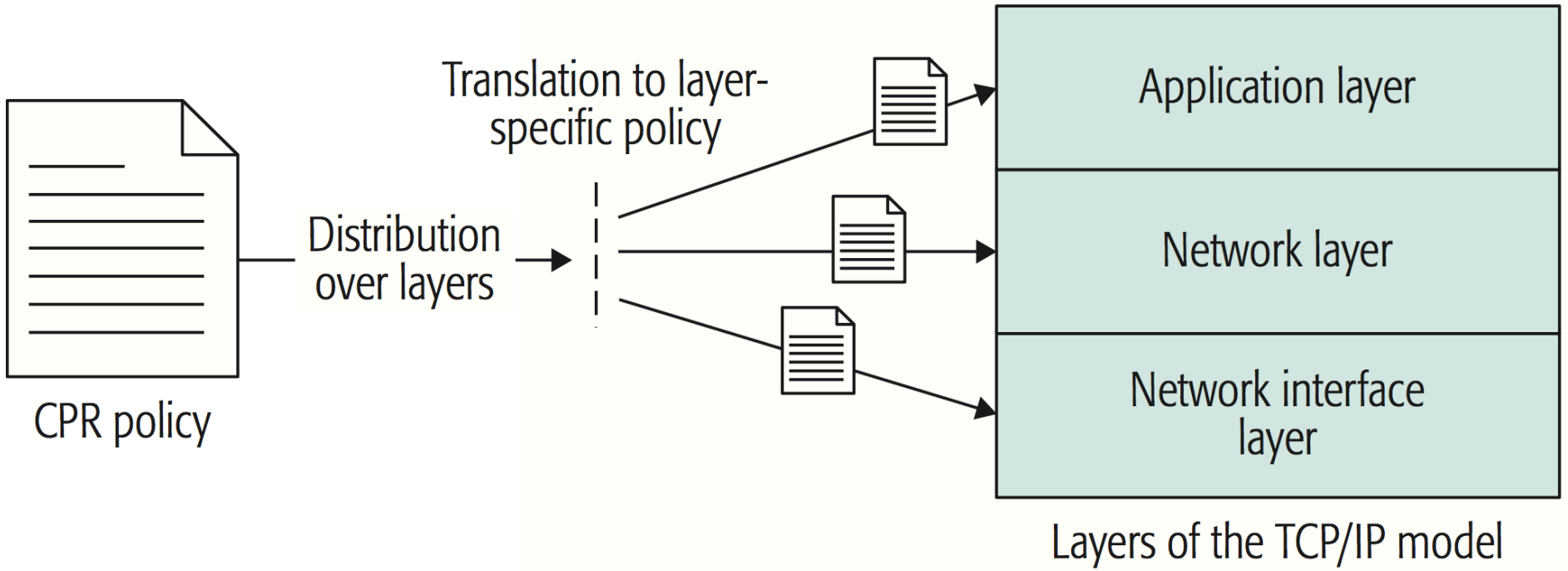
Data-centric security in software-defined networks

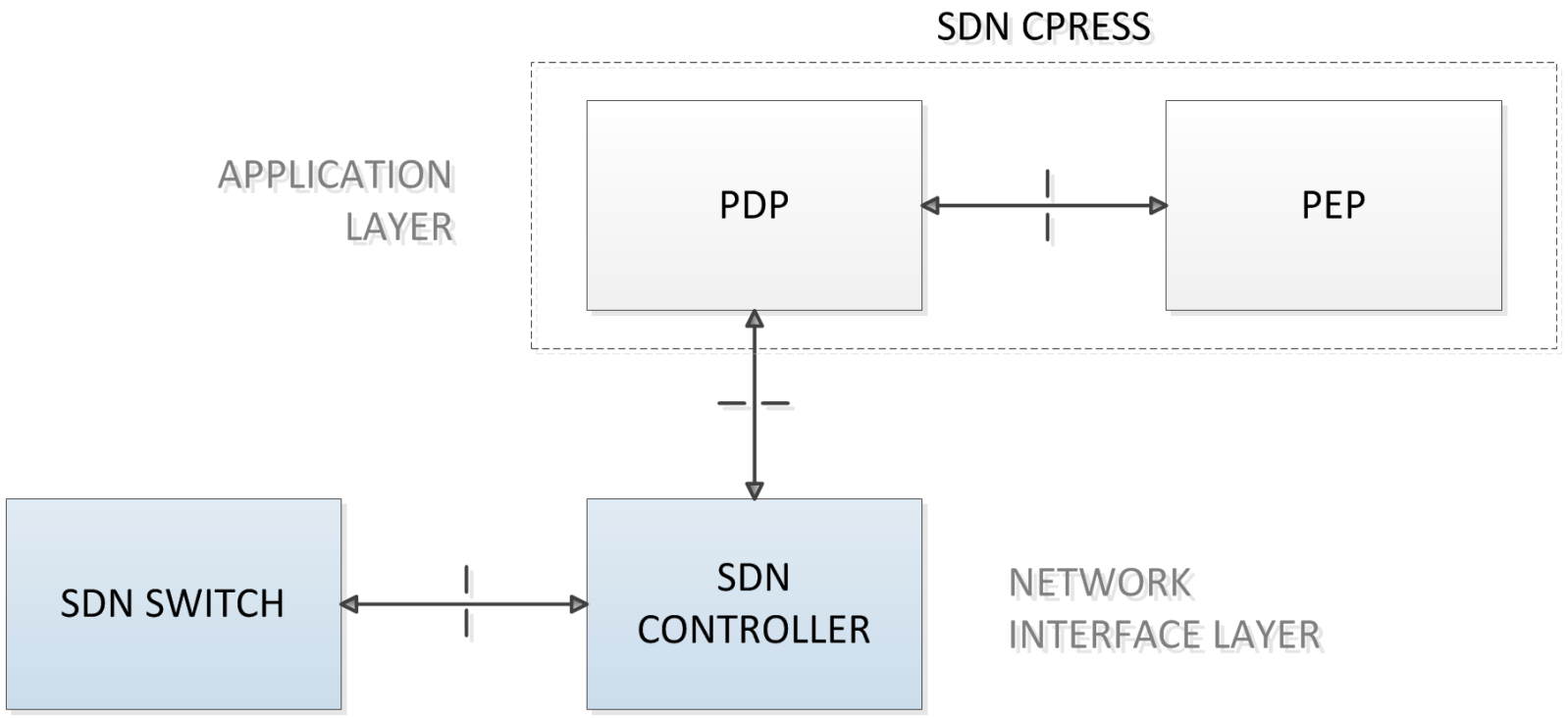
Dr.-Ing. Konrad Wrona

Lecture 6:
Data-centric security in software-defined networks

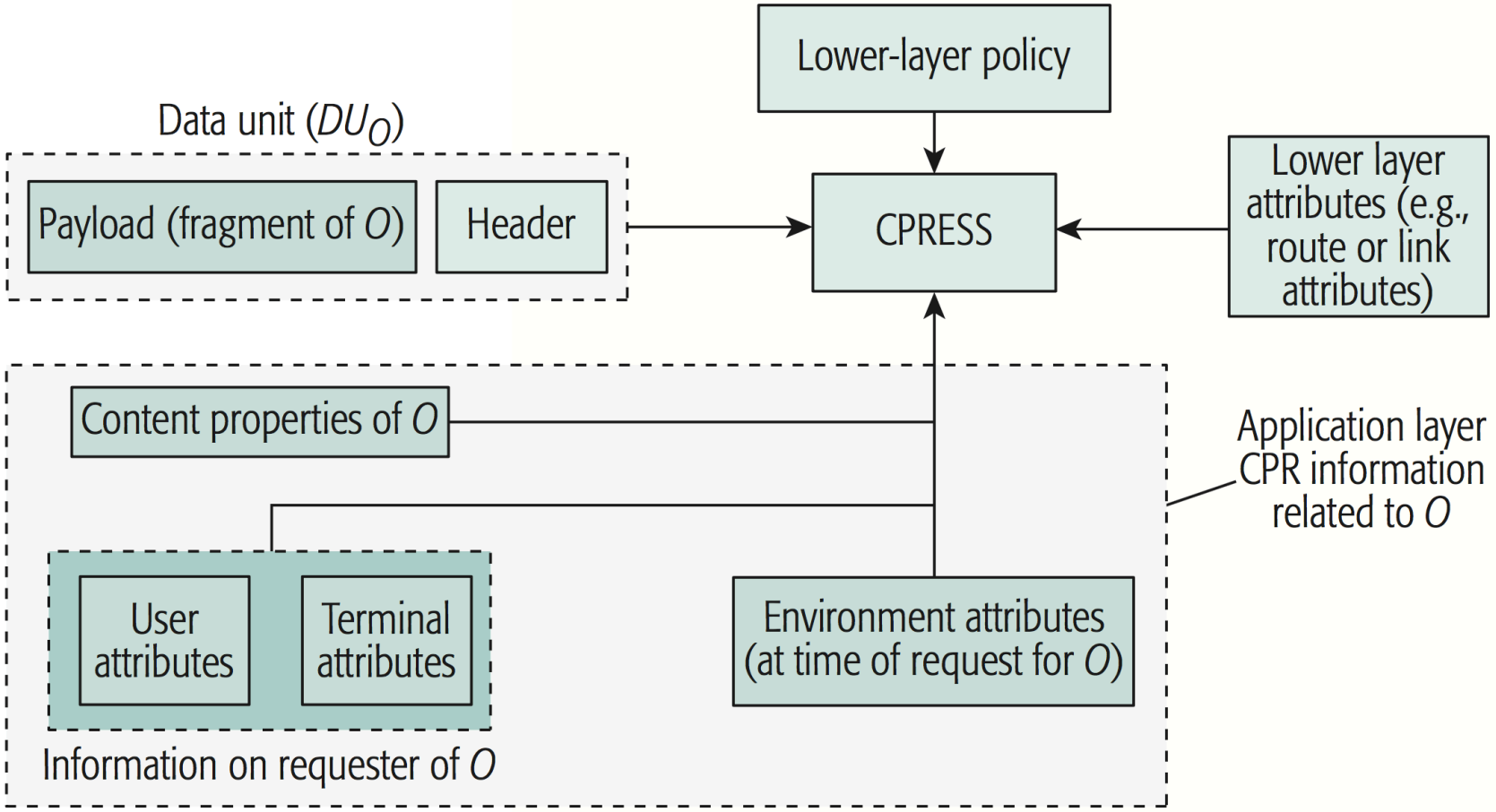
Cross-layer enforcement of DCS policies



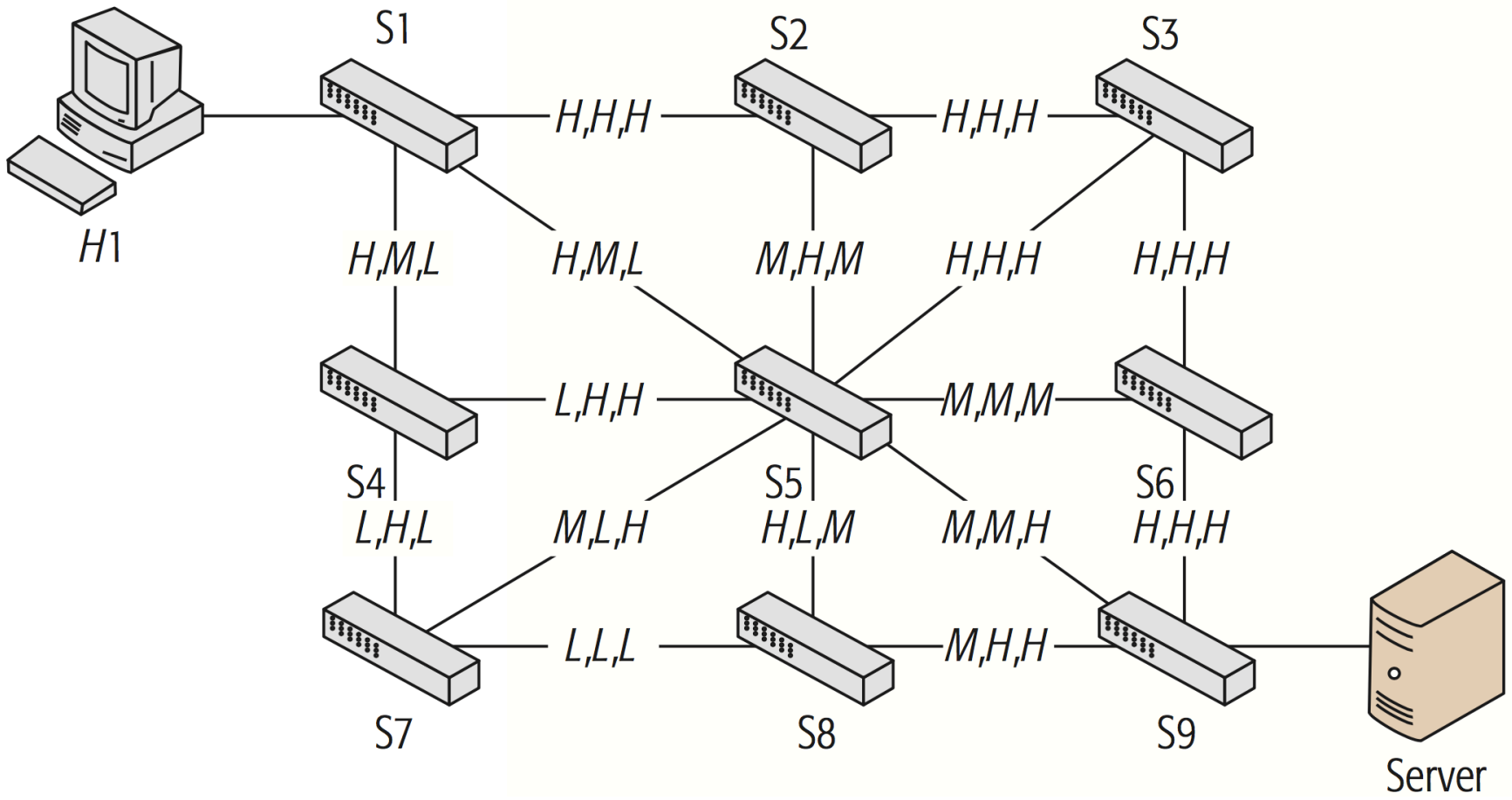
Enforcement of application-layer security policies in the network



Enforcement of application-layer security policies in the network

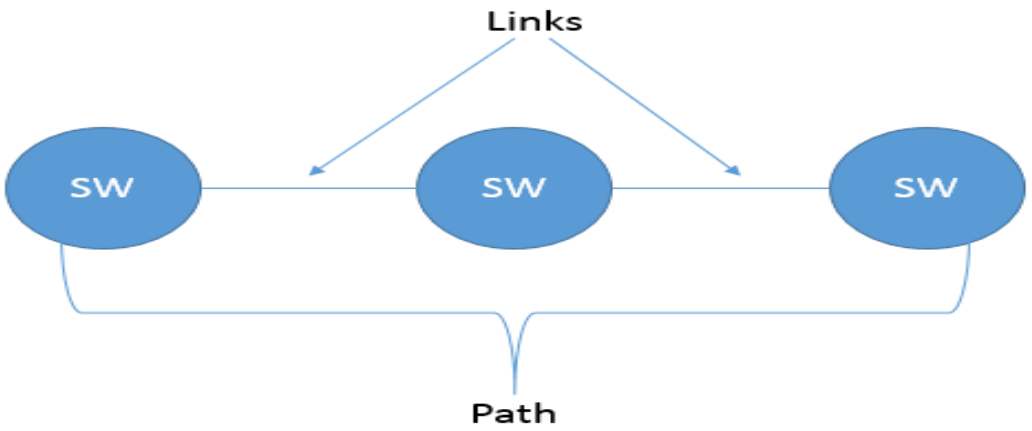


Data-centric software-defined networks



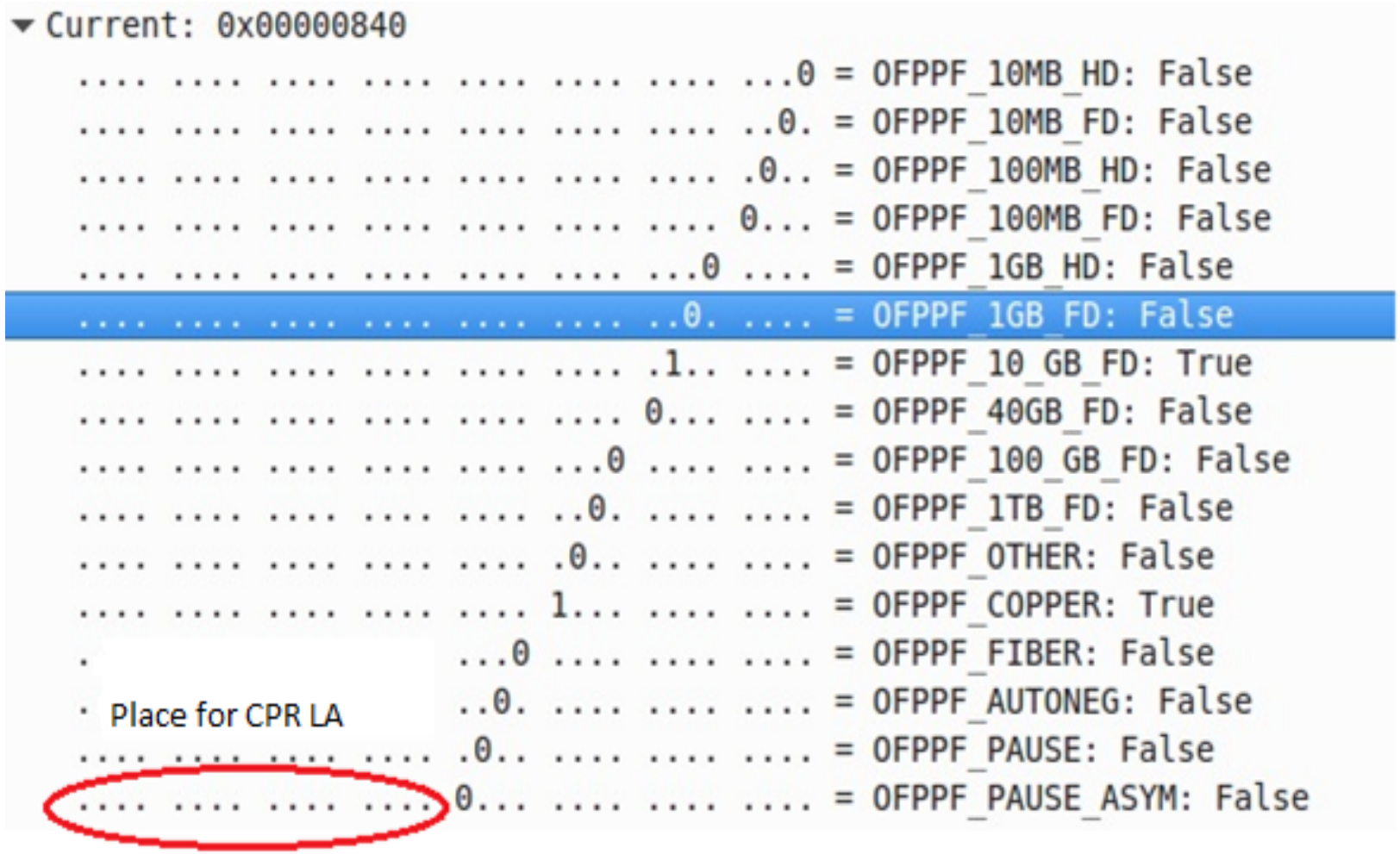
How to choose an optimally secure path?

- Path
  - Set of links between the switches in the SDN network



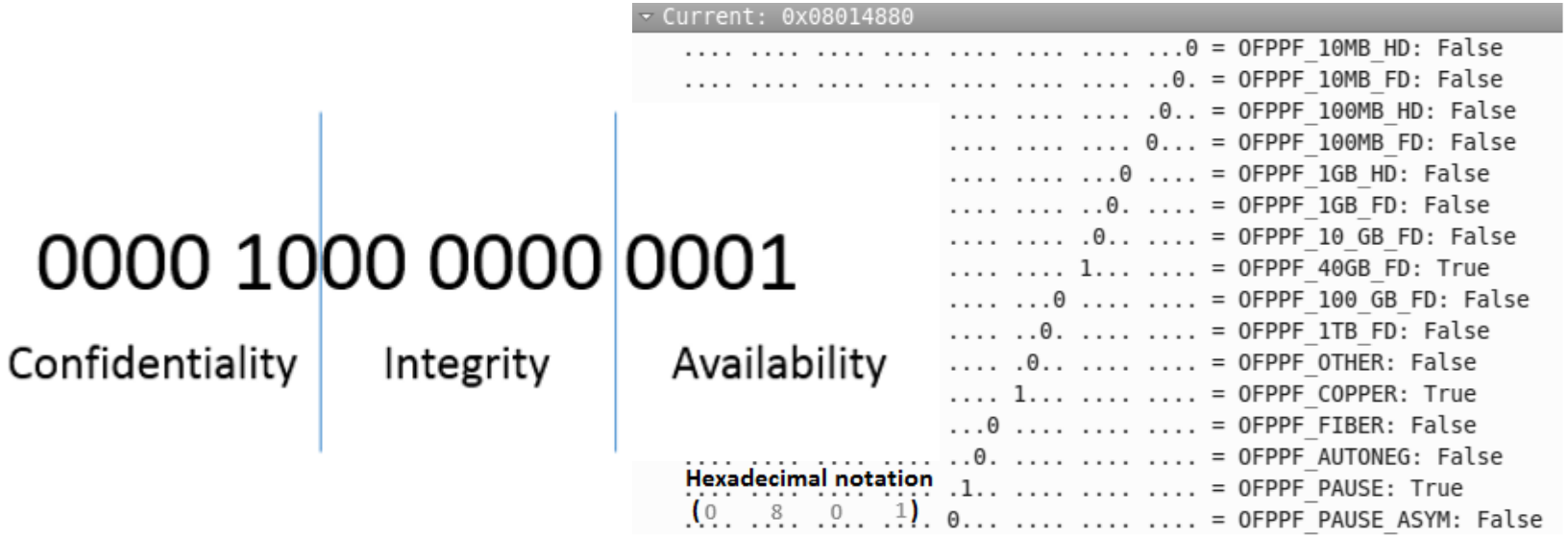
- Link Attributes
  - values which describes link properties

Open Flow Link Attributes: PORT_STATUS_REPLY message



Link Attributes in OpenFlow

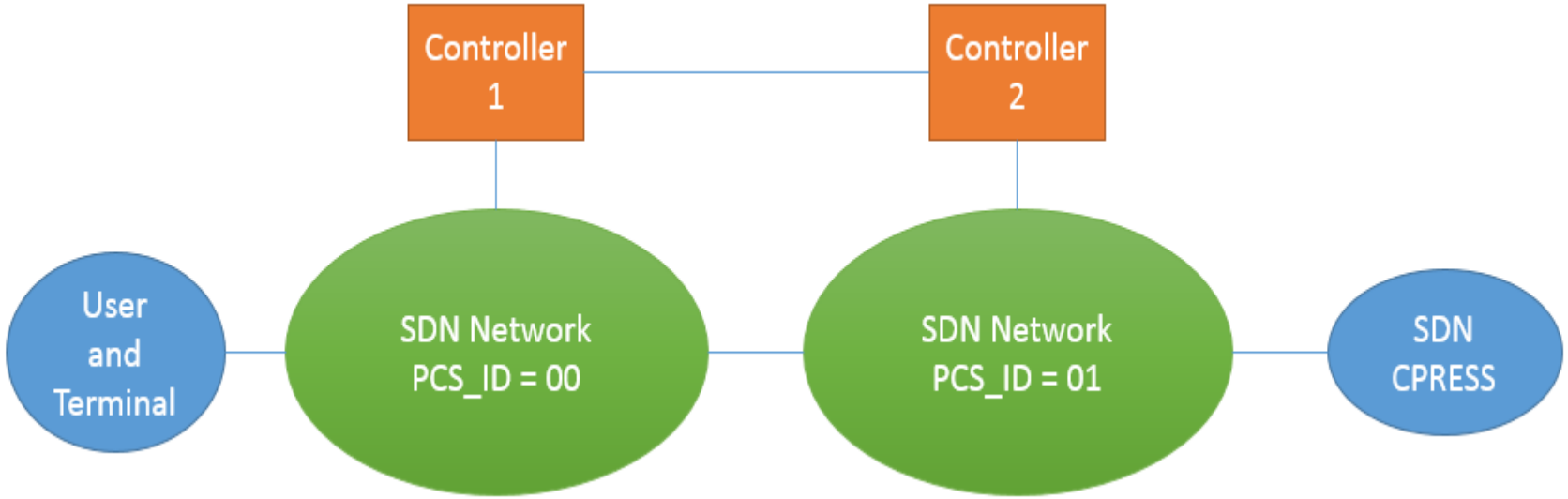
- Standard OpenFlow Link Attributes:
  - Bandwidth, Medium, Pause, Autonegotiation
- Extended CPR Link Attributes:
  - Confidentiality, Integrity, Availability



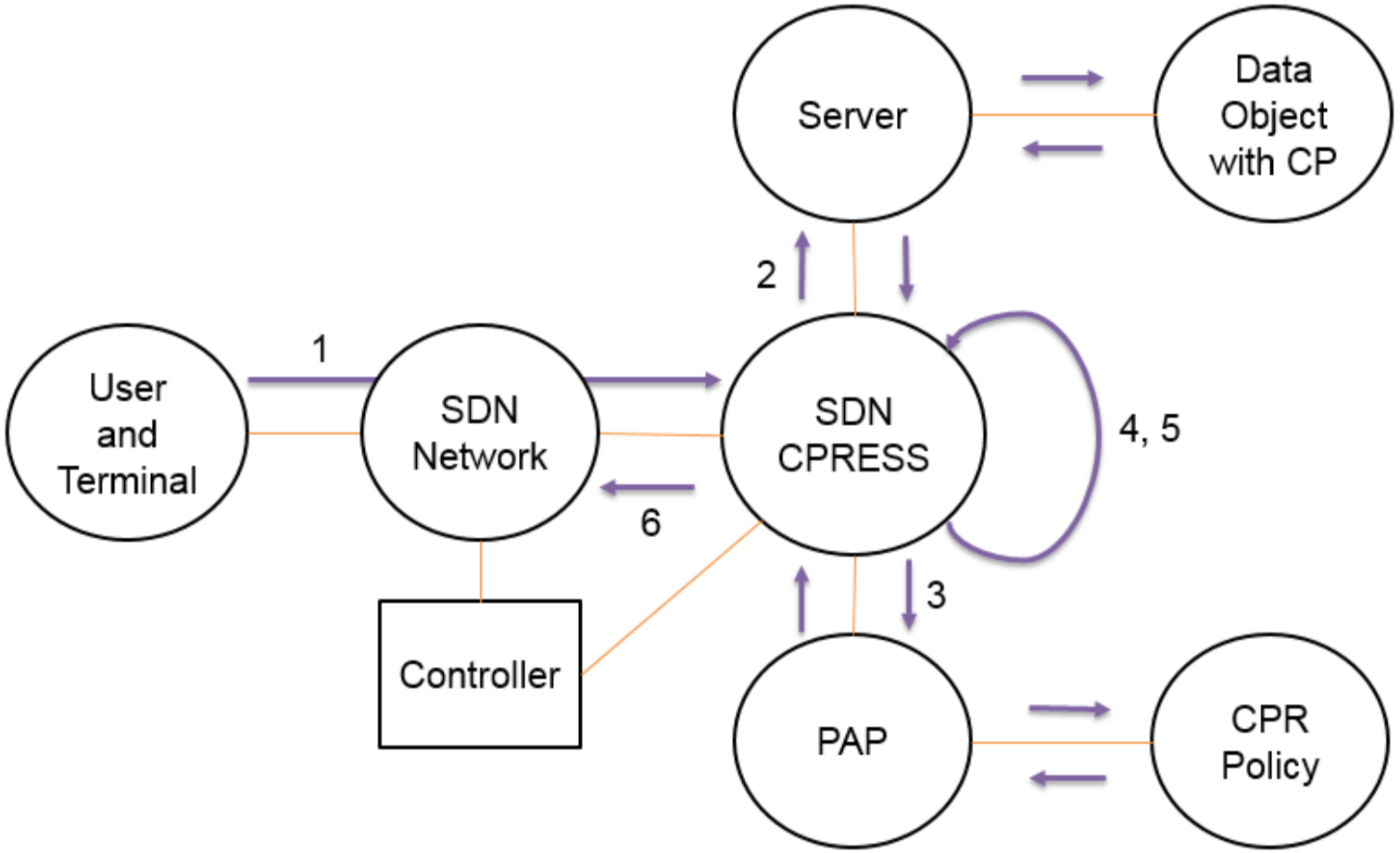
Sharing CPR LR between SDN networks

- EAI structure

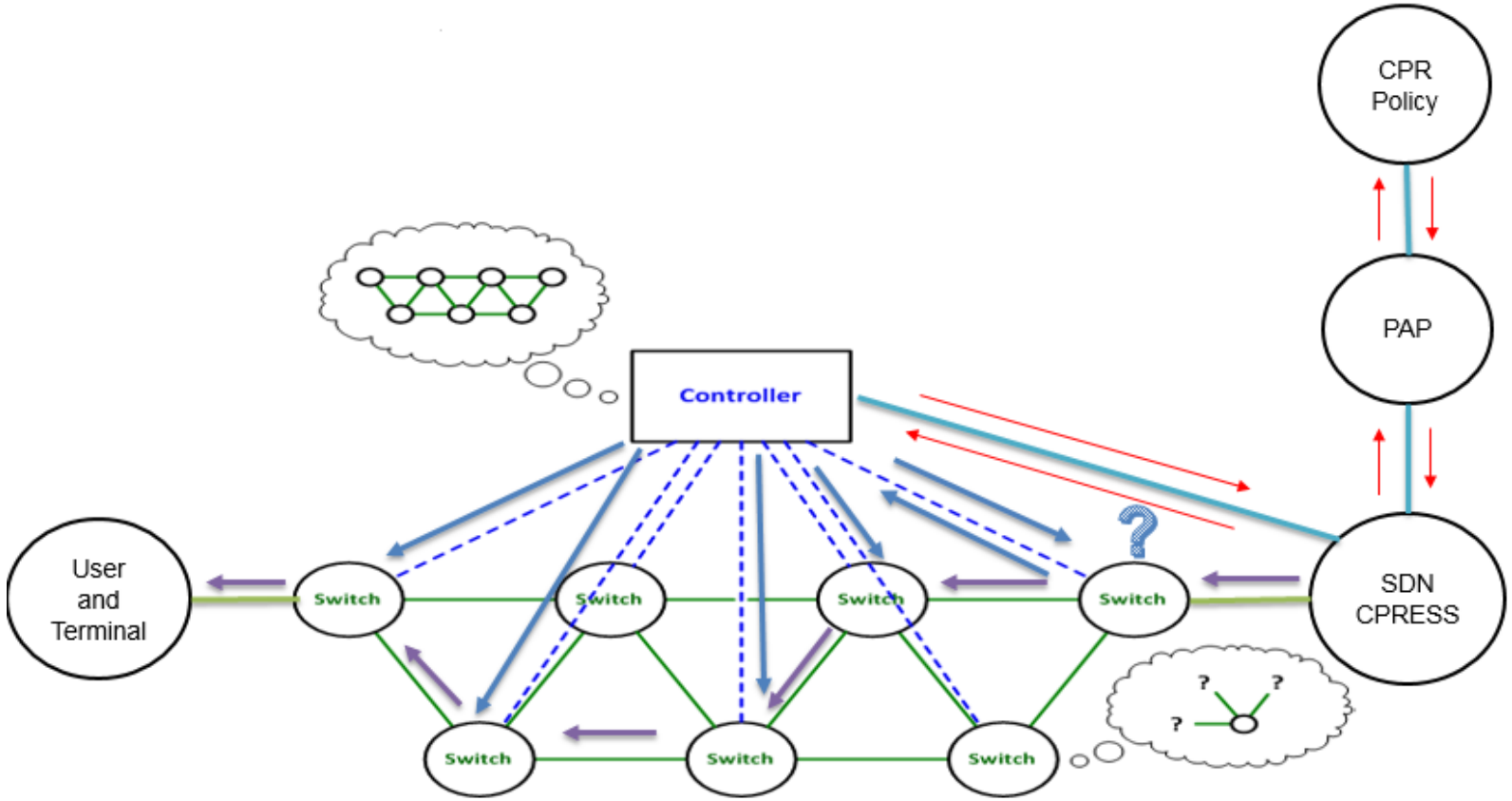
- Communication between controllers



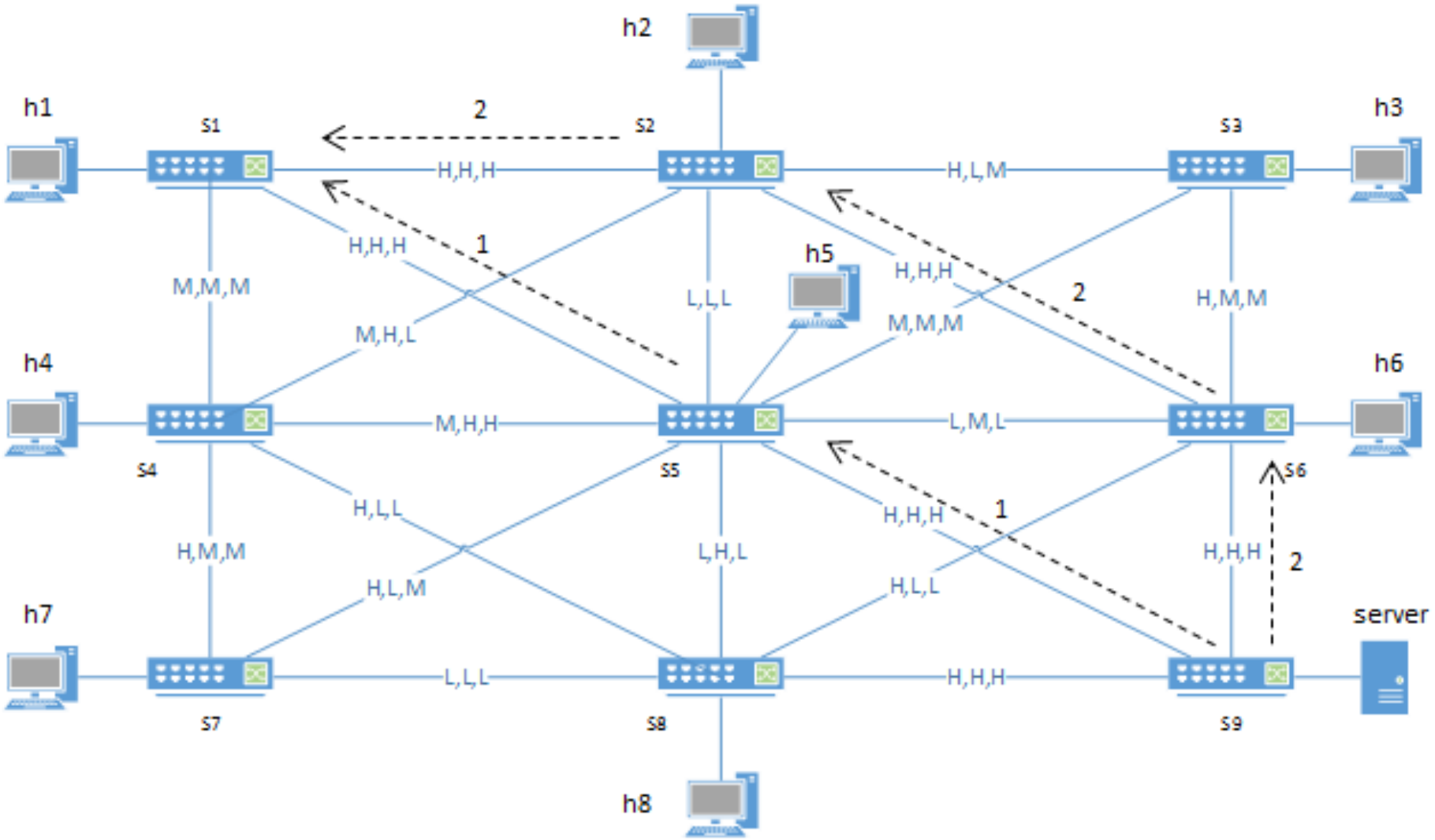
Path class approach (creating EAI)



Path Class approach (transferring data through SDN network)



Proof-of-Concept Setup

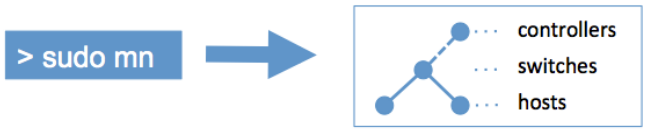


Data-centric software-defined networks

Number of paths not meeting protection requirements (shortest path algorithm)				
Network	**Confidentiality**	**Integrity**	**Availability**	**Total**
Static	9 (33%)	9 (33%)	18 (66%)	23 (85%)
Dynamic	9477 (48%)	9477 (48%)	9477 (48%)	16939 (86%)

Average path length (in number of used links)		
Network	**Shortest path**	**Path class identifier**
Static	2 (100%)	3.37 (169%)
Dynamic	2 (100%)	3.34 (167%)

SDN Proof of Concept

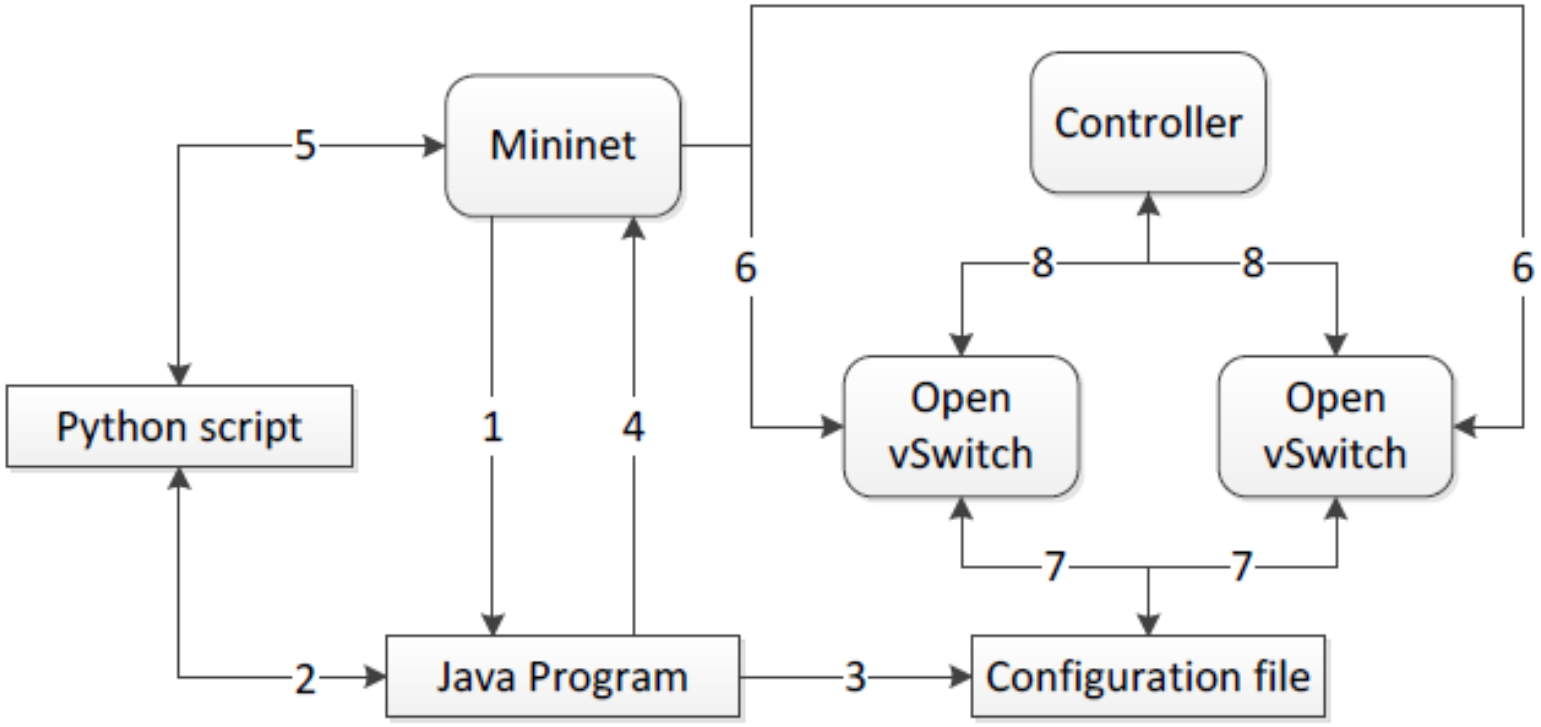


ns-3 NETWORK SIMULATOR

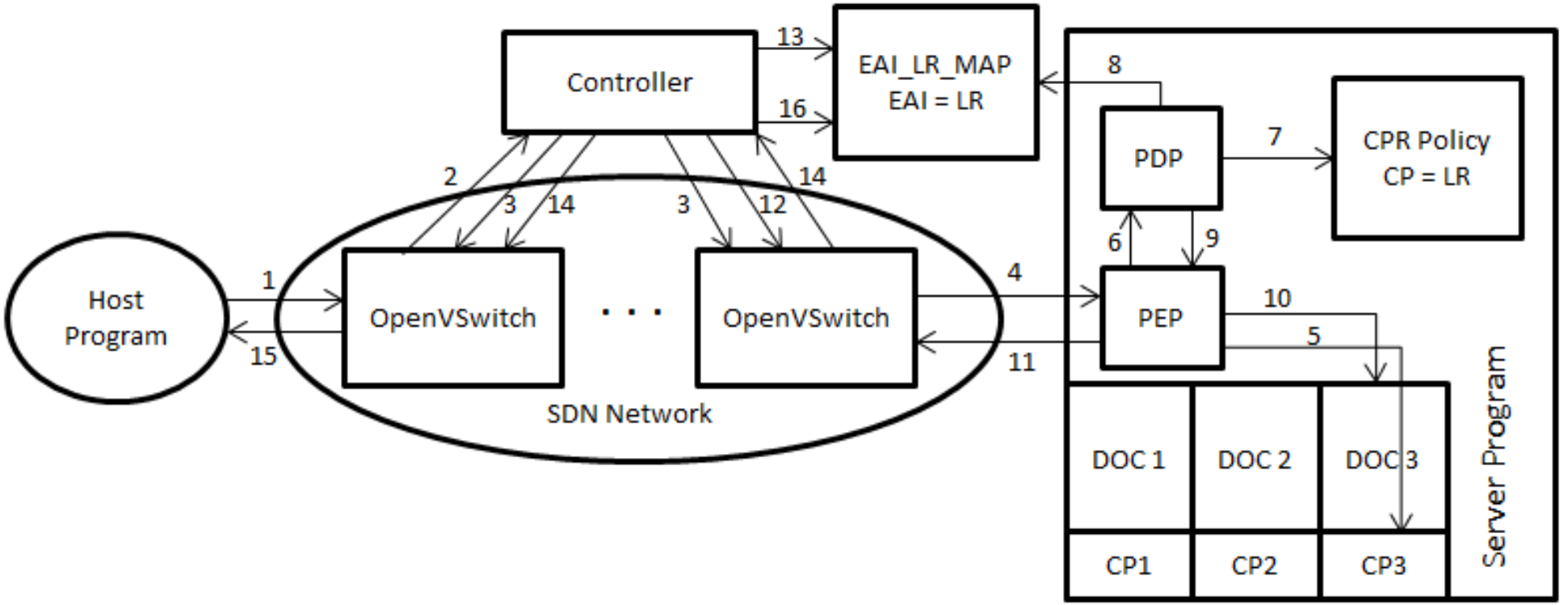
PL-LAB2020

eit Digital

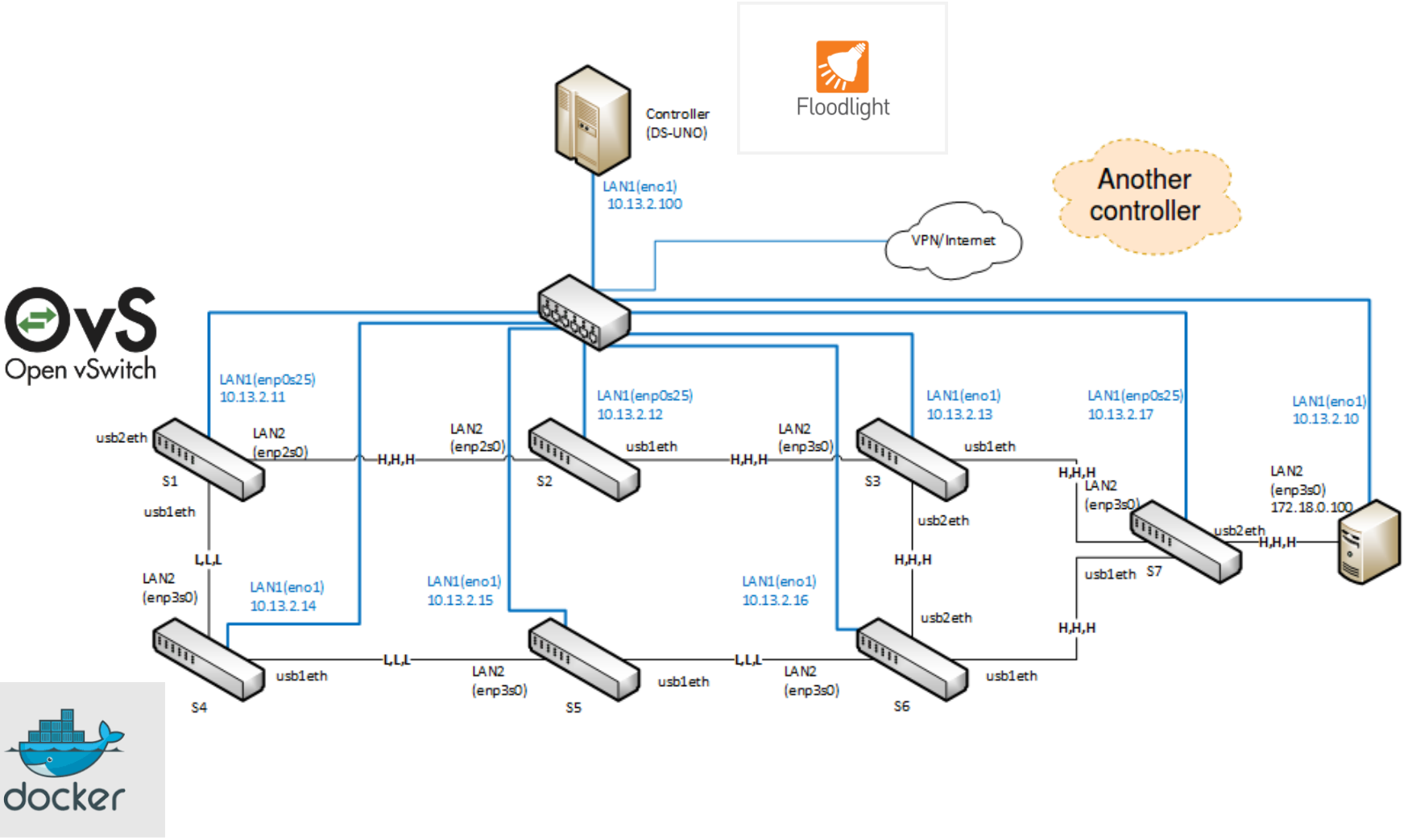
Implementation – starting and configuring switches



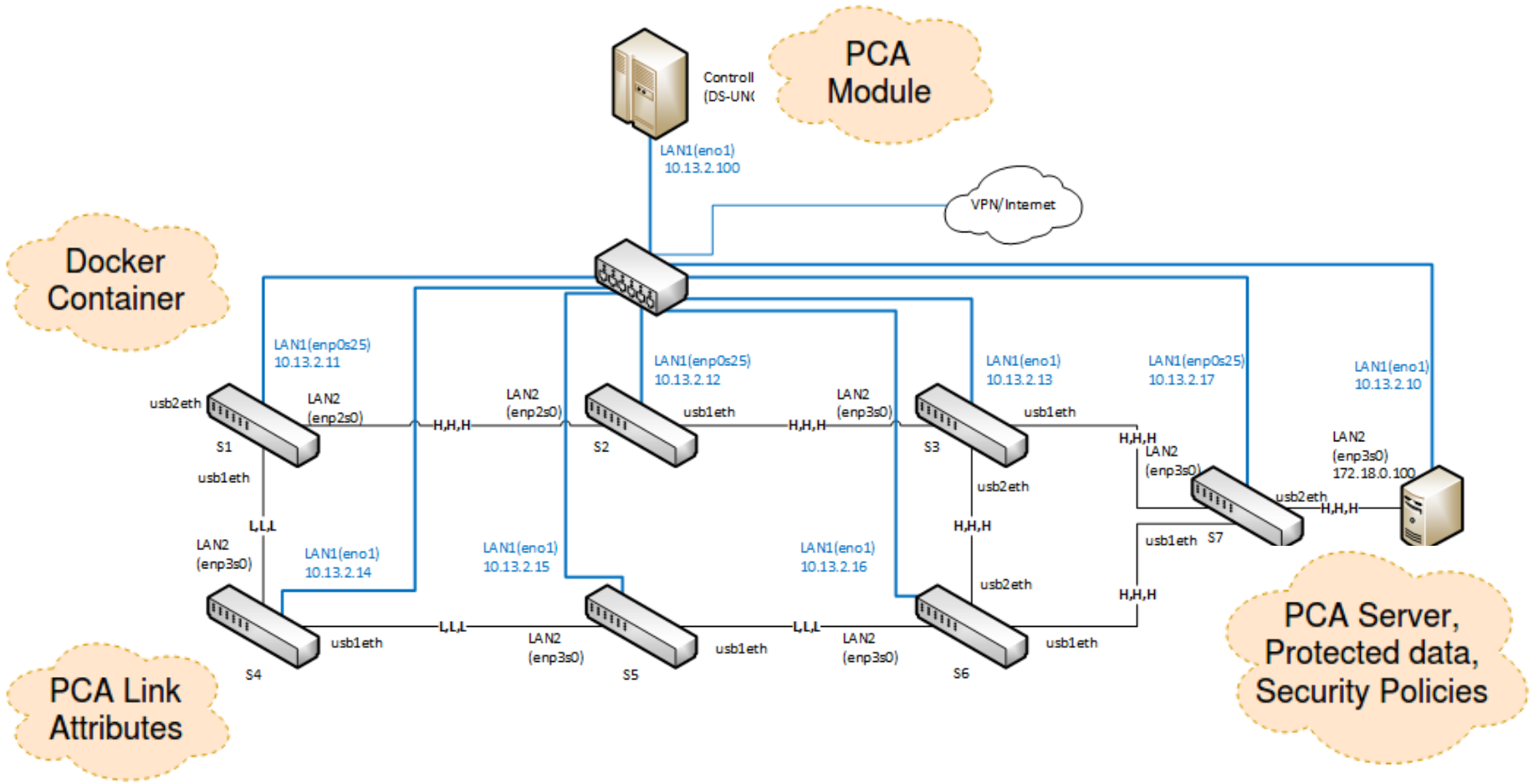
Implementation – Send Request, generate EAI, Send Response



DC/SDN Testbed



Extensions to a standard SDN environment



Experiment results: Influence of controller location

Location of the controller	Average reaction times		Time between updates
	Detect time [ms]	Remove time [ms]	
Local testbed	954	21,8	2s
Remote via VPN	1053	43,4	
Local testbed	2609	21,0	5s
Remote via VPN	2837	43,2	

Future: 5G slicing and data-centric security