Prof. Dr. Nils Gruschka

Network Systems and Security (MI102)

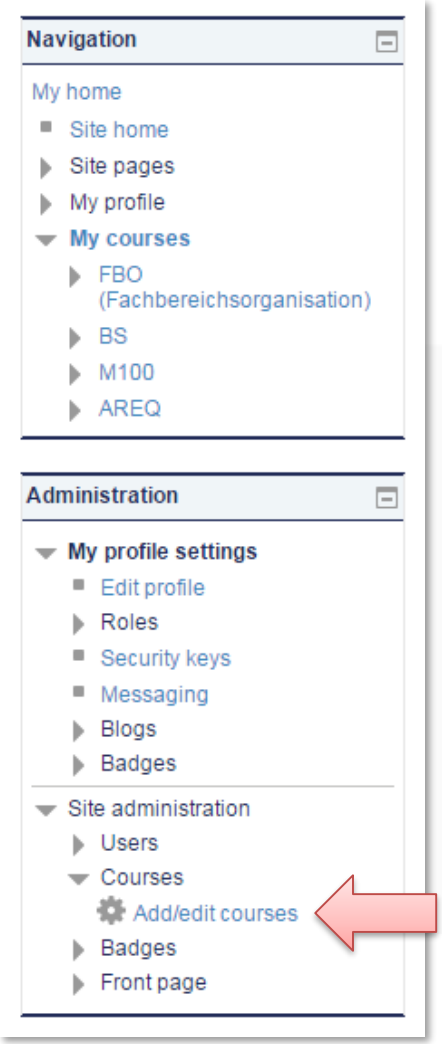
Introduction

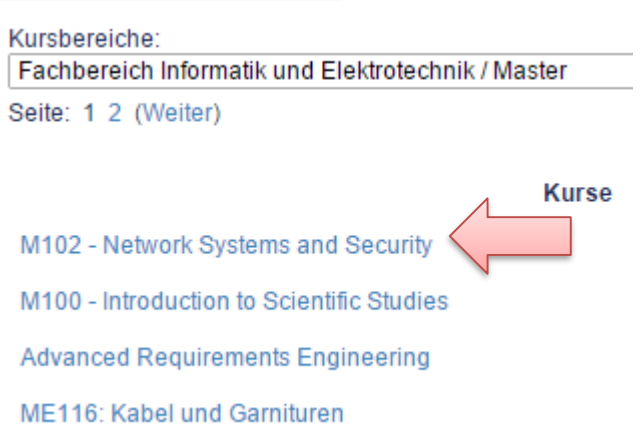
Introducing … myself

- Nils Gruschka
  - University Kiel (Diploma in Computer Science)
  - T-Systems, Hamburg
  - University Kiel (Dr. rer. nat.)
  - NEC Laboratories Europe, Heidelberg
  - FH Kiel (Networking, Security)
- Contact:
  - Nils.Gruschka@fh-kiel.de

Organisation

- Slides, submissions, other information: http://lms.fh-kiel.de/





Organisation

- LMS (Moodle):
  - Self enrolment required!
  - Lecture slides
  - General announcement
  - Questions to the whole class (students + professor)
  - Submission (e.g. presentations, hand outs)
  - LMS sends notifications to your …@student.fh-kiel.de email address

News forum

Organisation

- Lecture:
  - Wednesday, 08:15 – 09:45
- Seminar:
  - Saturday 10th June + Sunday 11th June + Sunday 18th June
  - talk + handout
  - (exactly) 2 persons per topic
- Exam:
  - 60 min
  - includes questions from seminar!

Not on April, 26th

Attendance mandatory

Lecture starts at 08:15 …

Organisation

- Seminar grading:

Content	30%
Slides	20%
Talk	30%
Handout	20%

-5% per session not attended
(except sick note)

- Final grade:

Written Exam	50%
Seminar	50%

Seminar

- Preparation
  - perform thorough research (standards/specs, Web blogs, white papers, books, *NOT just Wikipedia*)
  - one meeting for discussing the intermediary results / preliminary presentation
    (on 15th and 16th May; time table will be announced)
- Content (not necessarily in this order):
  - motivation / introduction
  - overview / functionality / examples / application
  - advantages / disadvantages / weaknesses
  - some technical details
  - summary / outlook

Seminar

- Slides:
  - “Nice” design
  - Figures (preferable own figures)
  - Referencing external sources (like seen in PM100)
  - Slide numbers
  - Plagiarism → seminar failed
- Presentation:
  - **30 – 35** min presentation (not less, not more!)
  - No videos
  - Live/practical demonstration (where suitable)
- Hand-out (exactly 2 pages)

Time Management is important

Seminar Talk

- How to get a good seminar talk? – 3 means
  1. Practice
  2. Practice
  3. Practice
- Practice:
  - Give the talk to other people (not just in your head)
  - Measure the time your need (the actual talk will probably be a little shorter)
  - Listen to the feedback
- Typical mistakes:
  - Speech: too fast, too loud, too quietly, monotonous
  - Body language: looking at the screen/wall, hands in pockets, extensive/nervous use of laser pointer
  - Talk: not fluent, literally reading from slides

Handout

- From http://www.sussex.ac.uk/s3/?id=65:
  - Handouts should **not** be a transcript of your presentation but a summary of the important points. Make sure your own presentations notes and the handouts you make for your audience are different so that each is doing its job.
  - Give the title, your name and the date at the top.
    Information should be given in bullet points. No paragraphs of prose!
  - Visually differentiate different levels of information (main points, supports, examples).
  - Cite any sources where appropriate. Give a bibliography of works cited at the end of the handout, using a standard bibliographical style.
  - Include any complicated important material e.g. definitions, tables, illustrations, etc.

Seminar Topics

1. VPN (e.g. PPTP, L2TP, IPSec)
2. Rainbow Tables
3. Tor (anonymity network)
4. Botnets
5. Zero Knowledge Protocols
6. Enigma cipher machine
7. Network penetration testing
8. Steganography
9. Pseudorandom number generator
10. SQL / Command injection
11. Web Attacks (XSS, CSRF etc.)
12. Web Tracking (Cookies etc.)
13. Elliptic Curve Cryptography
14. Crypto currencies (Bitcoin etc.)
15. Ransomware
16. Advanced Authentication (e.g. UAF, U2F, TOTP, HOTP)
17. Letsencrypt, ACME
18. IoT Security
19. Quantum Cryptography
20. PGP + S/MIME
21. Network time synchronization
22. SAML / Shibboleth
23. OAuth / OpenID Connect
24. Cloud Computing Security
25. Recent attacks on TLS
26. TLS 1.3
27. DNSSEC
28. Security for certificates (DANE, CA Pinning, Certificate Transparency etc.)
29. SHA-3 / Keccak
30. Intrusion Detection/Prevention
31. Wi-Fi Security
32. Database encryption
33. OWASP Project
34. Secure Messaging (e.g. OTR, Signal)
35. Voice over IP (incl. Security)
36. Web Application Firewalls
37. SSH
38. EAP / 802.1X
39. Cellular Security (GSM, 3G, 4G, …)
40. AES

Seminar Topics

- Seminar registration + topic selection: Google Form (link below)
- Only possible for 2 person teams
- Pick your 10 most favorite choices
- If possible: topic assigment according to these preferences
- Otherwise: random
- Deadline for registration/selection: Friday 24th (end of day)

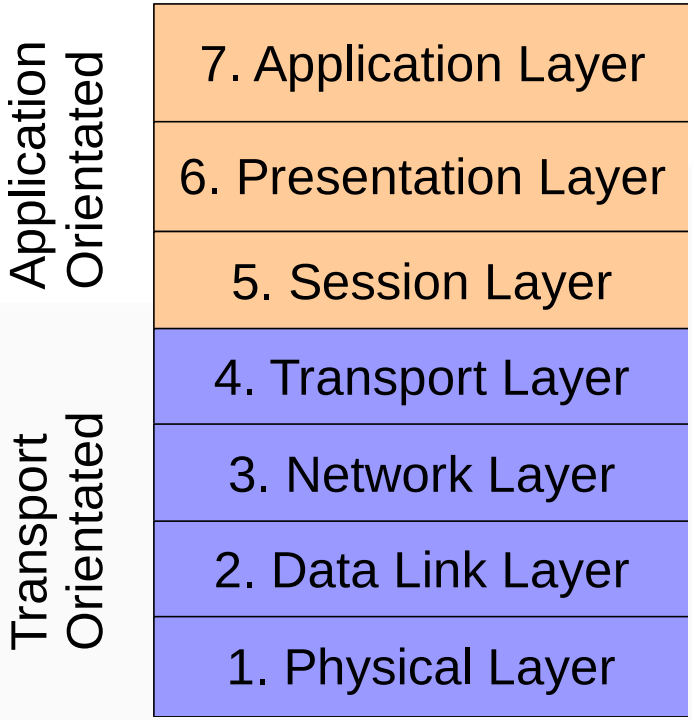
https://docs.google.com/forms/d/e/1FAIpQLSeaV3I4NIherAHBE5bN88VknNz2sYa9-56GXHHHjGqcYj17MA/viewform

Overview

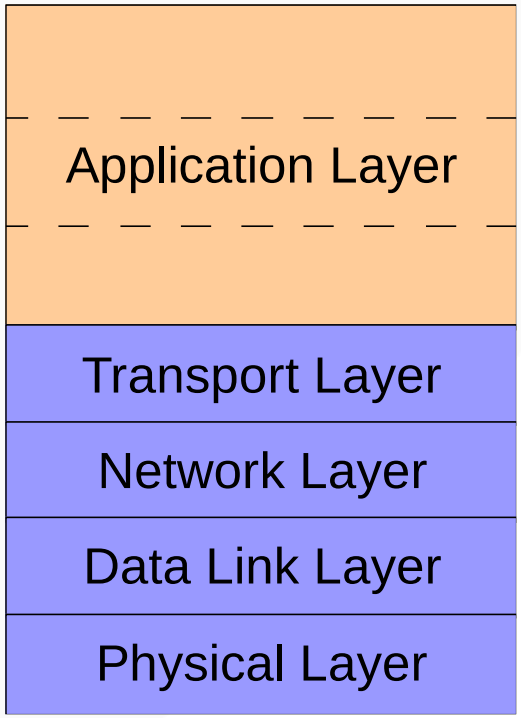
- Recapitulation: Networking
- Computer Security
- Network Design
- Cryptography
- Authentication mechanisms
- Security Protocols
- Web Security

Recapitulation: Networking

ISO/OSI: The Seven Layers Model



Internet:
Simplified Model



Examples

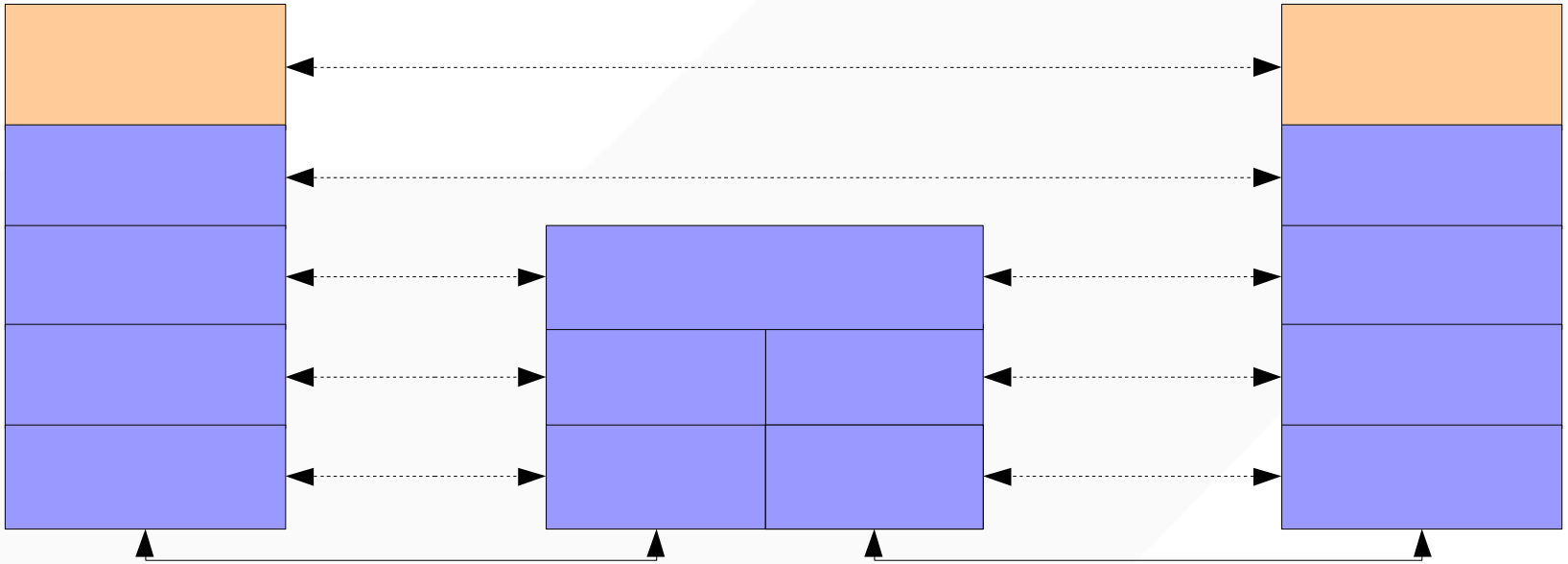
Application Layer	HTTP, FTP, Telnet, DNS, SMTP
	MIME
	SSL ?
Transport Layer	TCP, UDP
Network Layer	IP, ICMP, IPSec
Data Link Layer	PPPoE, 802.3, 802.11
Physical Layer	RS-232, 100Base-TX, 802.11

Protocol Example: Web Access

Notebook:
Web Browser

WLAN-Router:
Access Point +
Router

Server:
Web Server

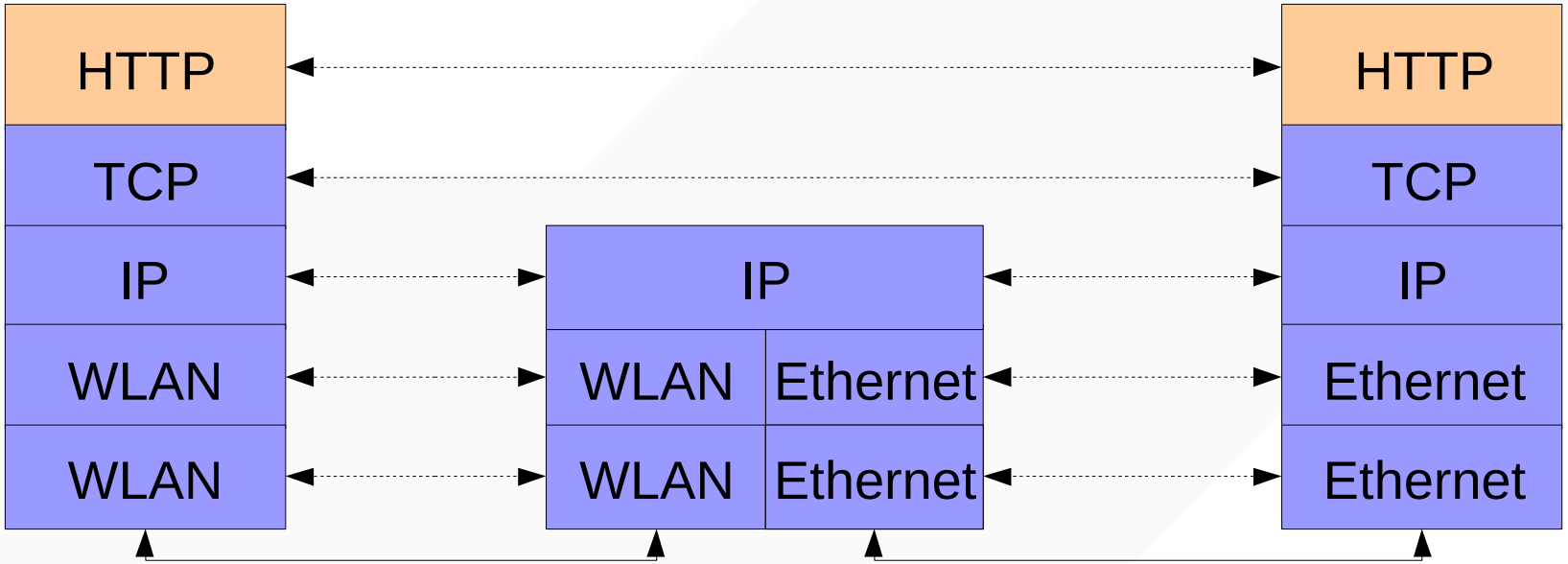


Protocol Example: Web Access

Notebook:
Web Browser

WLAN-Router:
Access Point +
Router

Server:
Web Server



Recapitulation: Networking

- Which QoS parameters are important for VoIP? Which of these are guaranteed by IP?

Recapitulation: Networking

- Which of these properties has IPv4?
  - ☐ connection-less
  - ☐ end-to-end transport
  - ☐ unreliable
  - ☐ multicasting enabled
  - ☐ applications multiplexing
  - ☐ Encryption
- What is the purpose of the TTL field in IPv4?

Recapitulation: Networking

- A host receives (via DHCP) the
  IP address 130.247.204.119, net mask 255.255.224.0
  - What is the address of his subnet?
  - What is the maximum number of hosts inside this subnet?
  - What is the broadcast address of the subnet?

Recapitulation: Networking

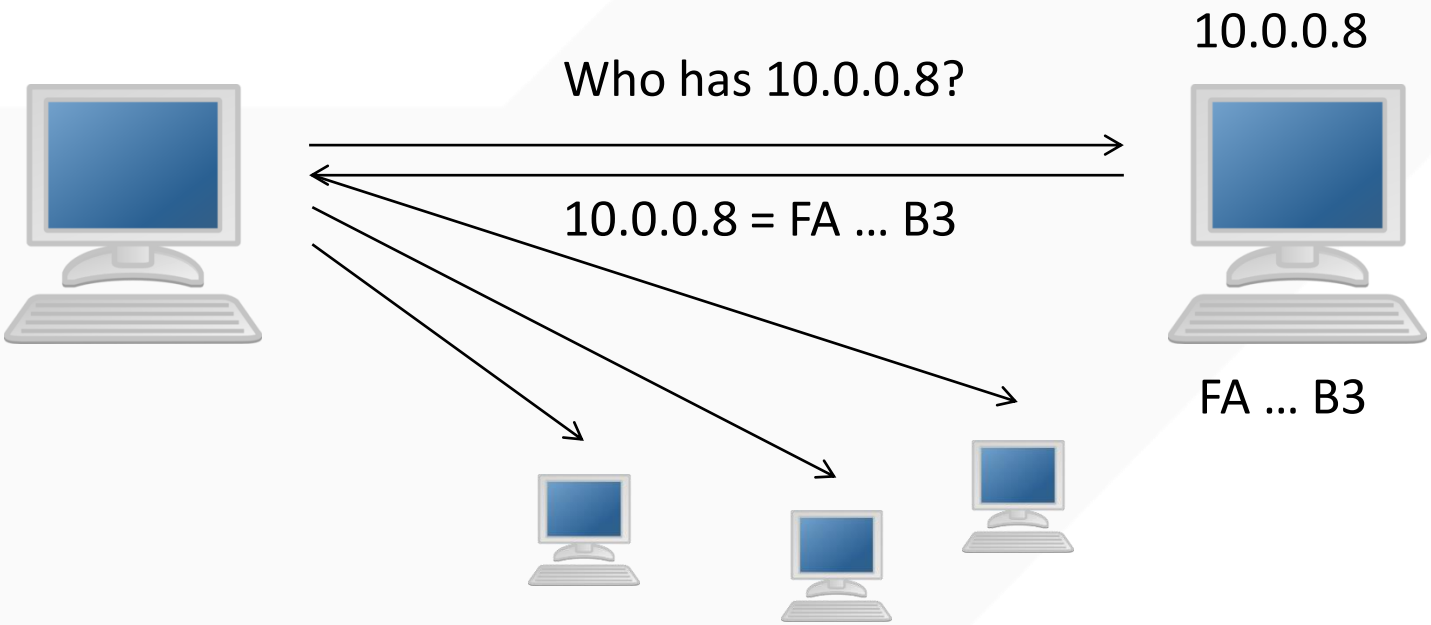
- Explain the following Routing Table
  (own IP address: 10.1.2.5, net mask: 255.255.255.0).

Destination	Gateway	Genmask	Iface
10.1.7.0	10.1.2.77	255.255.255.0	eth0
10.1.2.0	0.0.0.0	255.255.255.0	eth0
0.0.0.0	10.1.2.1	0.0.0.0	eth0

- How does the network environment look like?

ARP

- Adress Resolution Protocol
- Maps inside local networks from IP adress to MAC adress



ARP Spoofing (Redirection Attack)