

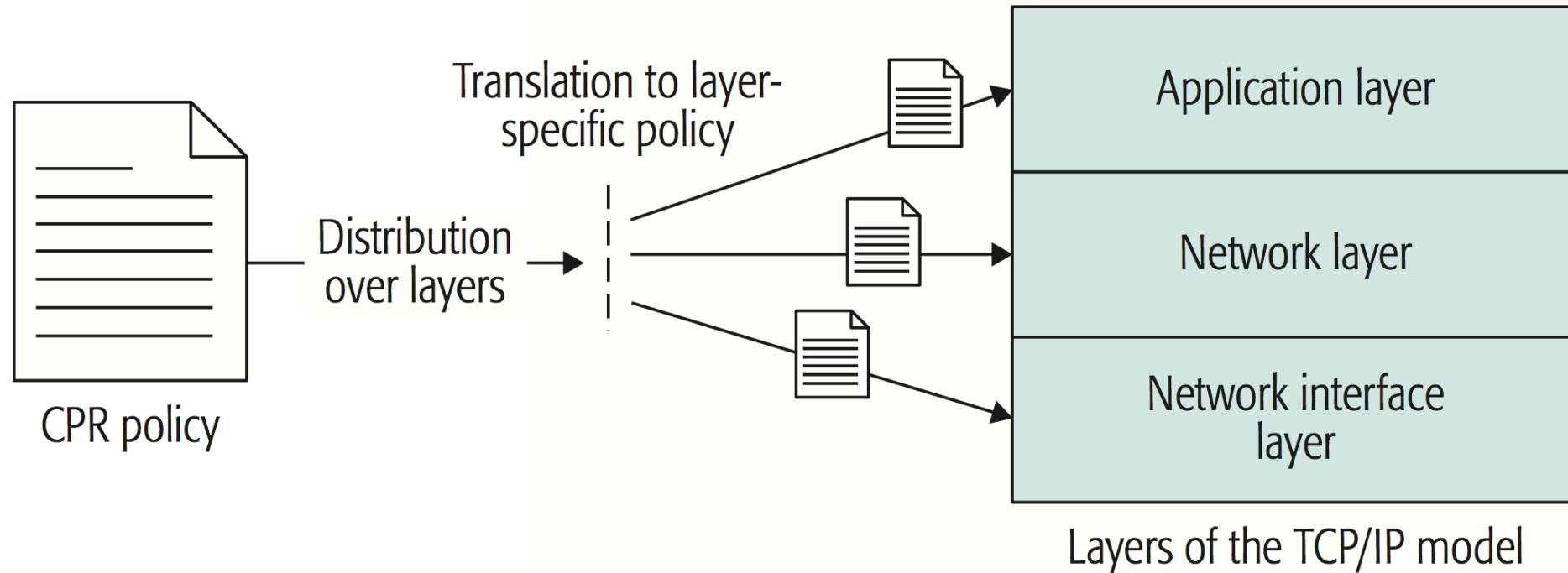
# Data-centric security in software-defined networks

Dr.-Ing. Konrad Wrona

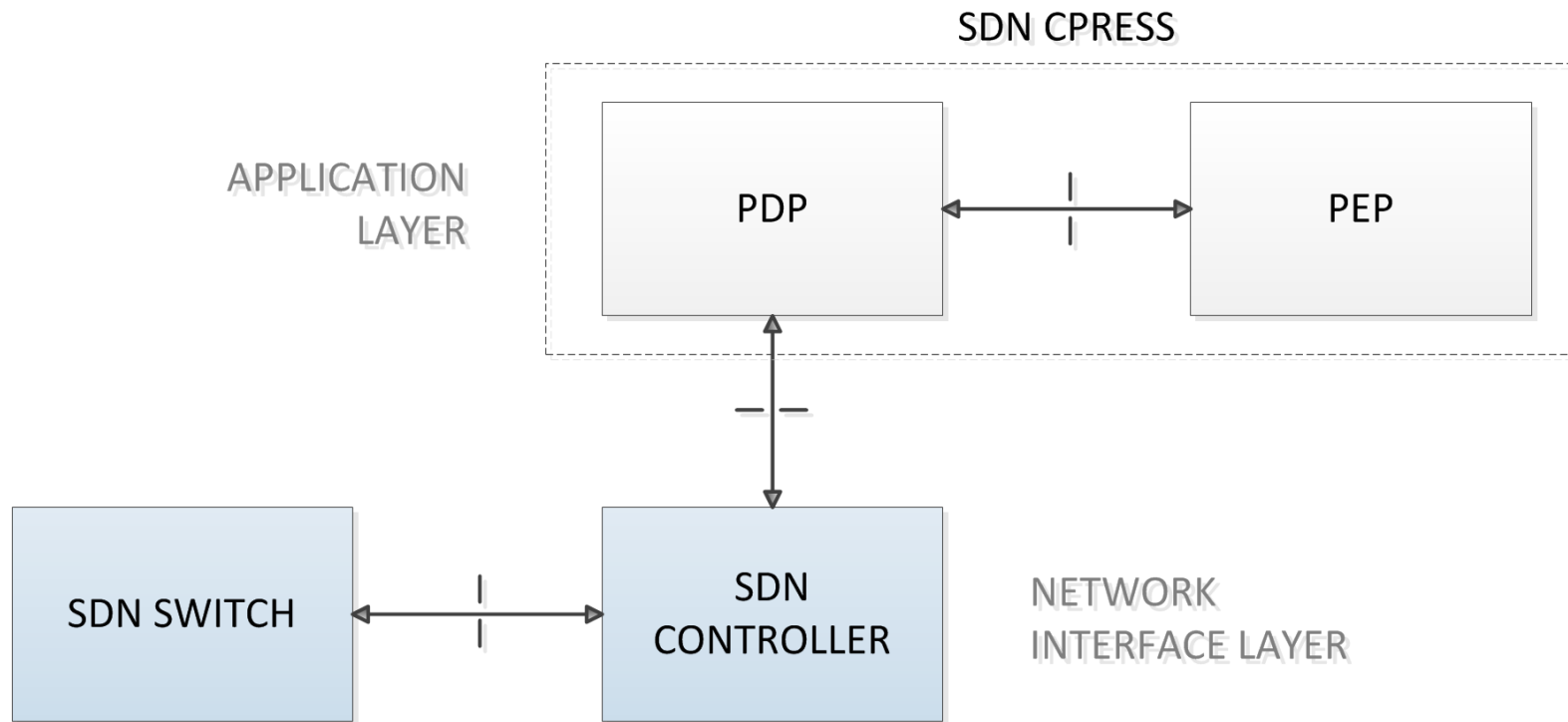
# Lecture 6:

## Data-centric security in software-defined networks

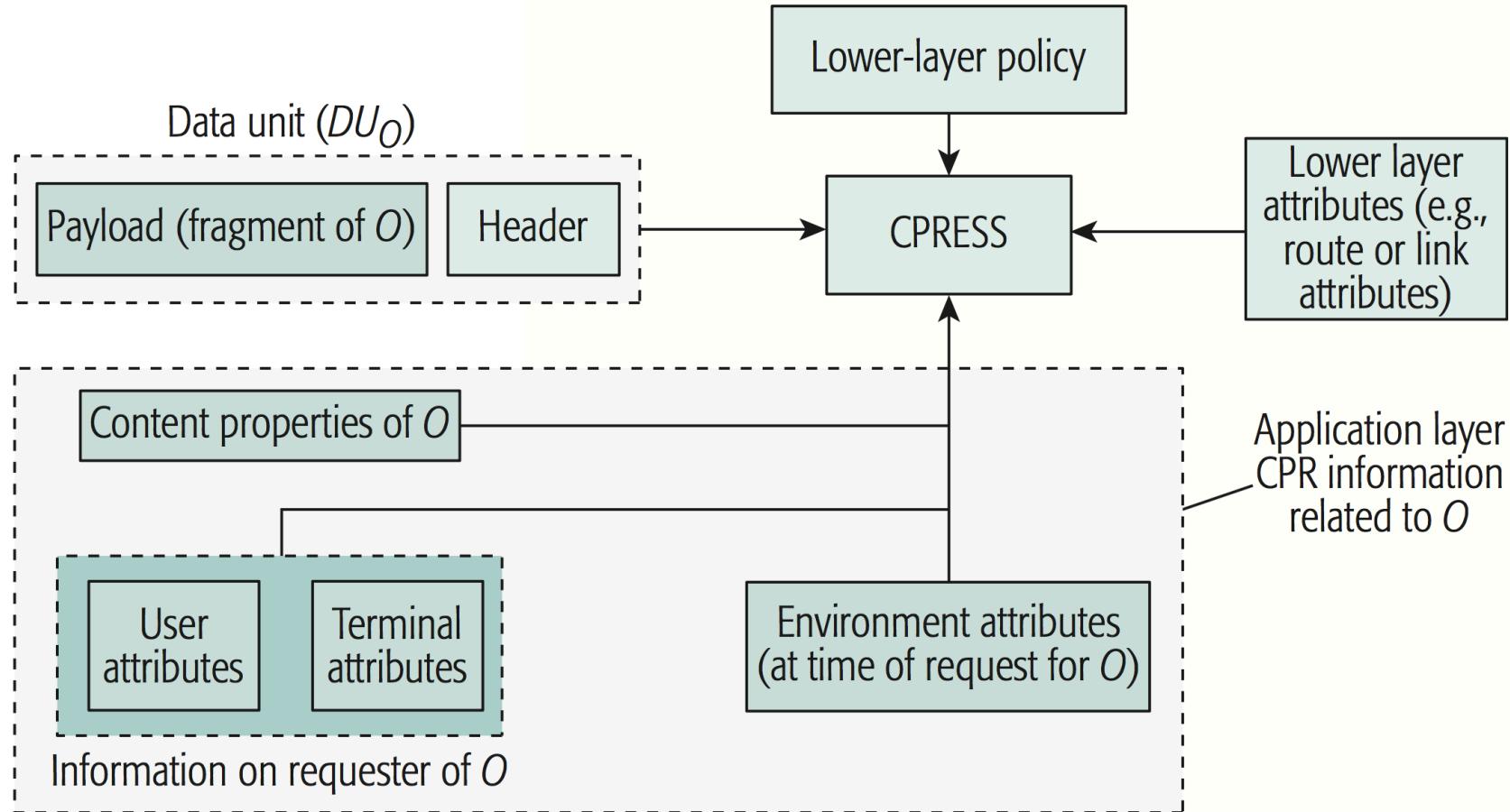
# Cross-layer enforcement of DCS policies



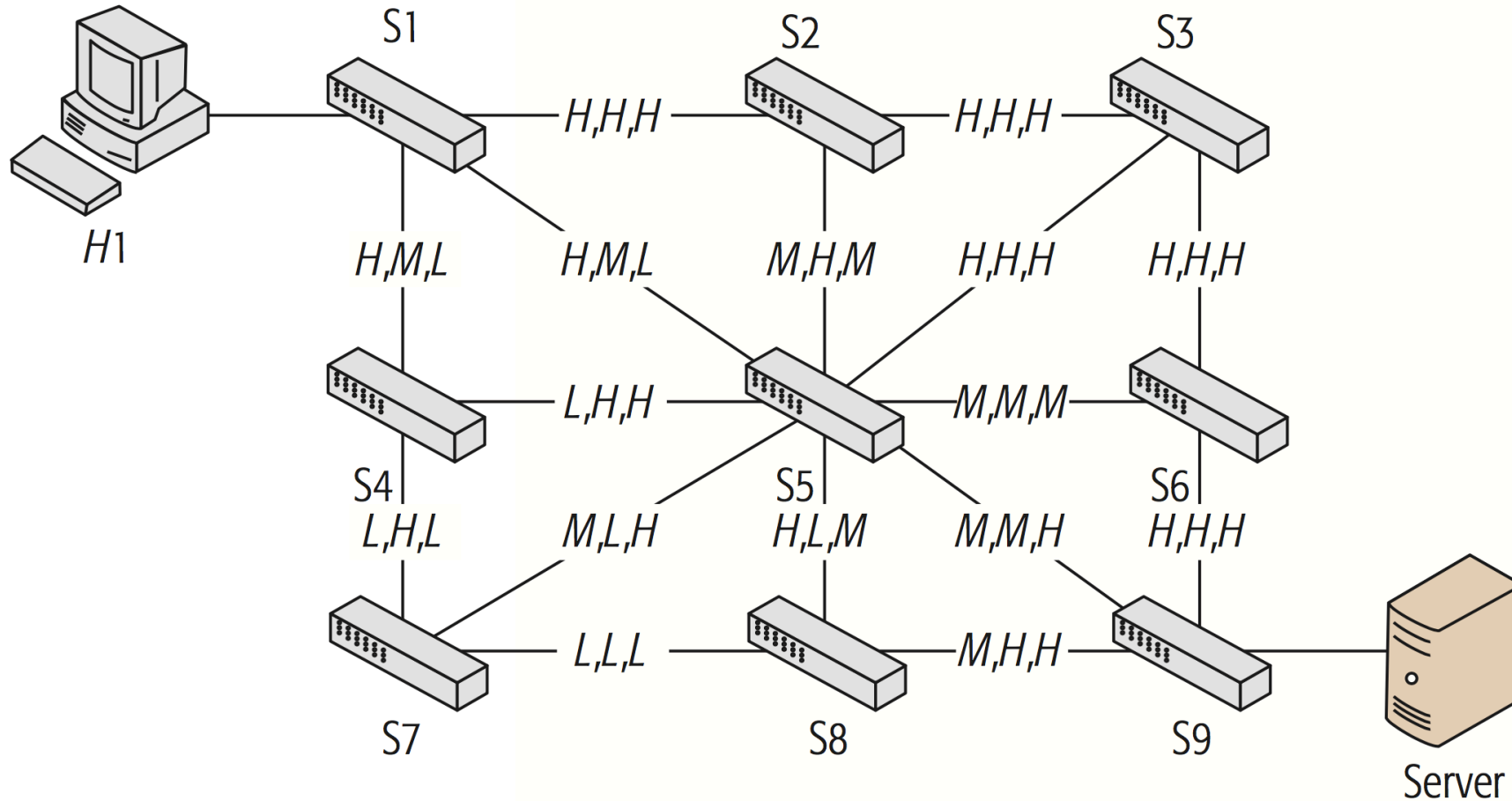
# Enforcement of application-layer security policies in the network



# Enforcement of application-layer security policies in the network

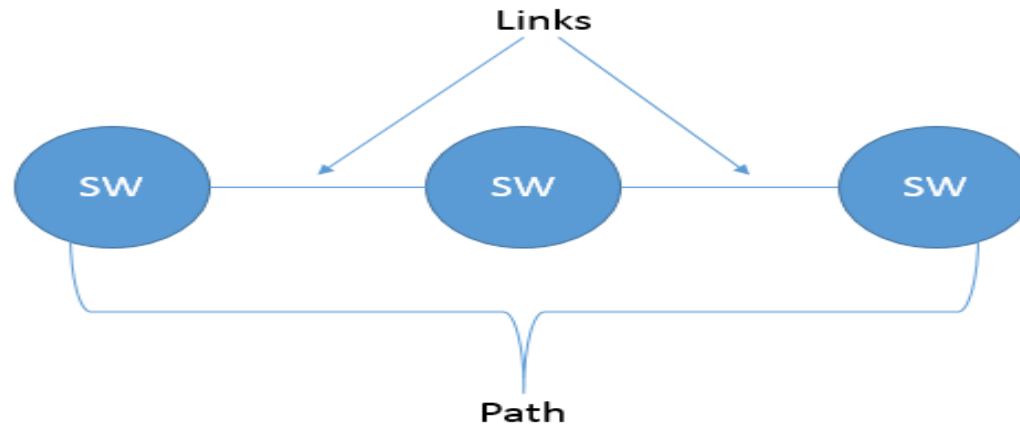


# Data-centric software-defined networks



# 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

▼ Current: 0x00000840

.....0	= OFPPF_10MB_HD: False
.....0.	= OFPPF_10MB_FD: False
.....0..	= OFPPF_100MB_HD: False
.....0...	= OFPPF_100MB_FD: False
.....0....	= OFPPF_1GB_HD: False
.....0.....	= OFPPF_1GB_FD: False
.....1..	= OFPPF_10_GB_FD: True
.....0...	= OFPPF_40GB_FD: False
.....0....	= OFPPF_100_GB_FD: False
.....0.....	= OFPPF_1TB_FD: False
.....0.....	= OFPPF_OTHER: False
.....1....	= OFPPF_COPPER: True
.....0.....	= OFPPF_FIBER: False
.....0.....	= OFPPF_AUTONEG: False
.....0.....	= OFPPF_PAUSE: False
.....0.....	= OFPPF_PAUSE_ASYM: False

Place for CPR LA



# Link Attributes in OpenFlow

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

0000 1000 0000 0001

Confidentiality Integrity Availability

Current: 0x08014880

.... 0	= OFPPF_10MB_HD: False
.... 0	= OFPPF_10MB_FD: False
.... 0	= OFPPF_100MB_HD: False
.... 0	= OFPPF_100MB_FD: False
.... 0	= OFPPF_1GB_HD: False
.... 0	= OFPPF_1GB_FD: False
.... 0	= OFPPF_10_GB_FD: False
.... 1	= OFPPF_40GB_FD: True
.... 0	= OFPPF_100_GB_FD: False
.... 0	= OFPPF_1TB_FD: False
.... 0	= OFPPF_OTHER: False
.... 1	= OFPPF_COPPER: True
.... 0	= OFPPF_FIBER: False
.... 0	= OFPPF_AUTONEG: False
.... 1	= OFPPF_PAUSE: True
.... 0	= OFPPF_PAUSE_ASYM: False

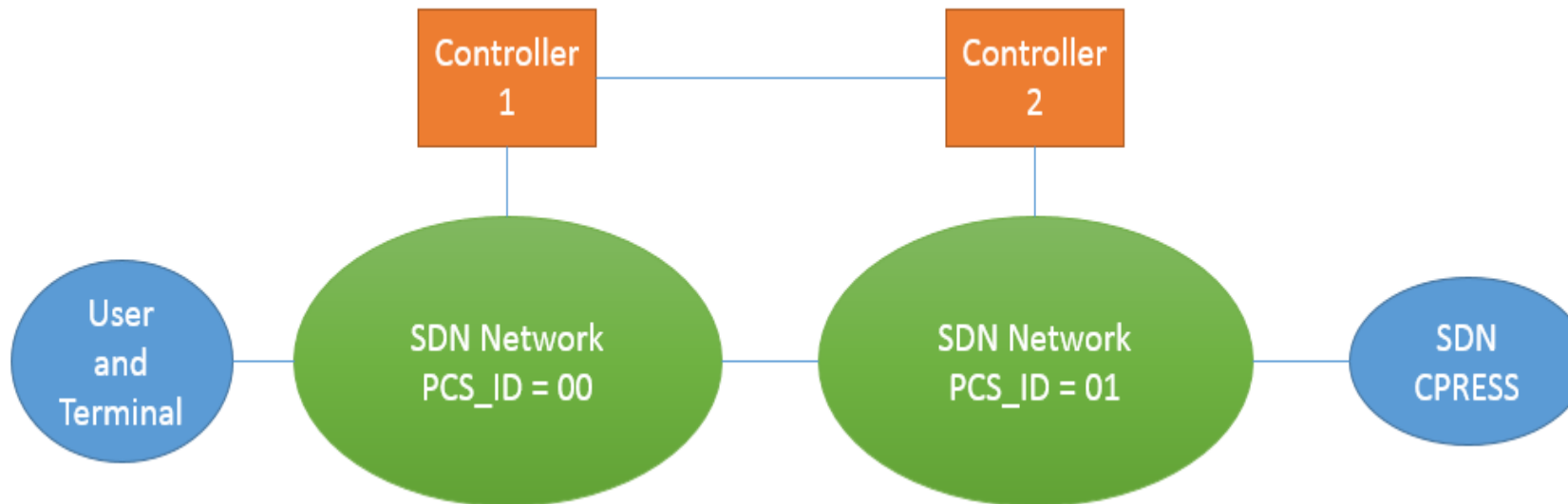
Hexadecimal notation  
(0 8 0 1)

# Sharing CPR LR between SDN networks

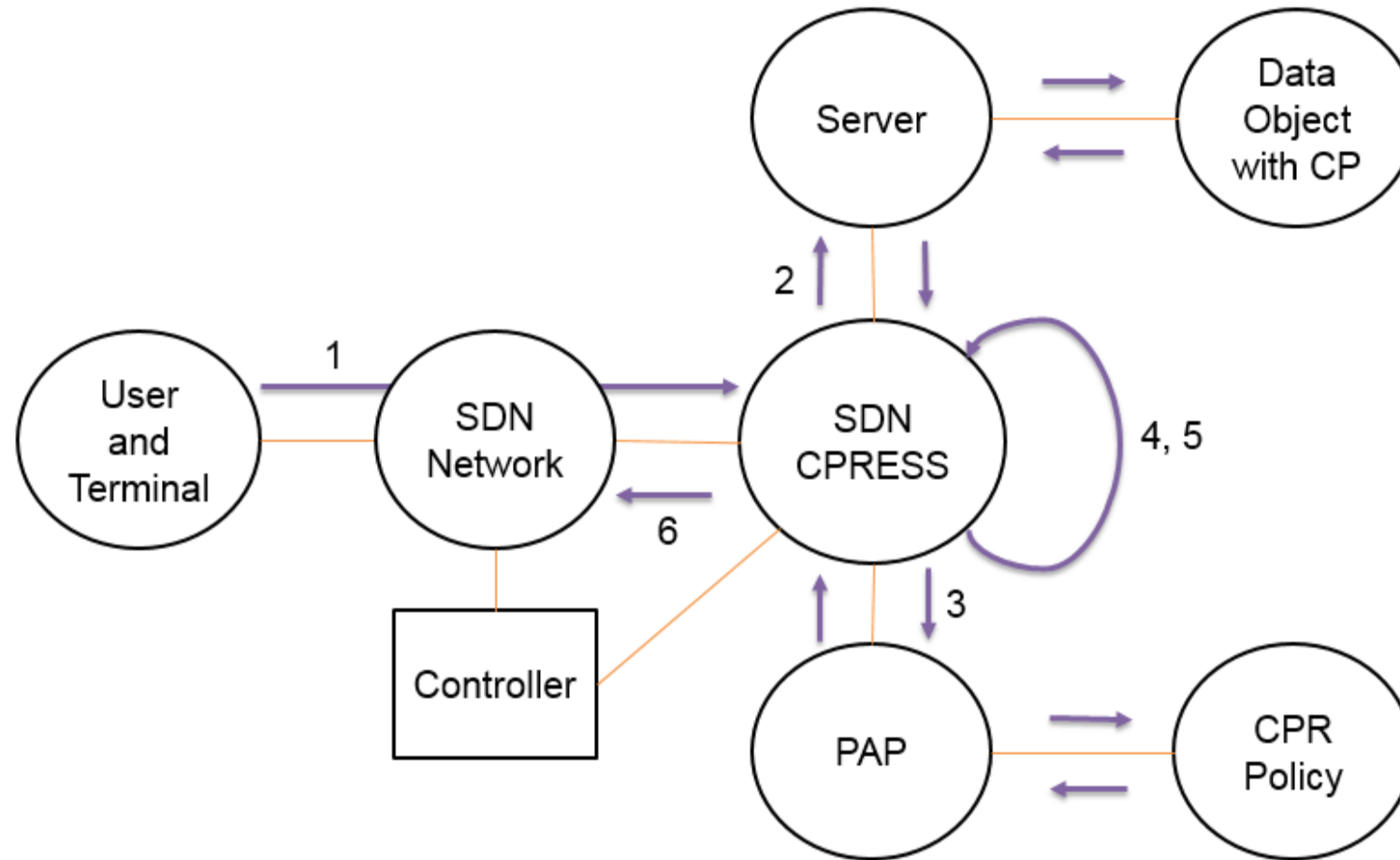
- EAI structure

01	101010
PCS_ID	VALUE

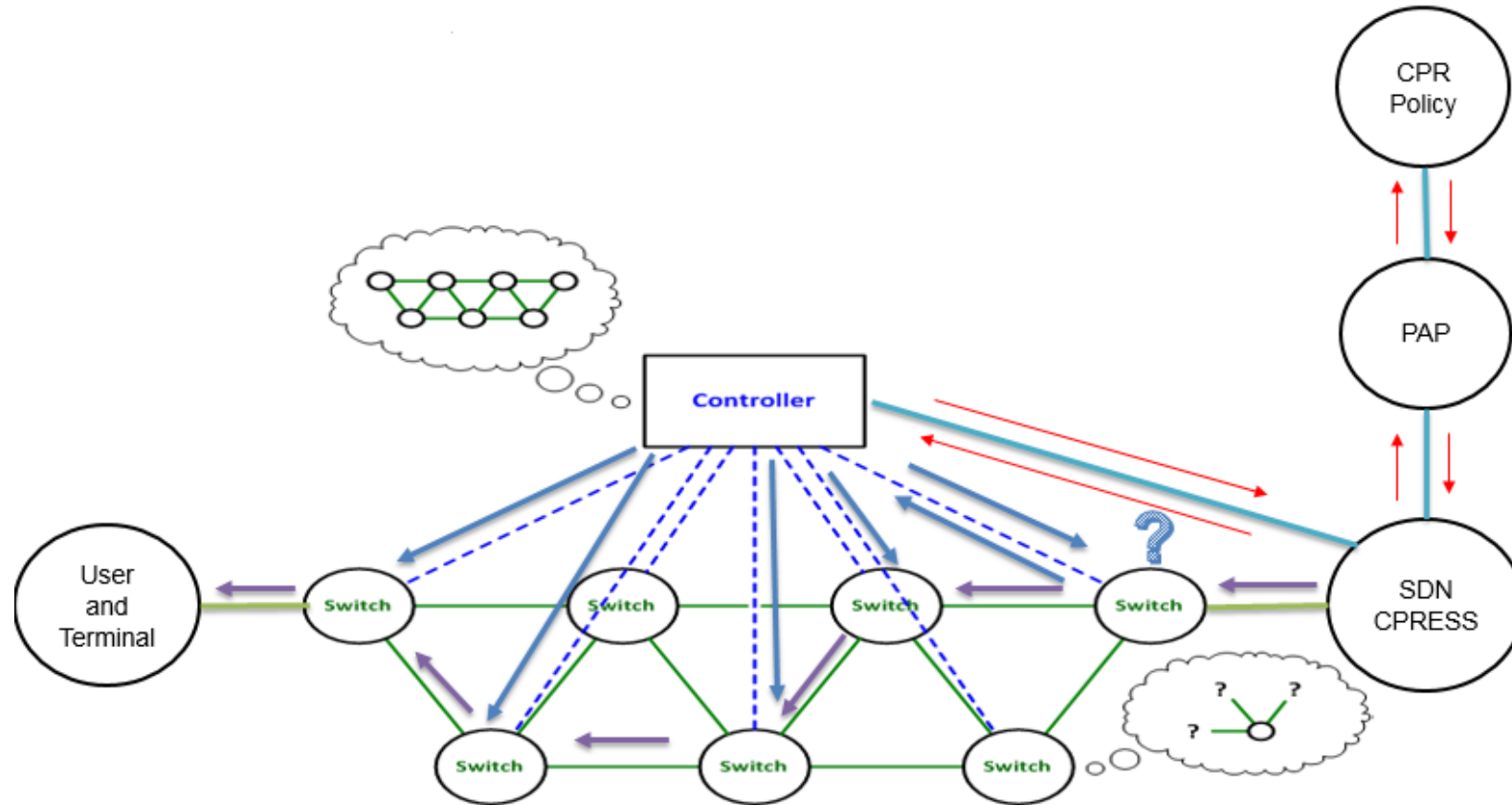
- Communication between controllers



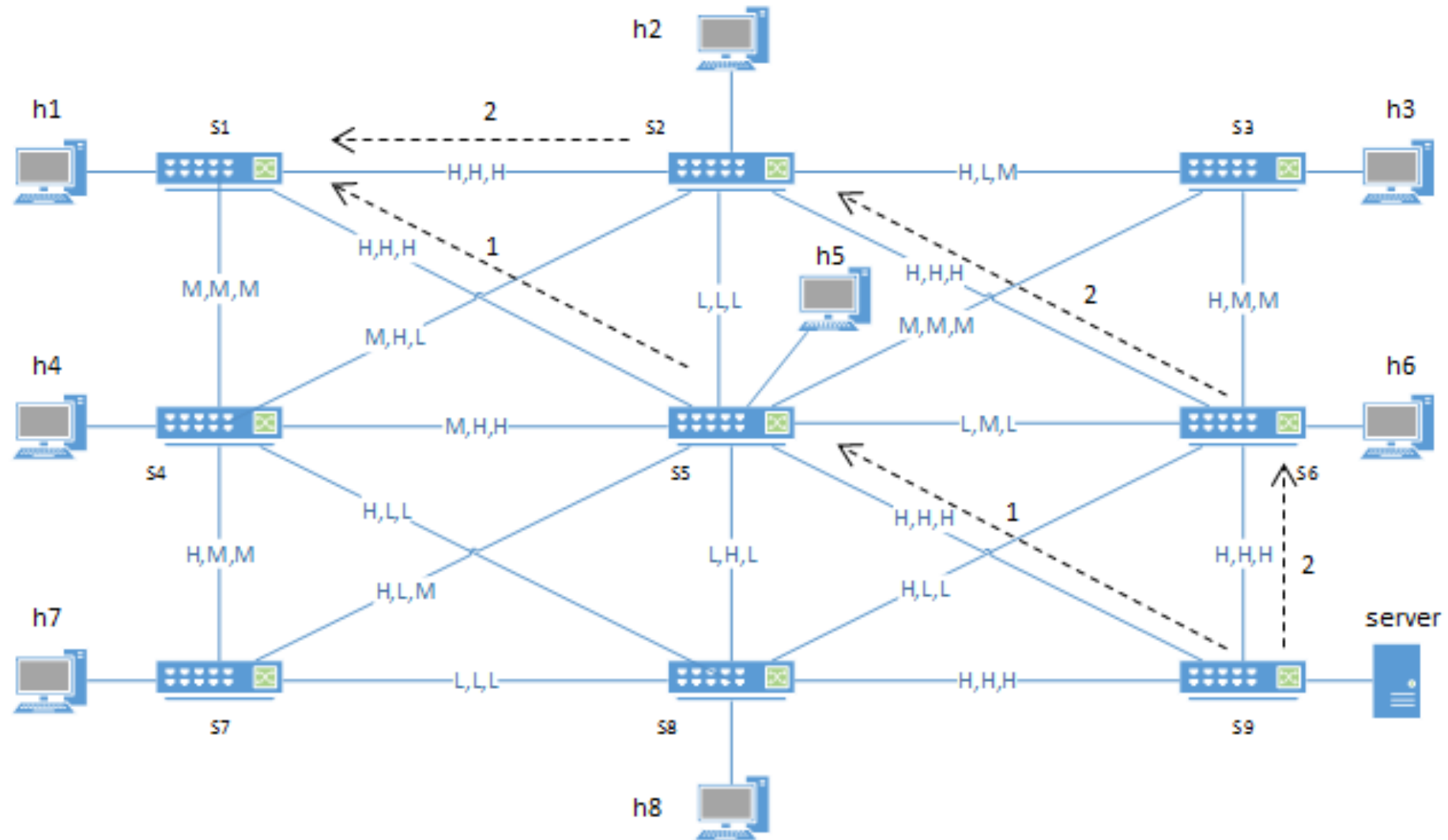
# Path class approach (creating EAI)



# Path Class approach (transferring data through SDN network)



# Proof-of-Concept Setup

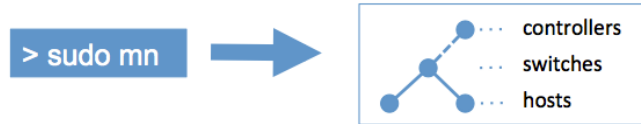


# Data-centric software-defined networks

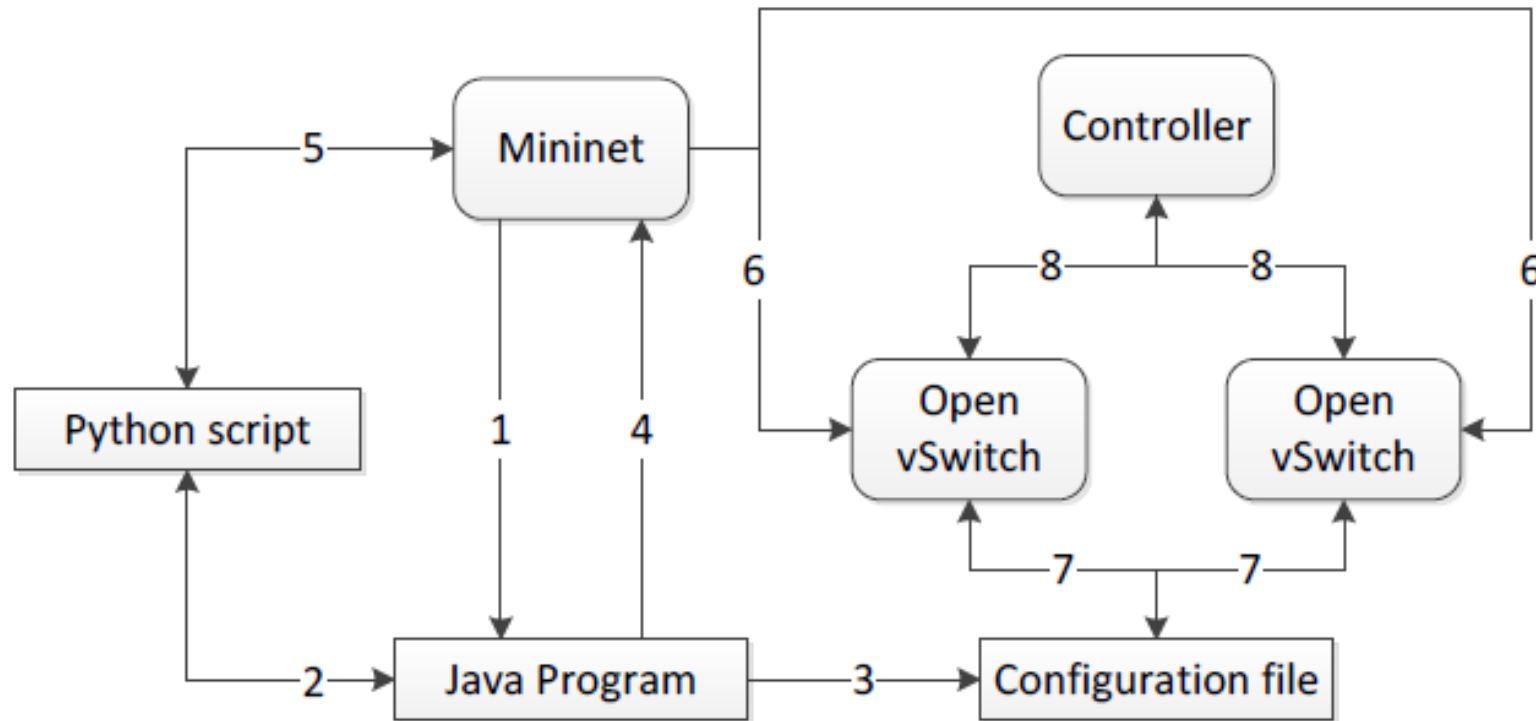
Number of paths not meeting protection requirements (shortest path algorithm)				
Network	Confidentiality	Integrity	Availability	Total
Static	9 (33%)	9 (33%)	18 (66%)	23 (85%)
Dynamic	9477 (48%)	9477 (48%)	9477 (48%)	16939 (86%)
Average path length (in number of used links)				
Network	Shortest path		Path class identifier	
Static	2 (100%)		3.37 (169%)	
Dynamic	2 (100%)		3.34 (167%)	



# SDN Proof of Concept

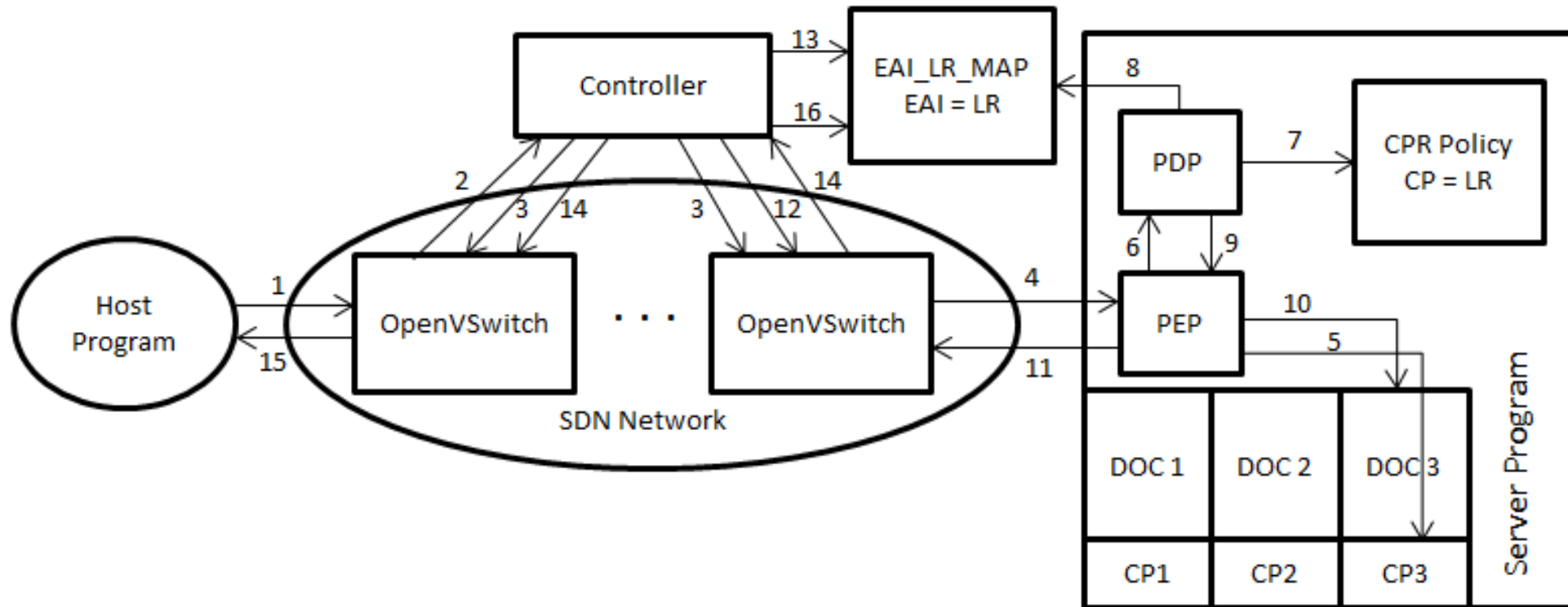


# Implementation – starting and configuring switches

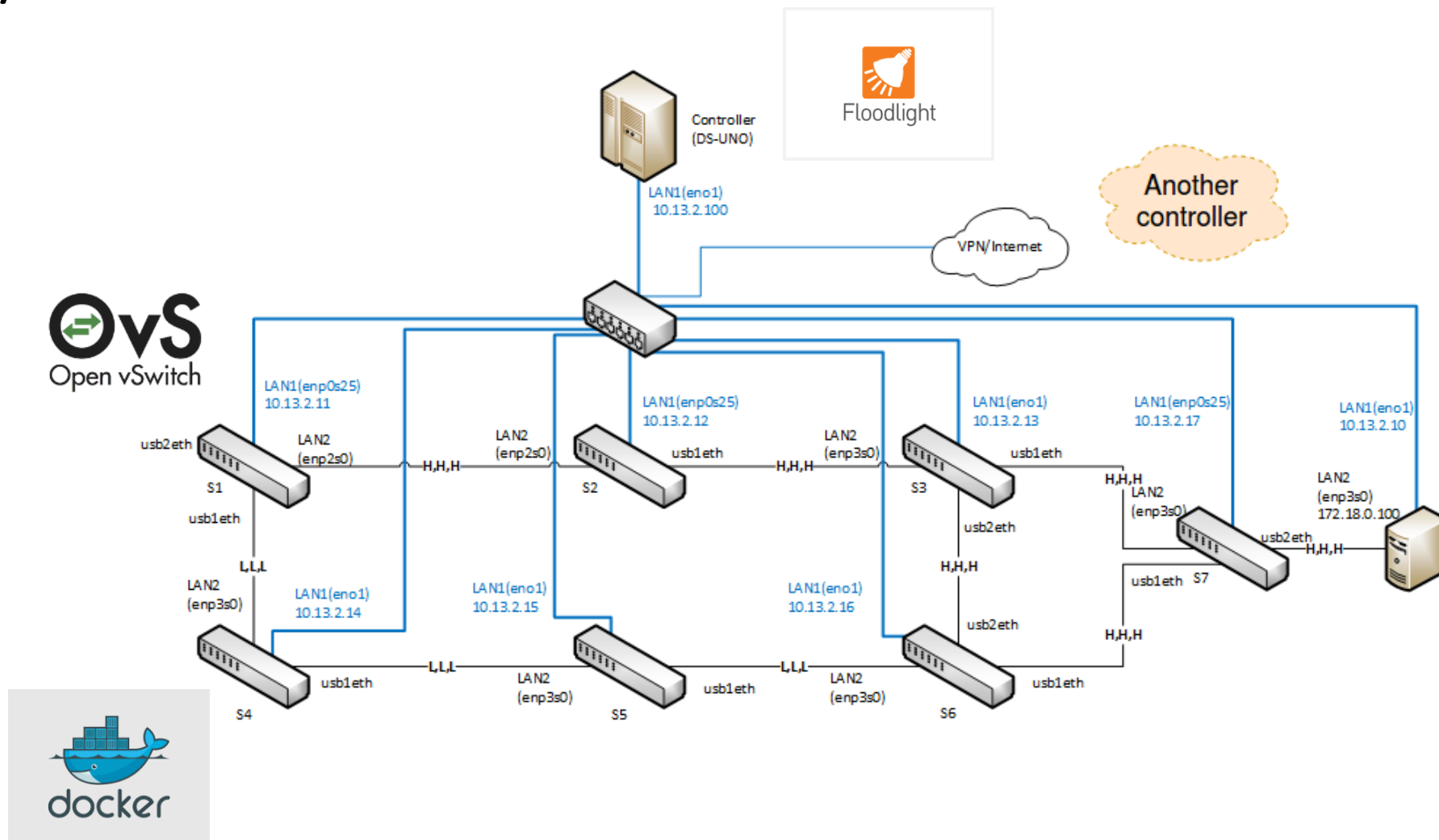




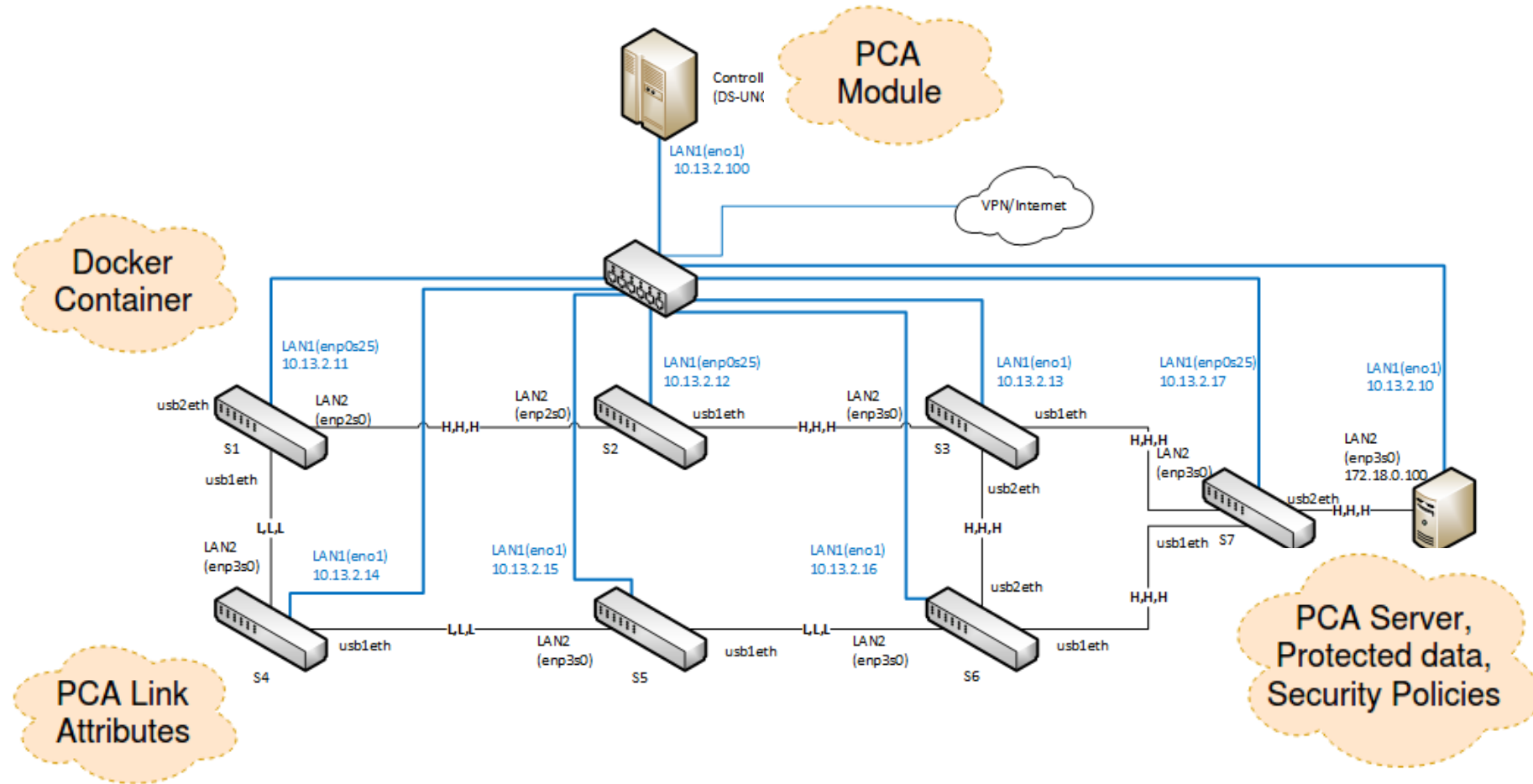
# Implementation – Send Request, generate EAI, Send Response



# 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

Content  
properties



Data-centric security slices



SDR



SDN



SDS, Containers

