Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 01: Fundamentals
Module 03: Design and Working of the Internet

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

Learning Objectives

The operation of the Internet in a nutshell

- Identify the key components of the Internet protocol suite
- Know bits of the philosophy behind the development of the Internet
- Understand the fundamental design principles underlying the Internet
- Discuss the development of the Internet and its implications on security
- Recognize that providing security-aware protocols is no panacea

You want to connect a bunch of heterogeneous computers that are potentially spread over the world …

Which layer is key?

Overview of this Module

(1) The network layer
(2) Design principles underlying the Internet
(3) Problems of IPv4 and the Internet in general
(4) The working of the Internet: an example
(5) Protocols, protocols, protocols
(6) Recommended readings

Chapter 01, Module 03

The Network Layer

The network layer

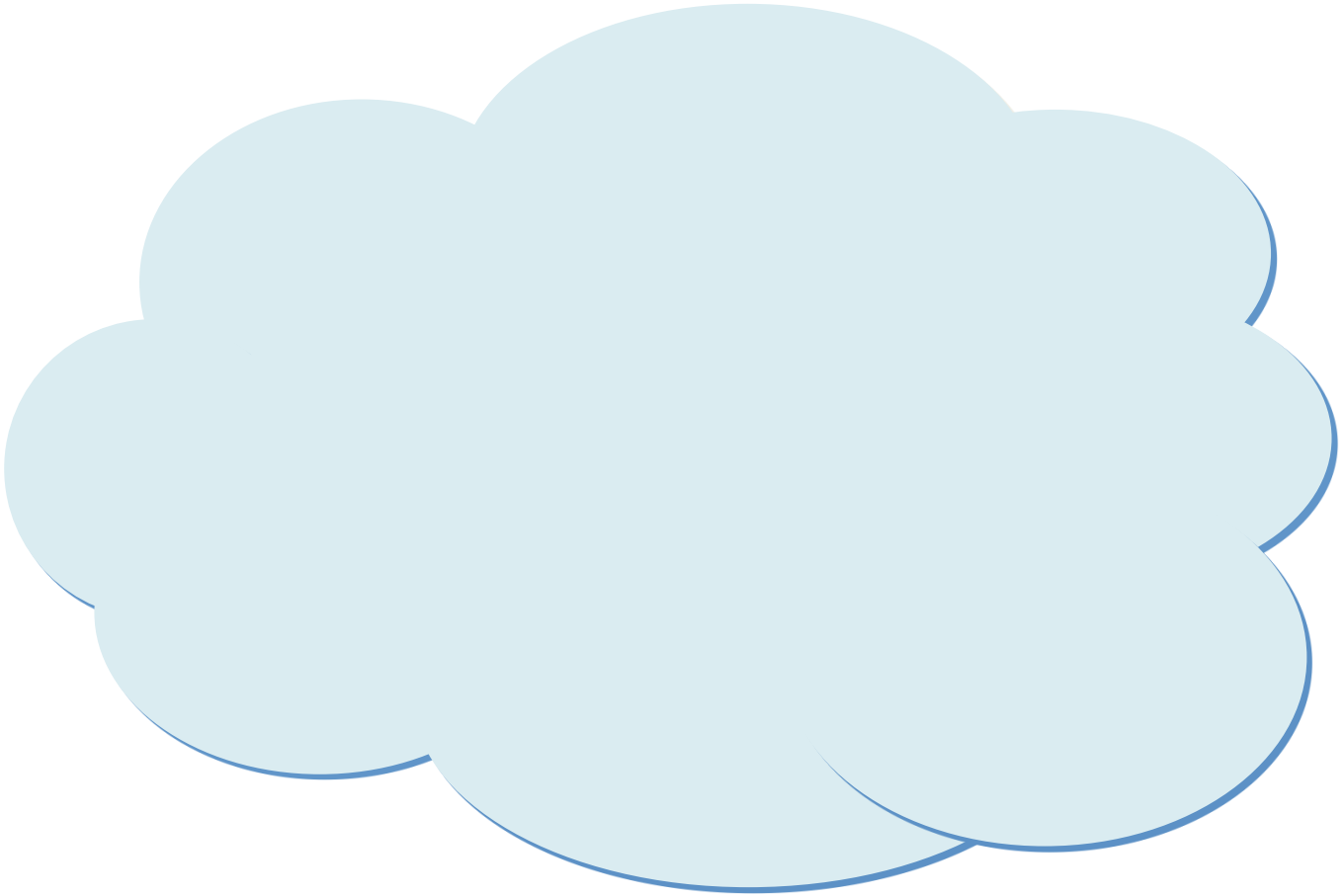
- Virtual circuits and/or datagram transmissions
- Routing
- Congestion control
- Internetworking
- Addressing
- Quality of Service (QoS) (e.g. bandwidth, delay, error rate)

[Tanenbaum2004]

- Enables any pair of systems in the network to communicate with each other
  - Finds a path through a series of connected nodes
  - Nodes along the path forward packets appropriately
  - Calculates routes, fragments and reassembles packets

[Perlman1999]

The Network Layer Visualized



The Internet Protocol (IPv4)

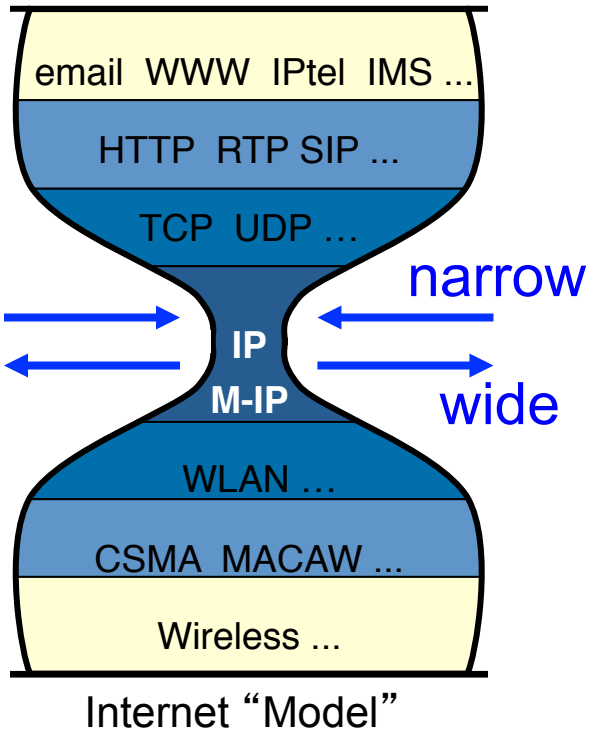
Before IP

- Networks connected by Application Layer Gateways (ALGs)
  - Loss of functionality
  - Difficult application deployment

Why an internet layer?

A single or multiple internet protocols?

A narrow or wide internet protocol?



Internet "Model"

The Internet Protocol (IPv4)

Why an internet layer?

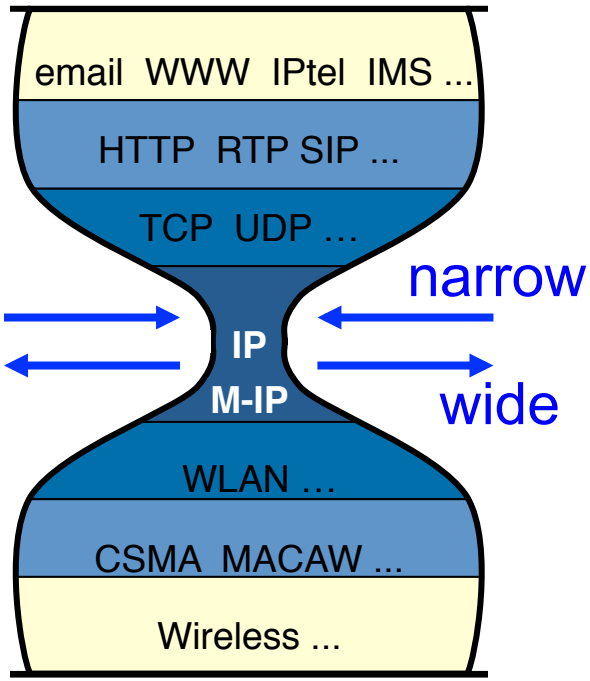
- Make a bigger network and overcome ALGs
- Global addressing
- Virtualize network to isolate end-to-end protocols from network details/changes

Why a single internet protocol?

- Maximize interoperability
- Minimize number of service interfaces

Why a narrow internet protocol?

- Assumes least common network functionality to maximize number of usable networks



Internet "Model"

History and Facts about IPv4

IPv4 has been incredible successful

- Was designed early in the 70s (packet switching idea)
- Was refined/enhanced/fixed to deal with problems

Many add-ons to the protocol

- Security (IPsec) to provide for network layer security
- Mobile IP to support mobility, DiffServ to support QoS
- Network Address Translation (NAT) to allow for private networks (Intranets) and to deal with address shortage
  - Using one add-on → trivial; using two at the same time → tricky; using three or more → acrobatic

The current Internet presents facts like

- Firewall Systems, VPNs, Proxies, Caches, SOCKS, dynamic and unstable addresses (PPP, DHCP), private addresses, …

Problems of IPv4

Today transparency has gone

- NAT, Intranets, VPNs, Firewall Systems, Proxies, Caches, …

Applications either fail completely, or need modification, or must be specially handled by Firewall/NAT

- Consequence: it's almost impossible to deploy new applications and/or protocols globally (think of IPSec and Mobile IP in IPv4)
- Consequence: there is a strong temptation to layer new applications over old ones ("everything over HTTP")

Solve Problems of IPv4

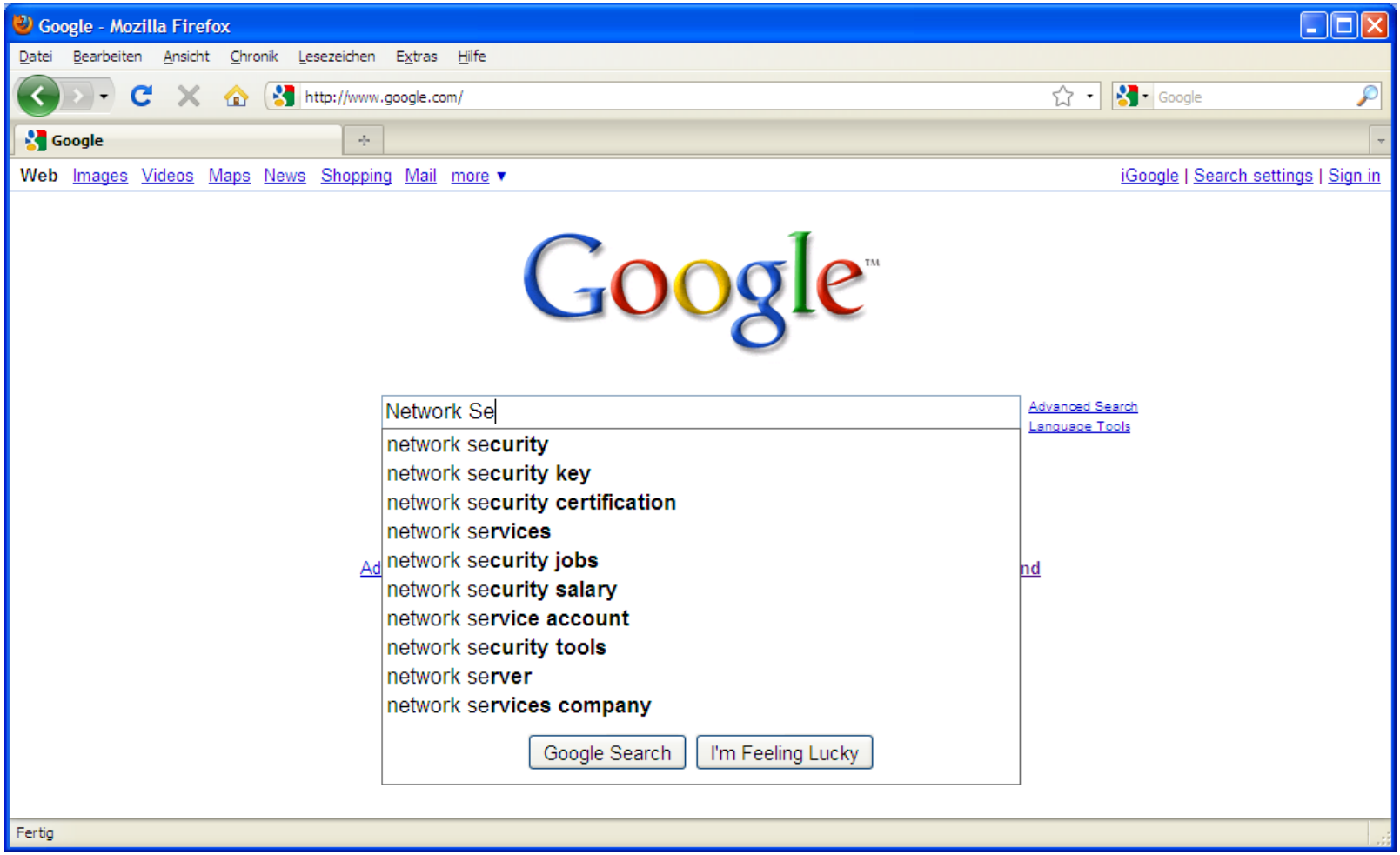
"All problems can be solved using add-ons, so what?"

- Basic concept of the Internet (~1973), is one of transparent transmission of datagrams across an arbitrary network of networks
  - Logical addresses were unique
  - Datagrams were not changed in transit
  - End-systems handle error detection, retransmission, security, naming, and binding
- This concept determined the basic design of most Internet applications

SEEMOO
SECURE MOBILE NETWORKING

Internet at Work

Example: Google Important Stuff



Which Steps are Performed

How to get there

Need to find a server first … Domain Name Service (DNS)

- Distributed database for looking up names and getting IP addresses (etc.)
- Control is delegated. If you control foo.com, you can assign names of the form *.foo.com, or delegate a subdomain
- Each client must know at least one DNS-server IP address (can be learned with DHCP)
- Each server knows addresses of subdomain servers, and at least one root server

DNS Lookup

- Sequence might be: your local server, the root, child, child, until target
- Server can answer your request (recursive) or tell you who to ask next (iterative)
- Caching at all places

What happens in the Network

Contd.

- DNS looks up GOOGLE.COM to find a corresponding IP address
- Network infrastructure (routers) cooperate to calculate paths to IP addresses
- One side needs to be easily findable, and listens for calls

Lower layers

- Layer 3 (e.g., IP) is just an envelope in which you specify source, destination address (and hop count)
- Layer 2 used to be point-to-point links, not needing an address, but became LANs, with their own addresses ("MAC" address)
- The way IP works is that all nodes on the LAN share a prefix

Start to move Packets

IP Forwarding

- You can tell from address if someone is a neighbor (iff same prefix)
- If so, send to them, but need their layer 2 address
- Use ARP…broadcast "who has this layer 3 address" get back reply from them
- If not on same link, send to router

How to discover router

- Lots of ad hoc methods. Was better designed in ISO's layer 3 (CLNP). In IP, some just configured with a static router (rtr) address
- Thus comes in VRRP (virtual router redundancy protocol)
  - CISCO Marketing: The *Virtual Router Redundancy Protocol* (*VRRP*) eliminates the single point of failure inherent in the static default routed environment

How to discover Gateways

How to identify gateway/router

- A bunch of routers on the LAN elect one of them to have the IP address “R1”, and associated MAC address. That one periodically issues “I’m still alive” messages to the other VRRP (Virtual router Redundancy Protocol) routers, sending from its MAC address

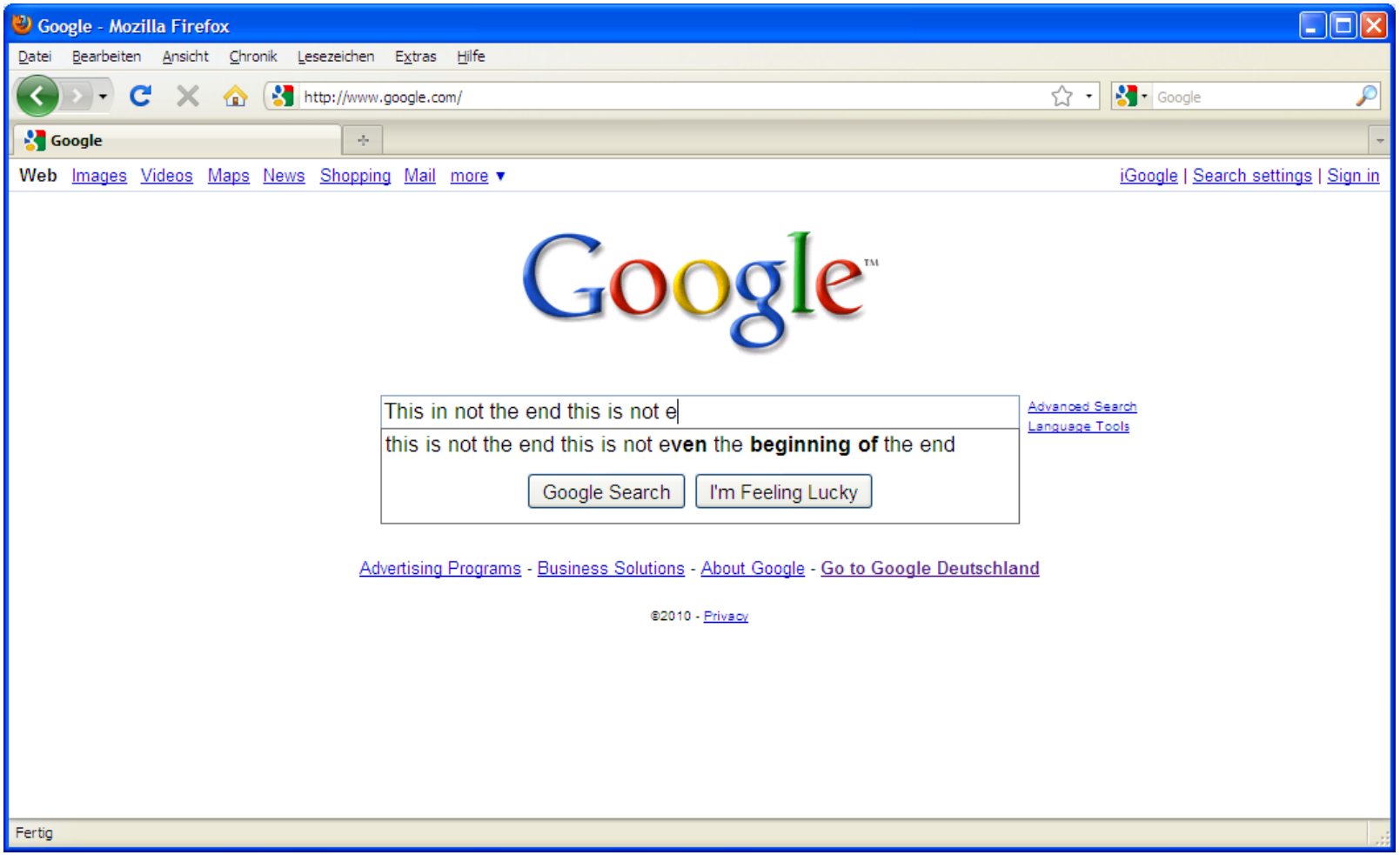
Interacts with Bridges

- Bridges/switches are “invisible” layer 2 devices which listen promiscuously and learn the location of stations based on the source address in the layer 2 header

VRRP is security-aware

- 2 types: cleartext password, cryptographic

We Stop our Example Here …



Discussion: Where do You see Potential Problems?

The Internet (as seen by Politicians)

SEEMOO
SECURE MOBILE NETWORKING

" Ten movies streaming across that, that Internet, and what happens to your own personal Internet? I just the other day got...an Internet was sent by my staff at 10 o'clock in the morning on Friday. I got it yesterday [Tuesday]. Why? Because it got tangled up with all these things going on the Internet commercially. [...] They want to deliver vast amounts of information over the Internet. And again, the Internet is not something that you just dump something on. It's not a big truck. ***It's a series of tubes.*** *And if you don't understand, those tubes can be filled and if they are filled, when you put your message in, it gets in line and it's going to be delayed by anyone that puts into that tube enormous amounts of material, enormous amounts of material. "*

Ted Stevens, US Senator

Protocols

Protocols

Protocols

Protocols

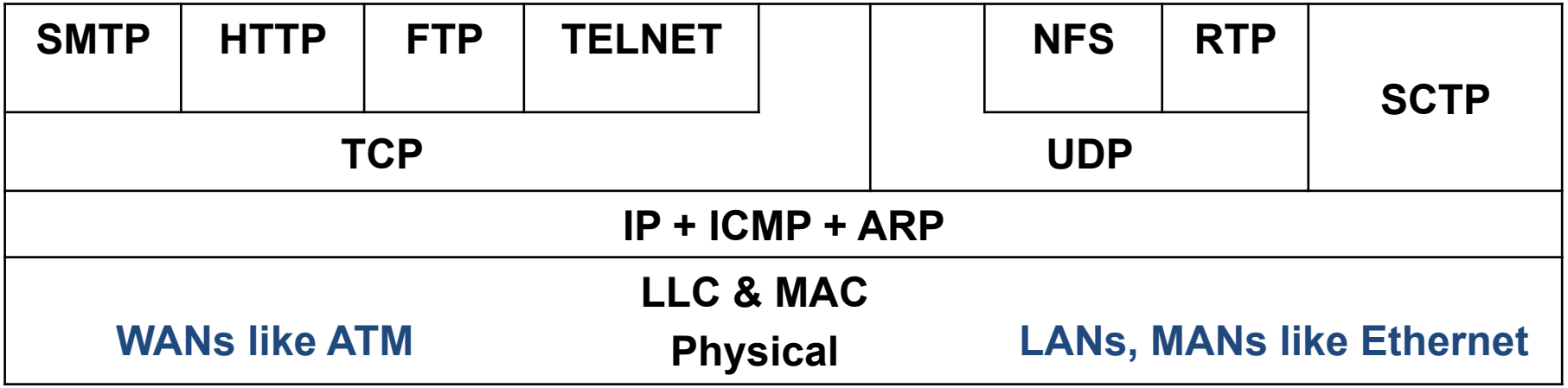
Protocols

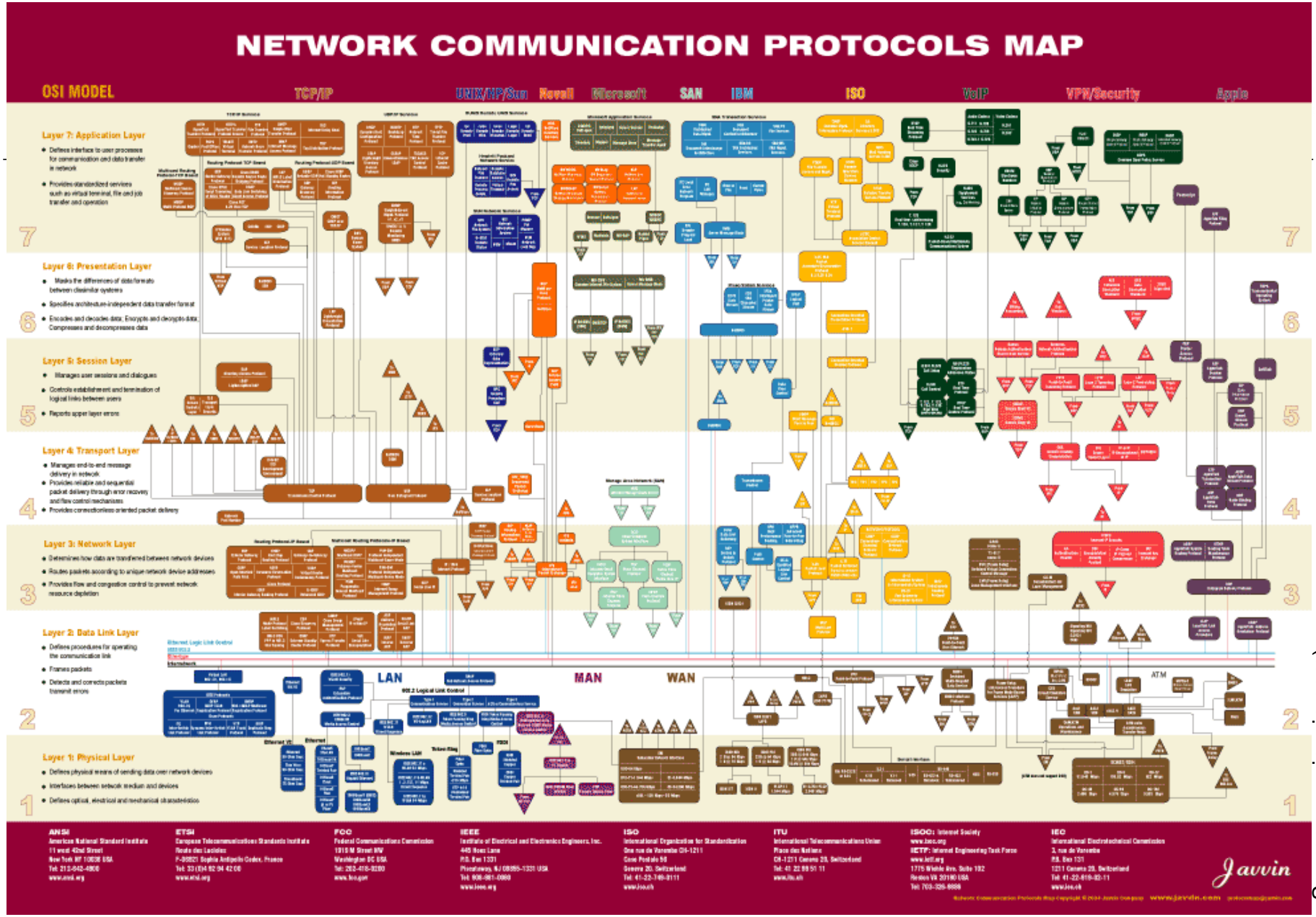
Protocols

Protocols

Well-Known Internet Protocols

ARP: Address Resolution Protocol
DNS: Domain Name Service
FTP: File Transfer Protocol
HTTP: Hypertext Transfer Protocol
IP: Internet Protocol
ICMP: Internet Control Message Protocol
LLC: Logical Link Control
MAC: Media Access Control
NFS: Network File System
RTP: Real-time Transport Protocol
SMTP: Simple Mail Transfer Protocol
TELNET: Remote Login Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
SCTP: Stream Control Transmission Protocol





Source www.javvin.com)

Summary

Recommended Reading

The following article discusses the end-to-end argument (one of the fundamental design paradigms underlying the internet):

- Saltzer et al. *"End-To-End Arguments In System Design"*

The following article discusses fundamental challenges for communication systems:

- Clark et al. *"Making the World (of Communications) a Different Place"*

Additionally, there are a number of textbooks on the subject, including the one by Kurose et al., the one by Tanenbaum, etc. (I guess, we keep repeating us ;-)

- [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

SECURE MOBILE NETWORKING

Take away message: some security mechanisms are just snake oil; just creating a false feeling of security (or even harm the system)