Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 01: Fundamentals
Module 02: Networking 101

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

CASED

SECURE MOBILE NETWORKING

Networking 101

Learning Objectives

Obtain a common understanding of communication networks

- Identify the most important basic concepts of communication networking
- Understand layering, services, protocols, etc.
- Have some idea of the philosophy behind the Internet and understand its fundamental design principles
- Identify networking aspects that might be directly security related

"The shortest distance between two points is usually under repair."
—Anonymous

Overview of this Module

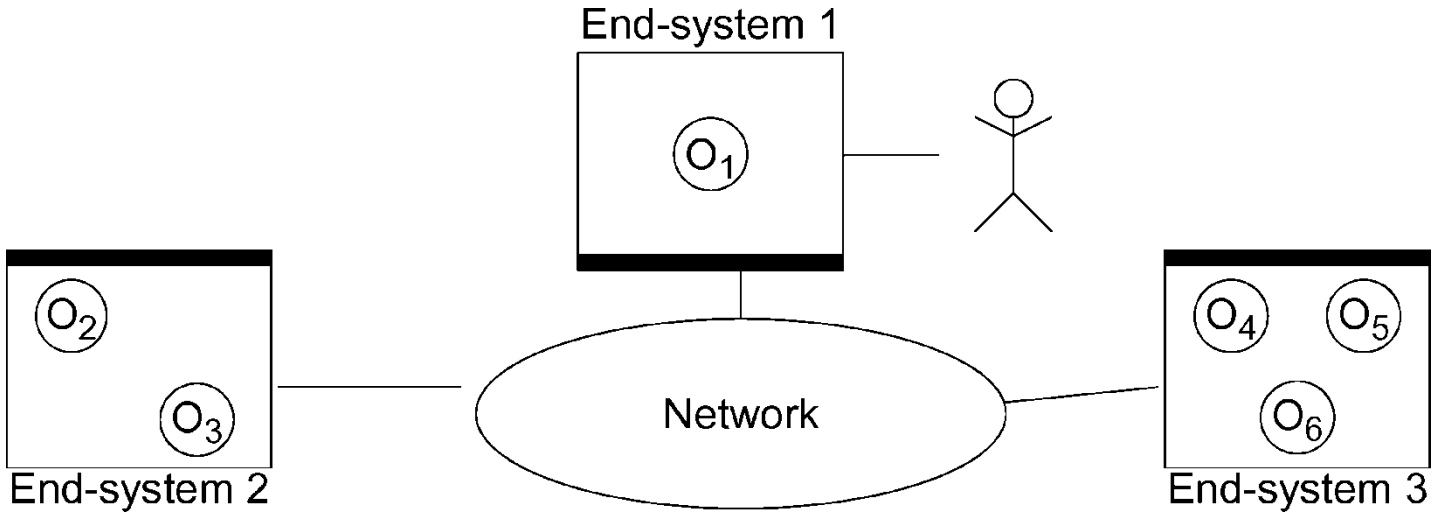
(1) What we consider to be a network throughout the lecture
(2) Layered architectures (including the Internet architecture)
(3) Basic network primitives and interaction with security
(4) Recommended readings

Chapter 01, Module 02

Computer and Communication Networks

Computer and communication networks

- Several autonomous computers/end-systems/processors interconnected with the aim to exchange information
- Here “interconnected" means: data can be exchanged, resources can be shared



Scope of Networks

Distance between Processors	CPUs jointly located on/in..	Example
<= 0,1 m	Boards	usually tightly coupled multi-processor system
1 m	Systems	e.g. body area network e.g. sensor area network e.g. storage area network
10 m	Rooms	LAN
100 m	Buildings	
1 km	Campuses	
10 km	Cities	MAN
100 km	Countries (national)	WAN
1.000 km	Continents (intern.)	
>= 10.000 km	Planets	

- Structure: point-to-point vs. point-to-multipoint
- Media: wireline vs. wireless

Motivating Layers

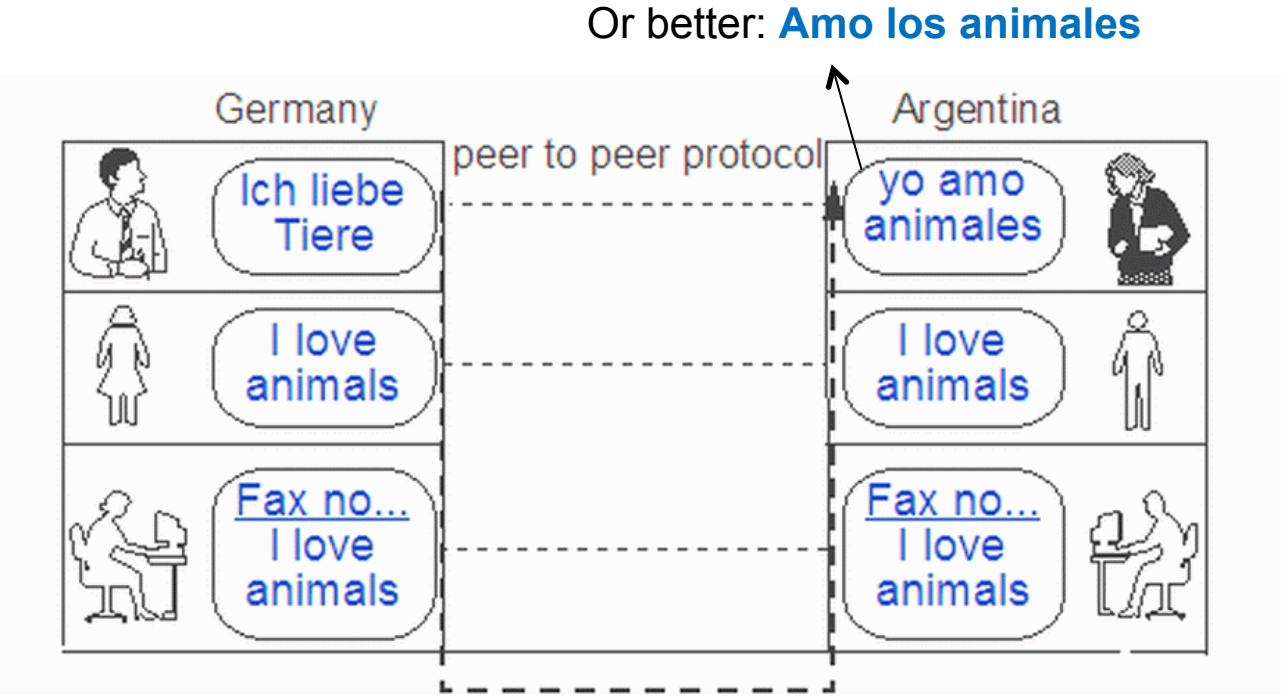
Problem: communication engineering means

- Multitude of partially very complex tasks
- Interaction of differing systems and components

Simplification:

- To introduce abstraction levels of varying functionalities
- General module, preferable: layer, level

See example



Layers

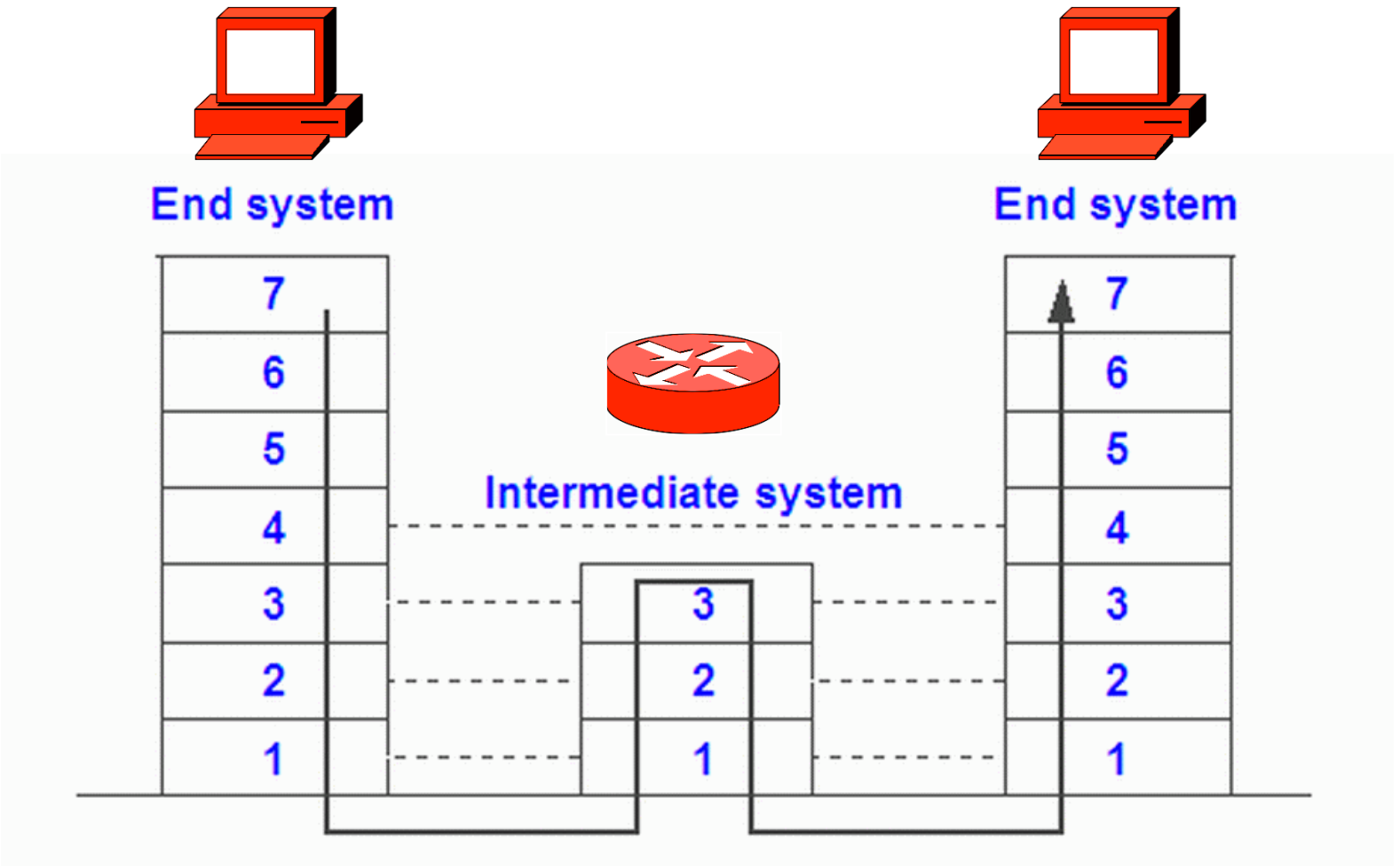
ISO-OSI (Open Systems Interconnection) Reference Model

- Model for layered communication systems
- Defines fundamental concepts and terminology
- Defines 7 layers and their functionalities (see textbook for details)

ISO-OSI Reference Model

- Layer 1: physical (PHY)
- Layer 2: data link (MAC)
  - Has neighbor-neighbor revelance
- Layer 3: network (NET)
  - Has relevance on entire path between systems
- Layer 4: transport (TRANS)
  - Has end-to-end revelance
- Layer 5-7: application, presentation, session (APP)

Data Flow


End system
End system
7
6
5
4
3
2
1
Intermediate system
3
2
1
7
6
5
4
3
2
1

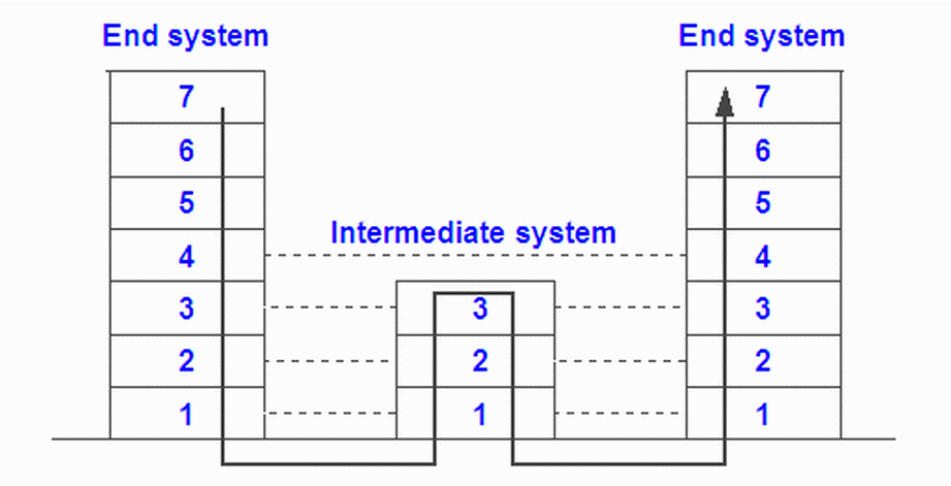
Protocols, Services

Protocol:

- Communication between same-layer entities

Service:

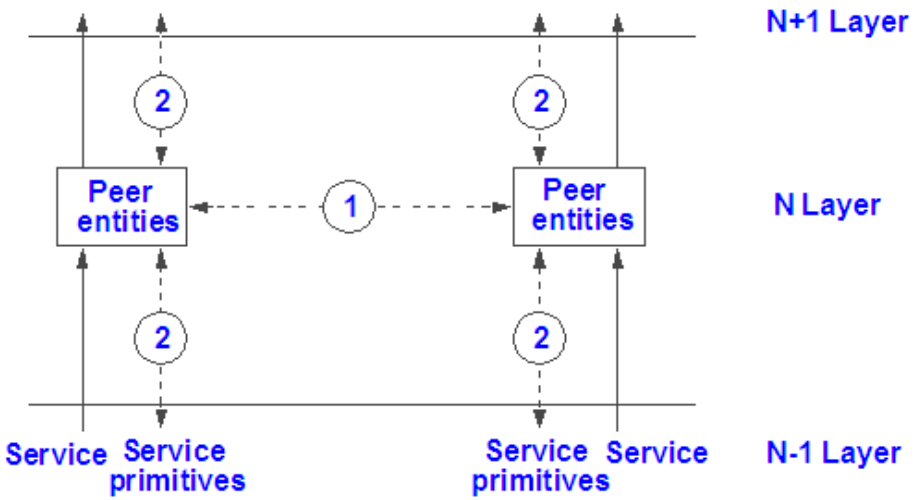
- Communication between adjacent Layers



Implementation: each layer provides some API (or SAP – Service Access Point) to that above it; the provided service can be

- Reliable: bit stream or packets, arrive in same order at other end
- Datagram: send chunk of data, maybe it gets there, possibly lost, duplicated, out-of-order; usually detects nonmalicious errors

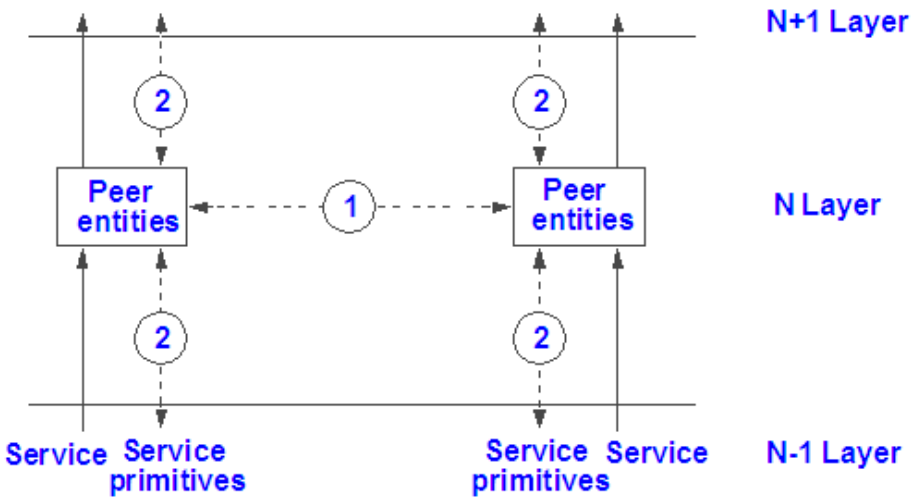
Protocol
Communication between same-layer Entities



Protocol

- rules for syntax (format) and semantics (contents)
  - of the data transfer (frames, packet, message) occurring between the respective, active peer entities
- analogy: programming, protocol corresponds to
  - realization of the data type (procedures, etc.)
  - the "interior" of the object

Service
Communication between adjacent Layers



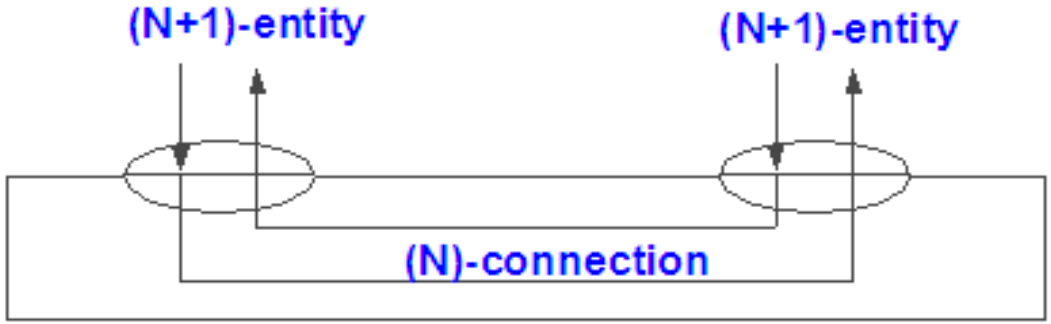
Service

- multiple of primitives/operations/functions
  - which one layer offers to the upper next layer
- characterized by the "interface"
- does not reveal anything about the implementation
- analogy: programming, service corresponds to
  - abstract data type, object

Connection-oriented vs. Connectionless Service

Connection-oriented:

- 3 phases:
  - 1. to connect
  - 2. to transfer data
  - 3. to disconnect
- Analogy: telephony
- Applications such as:
  - Regularly recurring data units, longer duration
  - Quality of service guarantees (time, bandwidth)



Connectionless (Datagram Service)

- Transfer of isolated data units
- Analogy: letter delivery
- Applications such as one-time data transfer, short duration

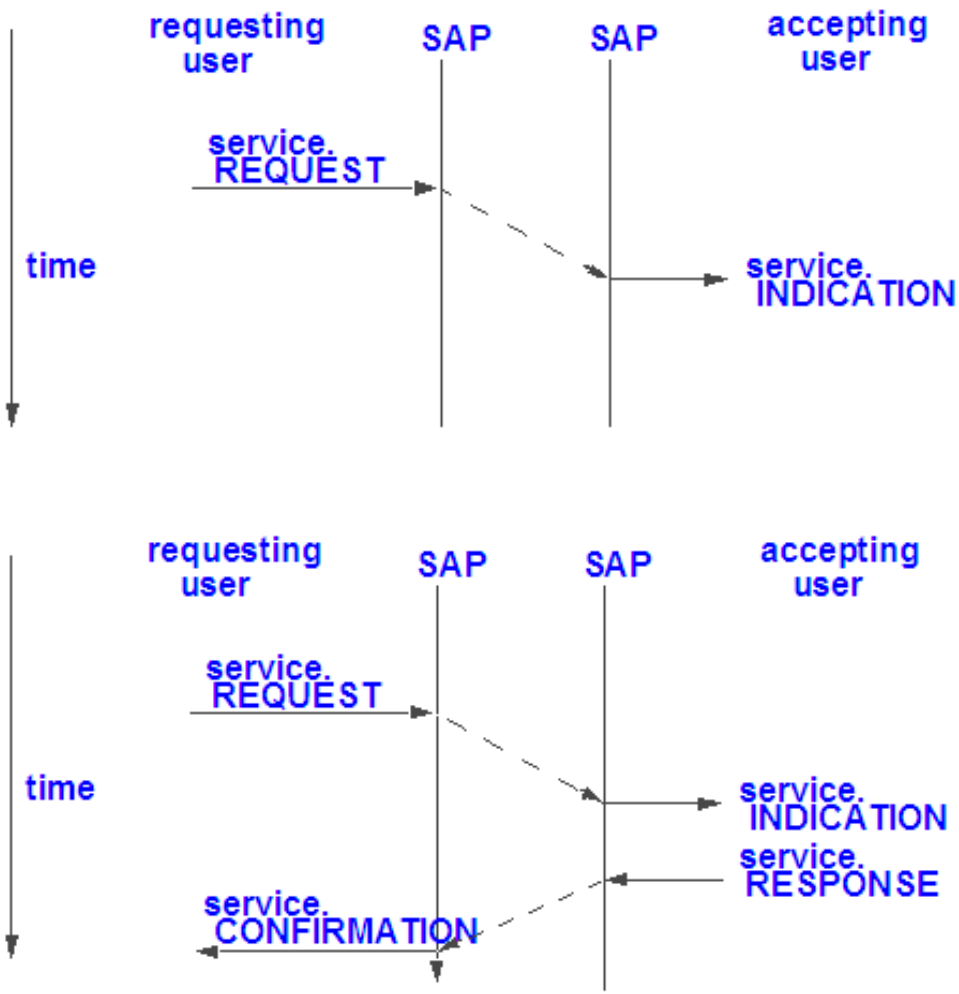
Confirmed and Unconfirmed Service

Service primitives

- Define a service in an abstract manner
- Are usually parameterized

Types:

- service.REQUEST
- Service.INDICATION
- service.RESPONSE
- service.CONFIRMATION



SECURE MOBILE NETWORKING

Reliability
(a cousin to Security)

Integrity Checks

Nonmalicious integrity checks

- Send it multiple times
- VRC (vertical redundancy check) parity within byte
- LRC (parity over a bit of all the bytes in a block)
- LRC+VRC catches what bit errors?

	Data							Parity
Row 1	1	1	0	1	0	1	1	1
Row 2	1	1	1	1	1	1	1	1
Row 3	0	1	0	1	0	1	0	1
Row 4	0	0	1	1	0	0	1	1
Parity Row	0	1	0	0	1	1	1	0

- CRC (make message + checksum divisible by the "CRC polynomial")
- Cryptographic integrity check

Intuition behind CRC

CRC (make message + checksum divisible by the "CRC polynomial")

CRC Example

- Pretend message is long number
- Suppose "CRC polynomial" is some number, say 17
- Suppose message is 5283
- Multiply it by 100=528300
- 528300 is 8 mod 17
- Subtract 8 from 528300=528292. Send that
- Rcvr checks divisibility by 17. If not, error. If so, round to nearest 100, then truncate to get message

(Two-way Reliable) Protocols

Those of you who attended KN or TK or NCS: which protocols do you know to be reliable/unreliable?

Two-way reliable protocols

- Used sometimes in layer 2, sometimes in layer 4 (e.g., TCP, but not UDP)
- Was more popular in layer 2 when lossy links
- Basic idea the same, sequence number on data, sequence number on ack, pipelining
- If n sequence numbers (and wrap around), how many can you send?

Where to put reliability: L2? L4?

Summary

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Radia Perlman
- Andrew Tanenbaum
- Lars Wolf, Ralf Steinmetz and the KN-team at KOM

Recommended reading

- Networking textbook, including the one by Kurose et al., the one by Tanenbaum, etc.
- [KuRo2010] James F. Kurose, Keith W. Ross: Computer Networking: A Top-Down Approach, 5th Edition, Addison Wesley, 2010, ISBN: 9780136079675

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de