Protocols

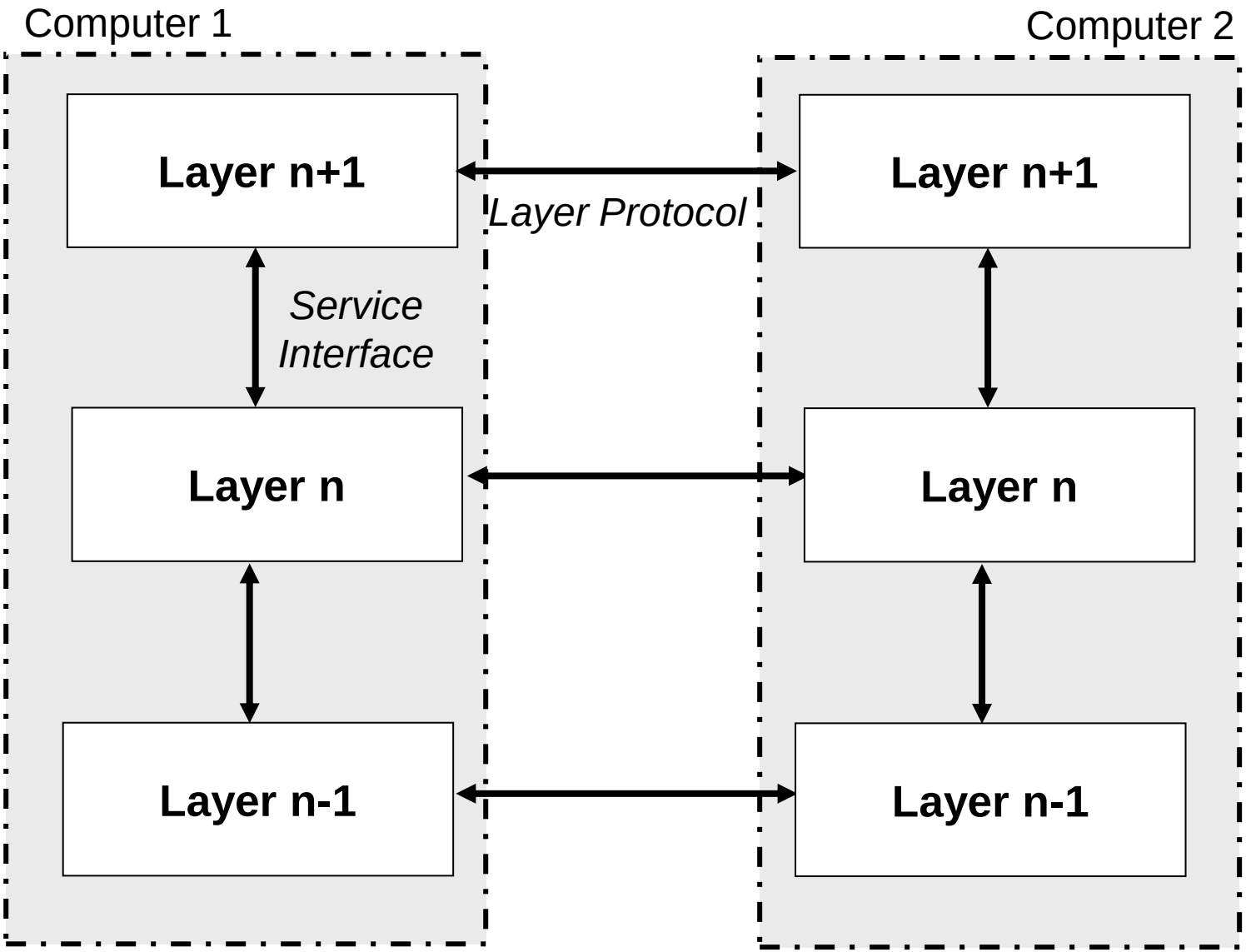
- Protocols are formal rules of behaviour and specify the "HOW"
- The Tasks of a Protocol are:
  - Addressing of Communication Endpoints
  - Management of Data Flow
  - Provision of a secure Data Transmission Service
- Example: PPP (Point-to-Point Protocol, Data Access via Modem)

- -> Serial/Parallel Communication

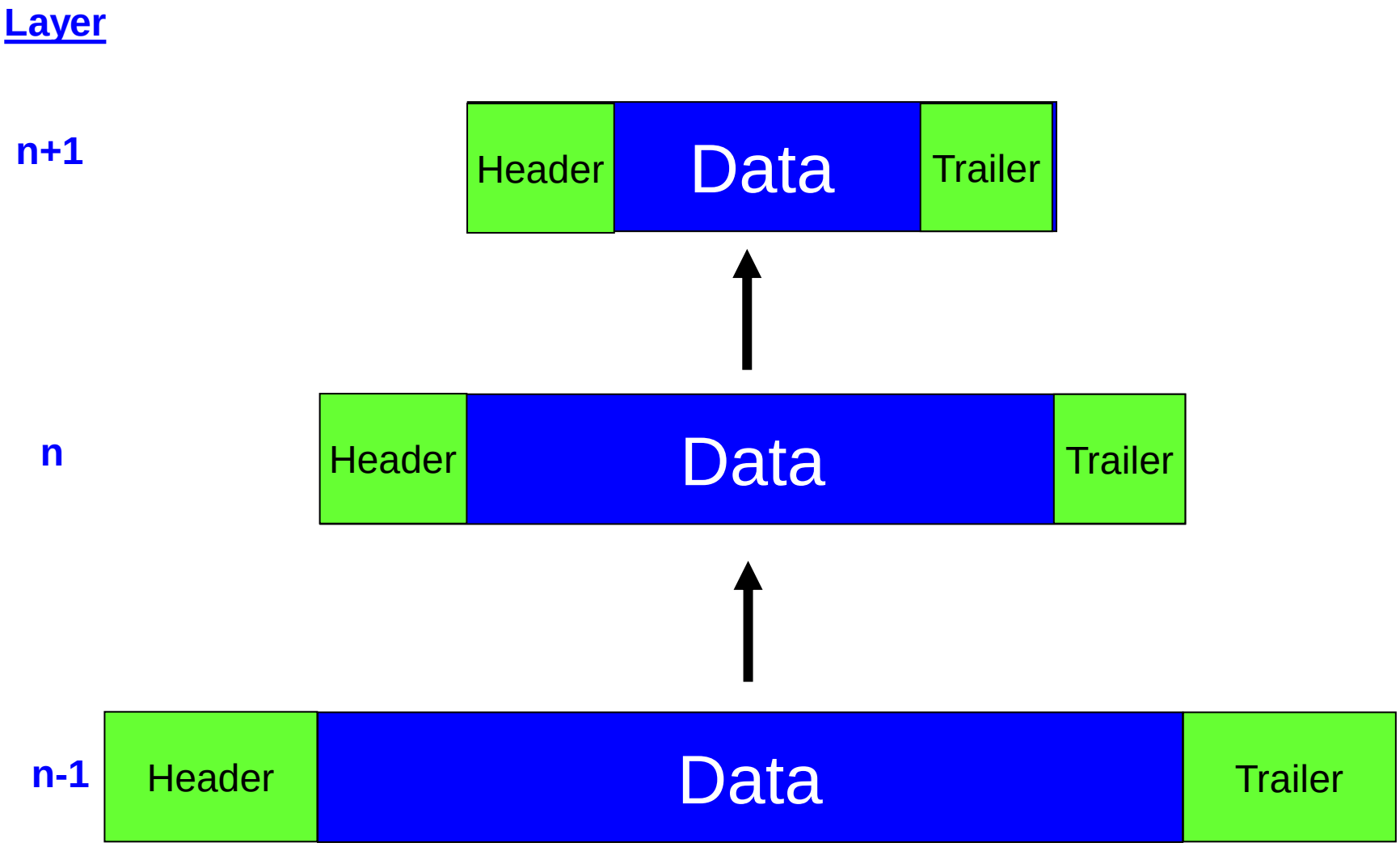
Services

- Services are Groups of Operations and specify the "WHAT"
- Can be connectionless (e.g., like "snail mail")
- Can be connection-oriented (e.g., like a phone call)
- Example: WWW (World Wide Web)

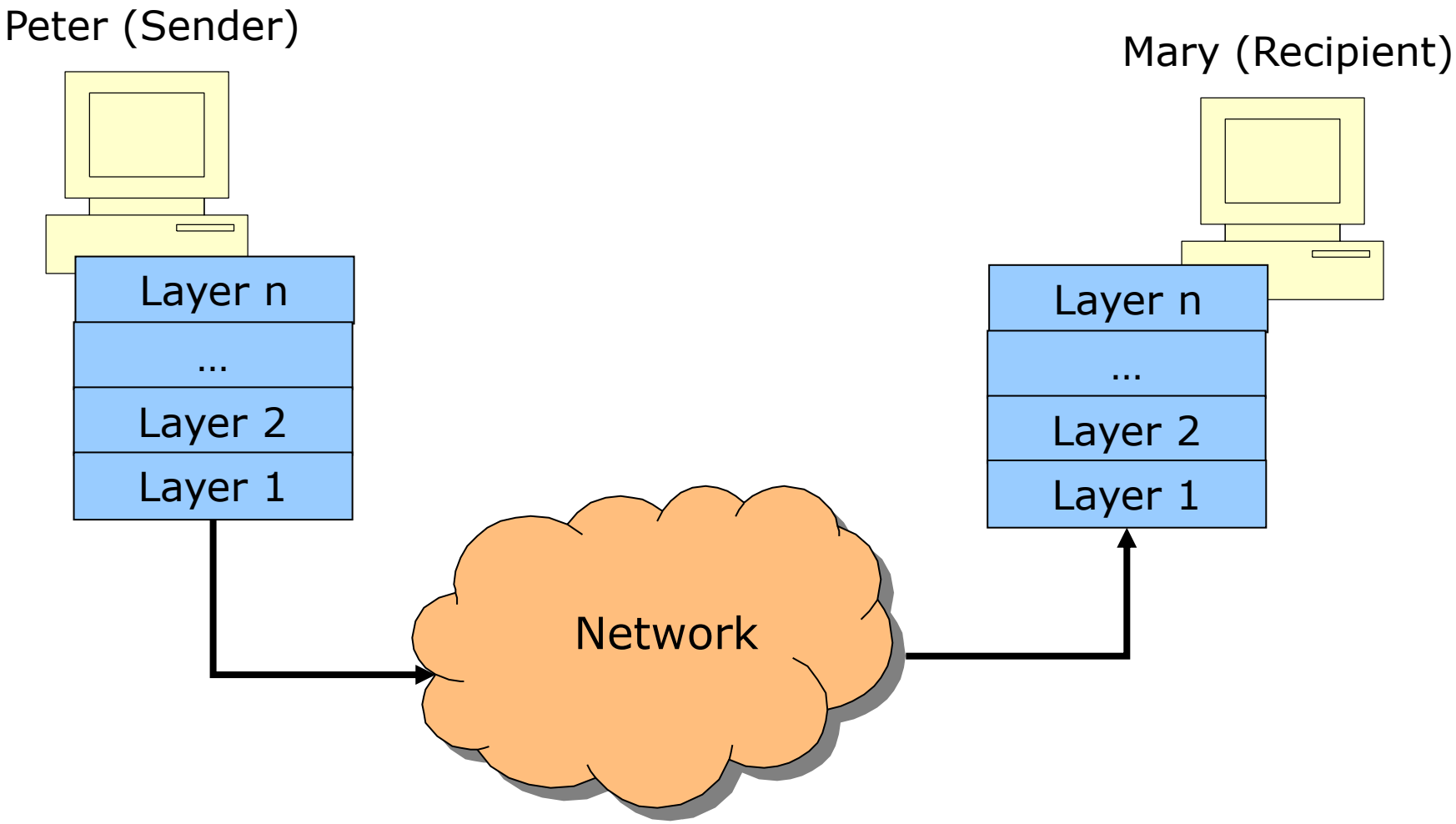
Layer Model


Computer 1
Computer 2
Layer n+1
Layer n+1
Layer Protocol
Service
Interface
Layer n
Layer n
Layer n-1
Layer n-1

Layer Data

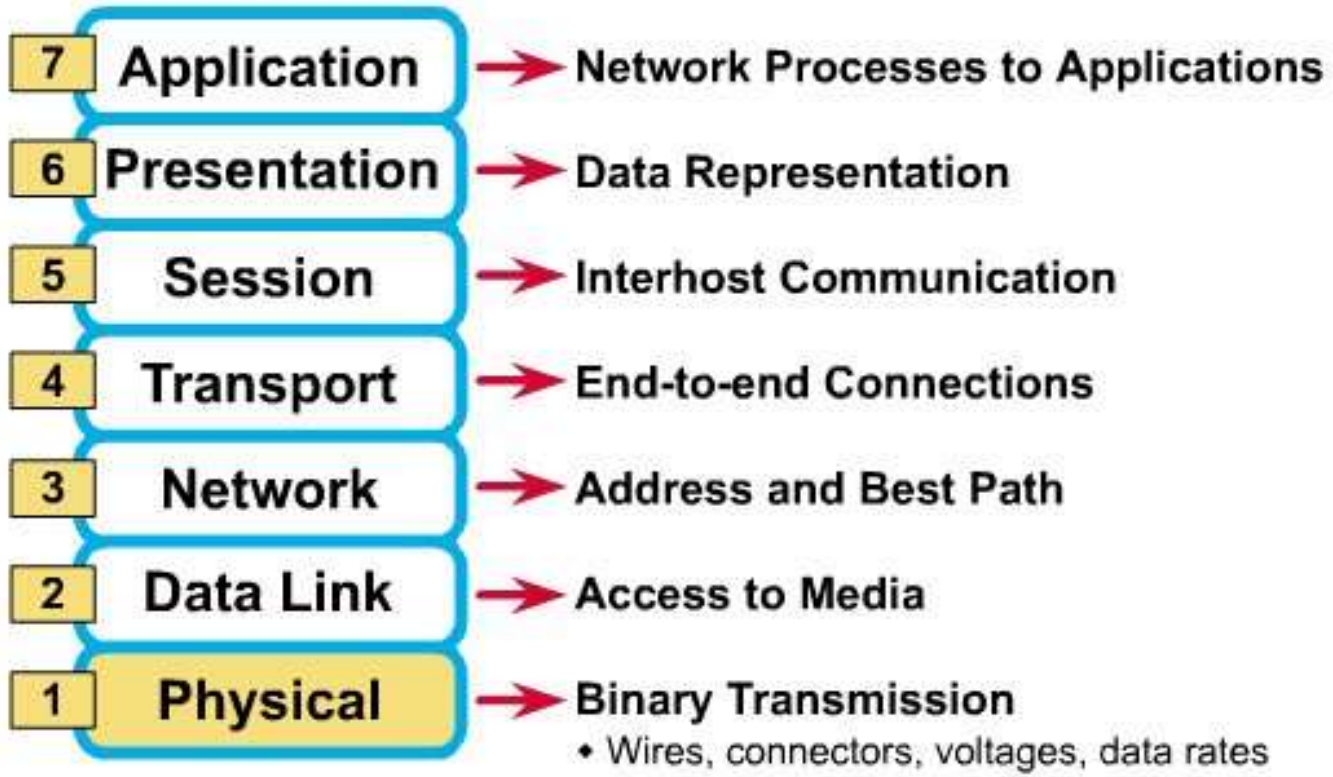


Layer-based Inter-Computer Communication



OSI Reference Model

- The OSI Reference Model is a “reference guide” for understanding network functionality.
- Each of the 7 layers (numbered from bottom to top) represents one step in the process of sending data packets from a source to a destination.



The Postal Analogy

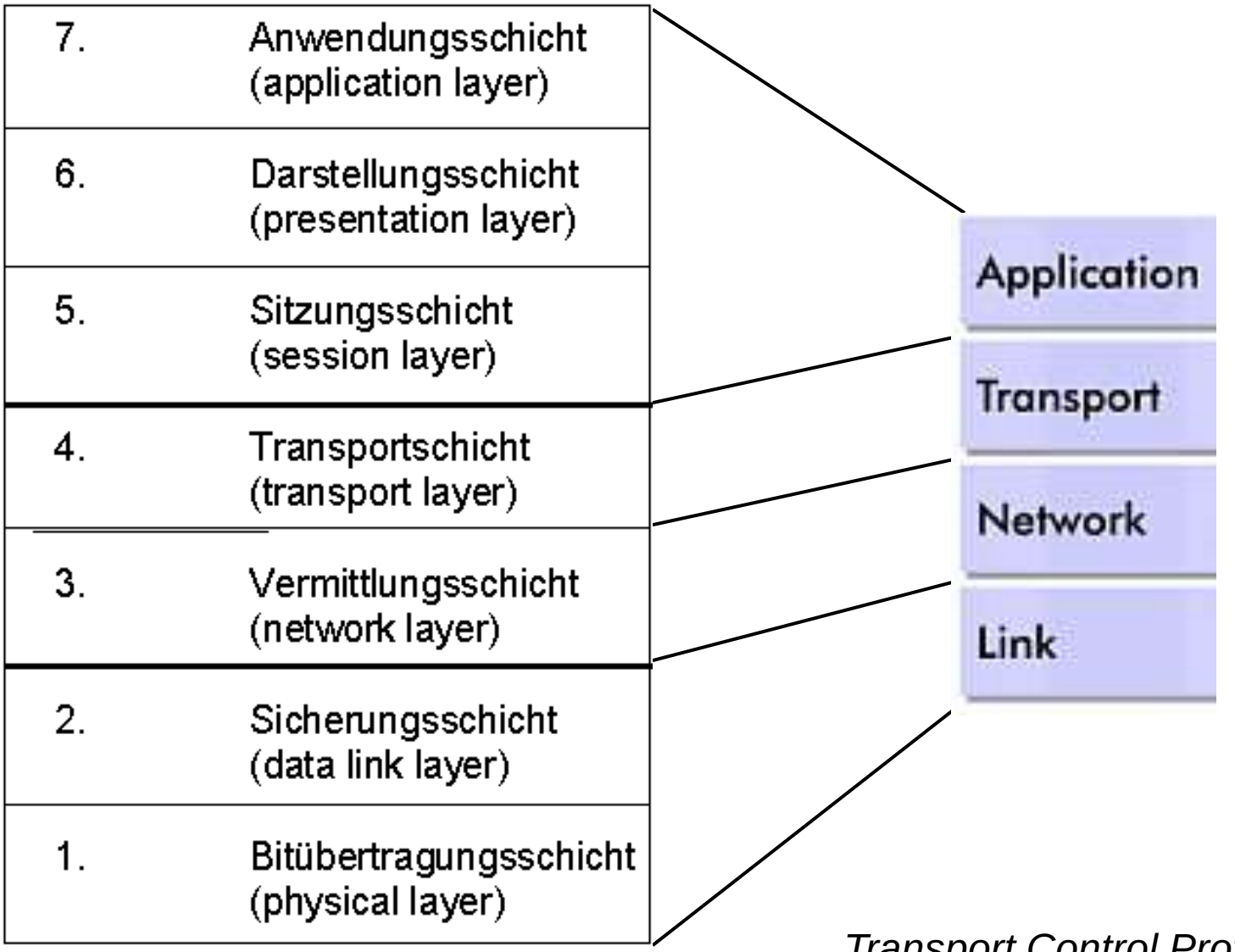
How would the OSI compare to the regular Post Office

- **A**pplication
- **P**resentation
- **S**ession
- **T**ransport
- **N**etwork
- **D**ata-Link
- **P**hysical

- **A-** Write a 20 page letter to a foreign country.
- **P-** Translate the letter so the receiver can read it.
- **S-** Insure the intended recipient can receive letter.
- **T-** Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
- **N-** Postal Center sorting letters by zip code to route them closer to destination.
- **D-** Local Post Office determining which vehicles to deliver letters.
- **P-** Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

"**A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing"

OSI Reference Model and TCP/IP Protocol



OSI Model

Transport Control Protocol/ Internet Protoocol

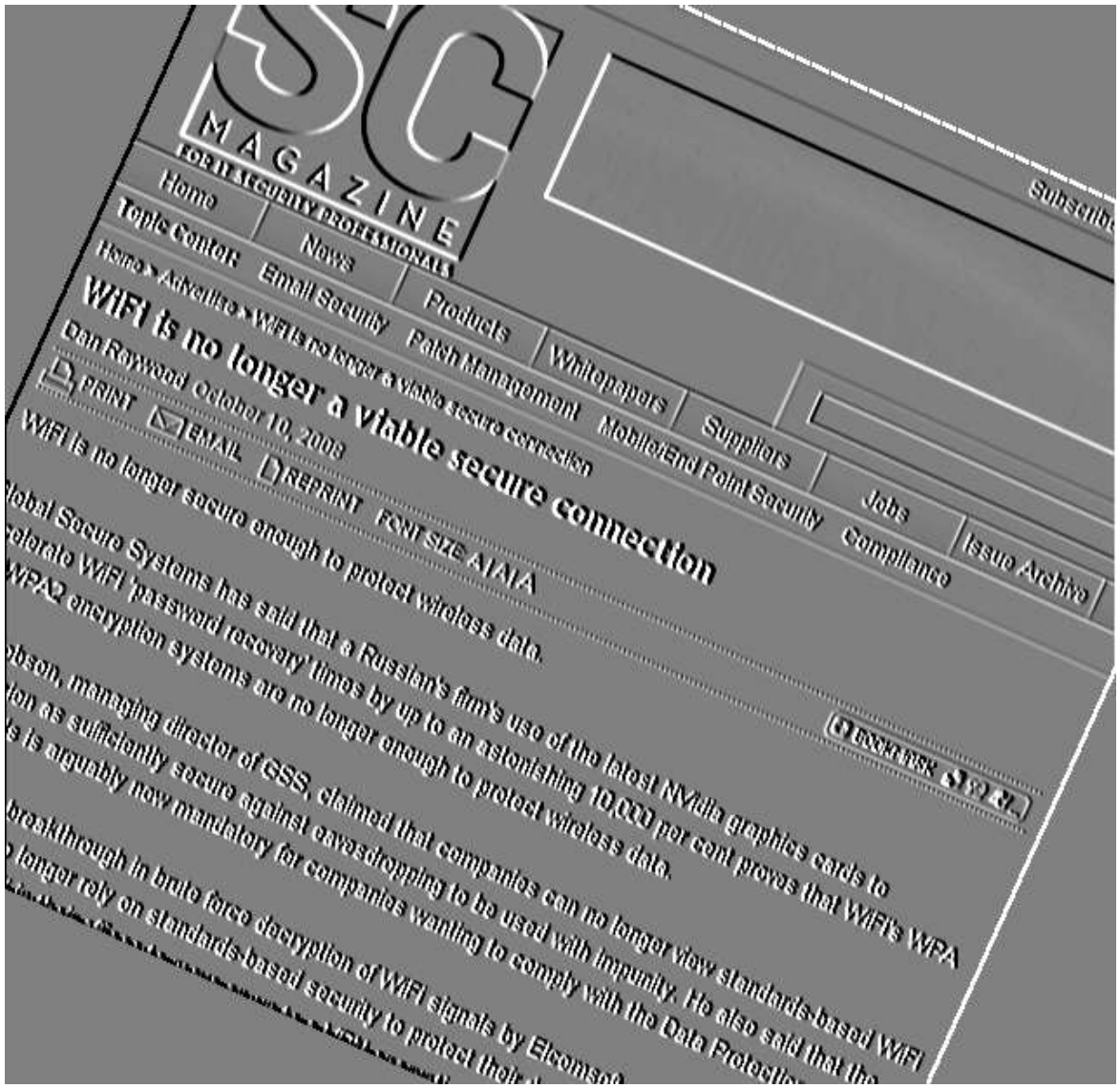
Internet Protocol Suite

- 5. Application Layer
  - DHCP · DNS · FTP · Gopher · HTTP · IMAP4 · IRC · NNTP · POP3 · SIP · SMTP · SNMP · SSH · TELNET · RPC · SOAP · NTP · …
- 4. Transport Layer
  - TCP · UDP · …
- 3. Network/Internet Layer
  - IP (IPv4 · IPv6) · IPsec · ARP · RARP · …
- 2. Data Link Layer
  - 802.11 (WLAN) · (Wi-Fi) · WiMAX · ATM · Token ring · Ethernet · FDDI · GPRS · PPP · ISDN · …
- 1. Physical Layer
  - Ethernet physical layer · Modems · Optical fiber · Coaxial cable · Twisted pair · …

Source: en.wikipedia.org

WiFi is secure, but...

Is Wifi still secure?



WiFi is no longer a viable secure connection?

tinyurl.com/4sq5fn

- Wifi (WPA, WPA2) is said to be "secure"
- Max. Password Length: 63

Characters	
A-Z	26
a-z	26
0-9	10
äüö/\?!-&%$"()=+#ß	18
Sum:	80

- Can only be attacked by "brute-force" attacks
- Russian Company ELMSOFT announces in 2008 "to break Wi-Fi encryption up to 100 times faster than by using CPU only" (tinyurl.com/4585wv)
- Should be all return to cable-based networks?

The Approach of Wifi Hacking

- Logging of Network Traffic (esp. Authentication)
- Offline Brute-Force Attack (pot. dictionary-based)

- Max. Password Length: 63, Number of Characters: 80
  - -> 80^n permutations for a password of length n

- Dictionaries can speed-up the hacking... however
  - language-specific dictionaries are required ("Vogel", "Bird", "Uccello")
  - what about combination of words and numbers/spec. characters like
    - "Vogel0815", "Bird;!$%&", ...

How long does it actually take?

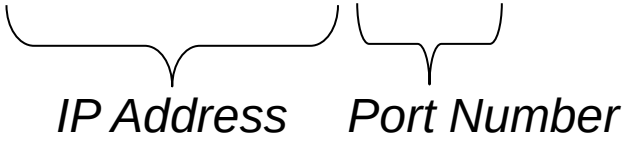
Passwort Length	Permutations	100 PWs/sec (years)	1000 PWs/sec (years)	100.000 PWs/sec (years)	1 Mio. PWs/sec (years)	10 Mio. PWs/sec (years)	100 Mio. PWs/sec (years)
1	80	2,53678E-08	2,53678E-09	2,53678E-11	2,53678E-12	2,53678E-13	2,53678E-14
2	6400	2,02943E-06	2,02943E-07	2,02943E-09	2,02943E-10	2,02943E-11	2,02943E-12
3	512000	0,000162354	1,62354E-05	1,62354E-07	1,62354E-08	1,62354E-09	1,62354E-10
4	40960000	0,012988331	0,001298833	1,29883E-05	1,29883E-06	1,29883E-07	1,29883E-08
5	3276800000	**1,039066464**	0,103906646	0,001039066	0,000103907	1,03907E-05	1,03907E-06
6	2,62144E+11	83,1253171	**8,31253171**	0,083125317	0,008312532	0,000831253	8,31253E-05
7	2,09715E+13	6650,025368	665,0025368	**6,650025368**	0,665002537	0,066500254	0,006650025
8	1,67772E+15	532002,0294	53200,20294	532,0020294	**53,20020294**	**5,320020294**	0,532002029
9	1,34218E+17	42560162,35	4256016,235	42560,16235	4256,016235	425,6016235	**42,56016235**
10	1,07374E+19	3404812988	340481298,8	3404812,988	340481,2988	34048,12988	3404,812988
20	1,15292E+38	3,65589E+28	3,65589E+27	3,65589E+25	3,65589E+24	3,65589E+23	3,65589E+22
30	1,23794E+57	3,92548E+47	3,92548E+46	3,92548E+44	3,92548E+43	3,92548E+42	3,92548E+41
40	1,32923E+76	4,21495E+66	4,21495E+65	4,21495E+63	4,21495E+62	4,21495E+61	4,21495E+60
50	1,42725E+95	4,52577E+85	4,52577E+84	4,52577E+82	4,52577E+81	4,52577E+80	4,52577E+79
60	1,5325E+114	4,8595E+104	4,8595E+103	4,8595E+101	4,8595E+100	4,8595E+99	4,85951E+98
63	7,8464E+119	2,4881E+110	2,4881E+109	2,4881E+107	2,4881E+106	2,4881E+105	2,4881E+104

Core2 Duo: ~1.000 PWs/sec.
-> 100 times faster: 100.000 PWs/sec.
-> 100 PCs: 10 Mio. PWs/sec

Exercise 1.2

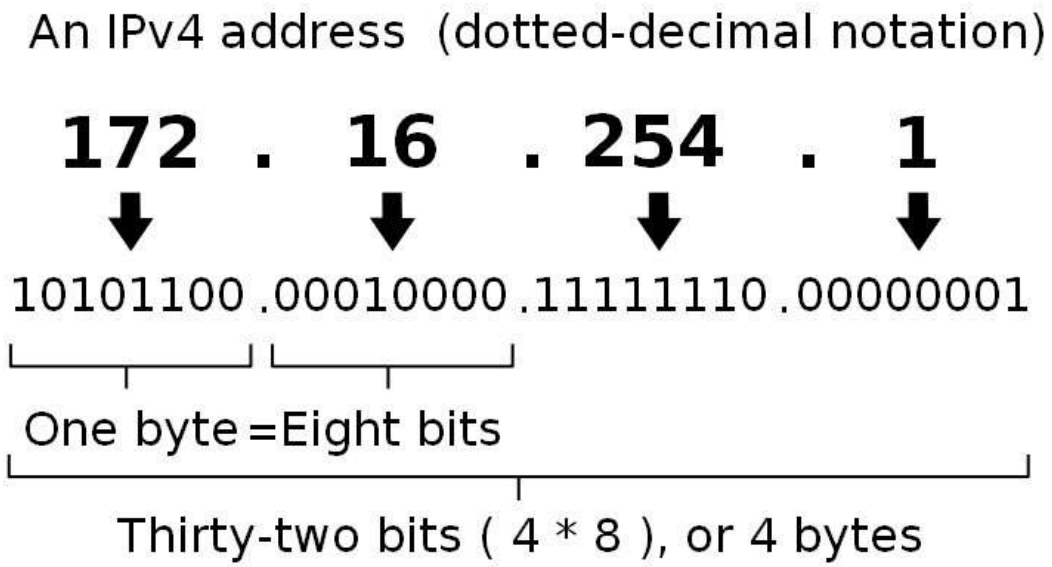
IP Addressing

- Goal: Unambiguous addressing of hosts
- Addressing (within the 4 layers) via:
  - Network Address (e.g., Ethernet Address)
  - Internet Address
  - Transport Protocol Address
  - Port Number
- Example: 192.168.1.5:8080



IP Addresses

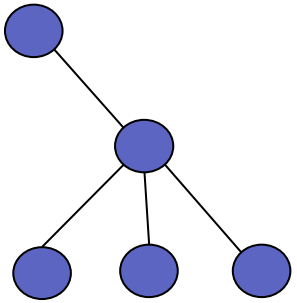
- Numerical Address associated with a network device
- Can be 32-bit number ("original TCP/IP adressing", IPv4) or 128-bit number (IPv6, RFC 1883)
  - IPv4: 2^{32} addresses = 4.294.967.296
  - IPv6: 2^{128} addresses = $3,4 * 10^{38}$



Source: en.wikipedia.org

Classful Networks

- Introduced in 1981 with IP protocol
- First Byte (octet) defines network number, rest defines hosts



Class	First octet in binary	Range of first octet	Network ID	Host ID	Possible number of networks	Possible number of hosts
A	0XXXXXXX	0 - 127	a	b.c.d	128 = 2^7	16,777,214 = (2^{24} - 2)
B	10XXXXXX	128 - 191	a.b	c.d	16,384 = 2^{14}	65,534 = (2^{16} - 2)
C	110XXXXX	192 - 223	a.b.c	d	2,097,152 = 2^{21}	254 = (28 - 2)

Source: en.wikipedia.org

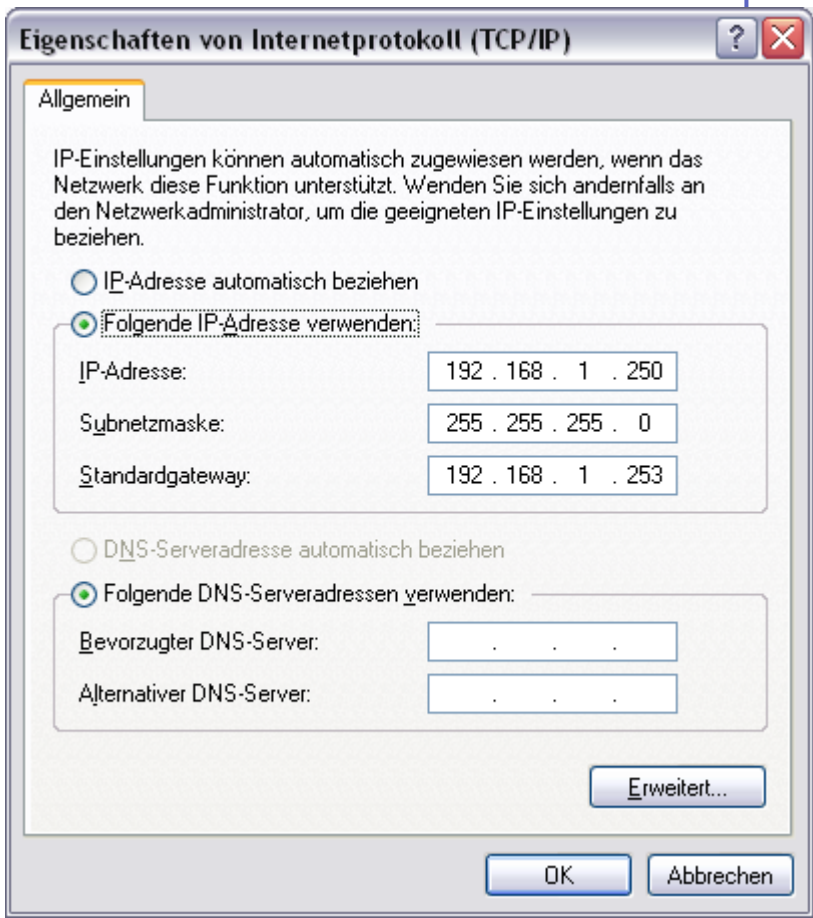
- However, classful networks turned out to be not flexible enough for the Internet

Classless Inter-Domain Routing

- Classless Inter-Domain Routing (CIDR)
- Published in 1993 by IETF (RFC 1518, RFC 1519) to cope with problems of classful networks
- Introduced variable-length subnet masking (VLSM)
  - Address is specified with the number of bits indicating network number, e.g., 192.168.1.253/16

Private Internets

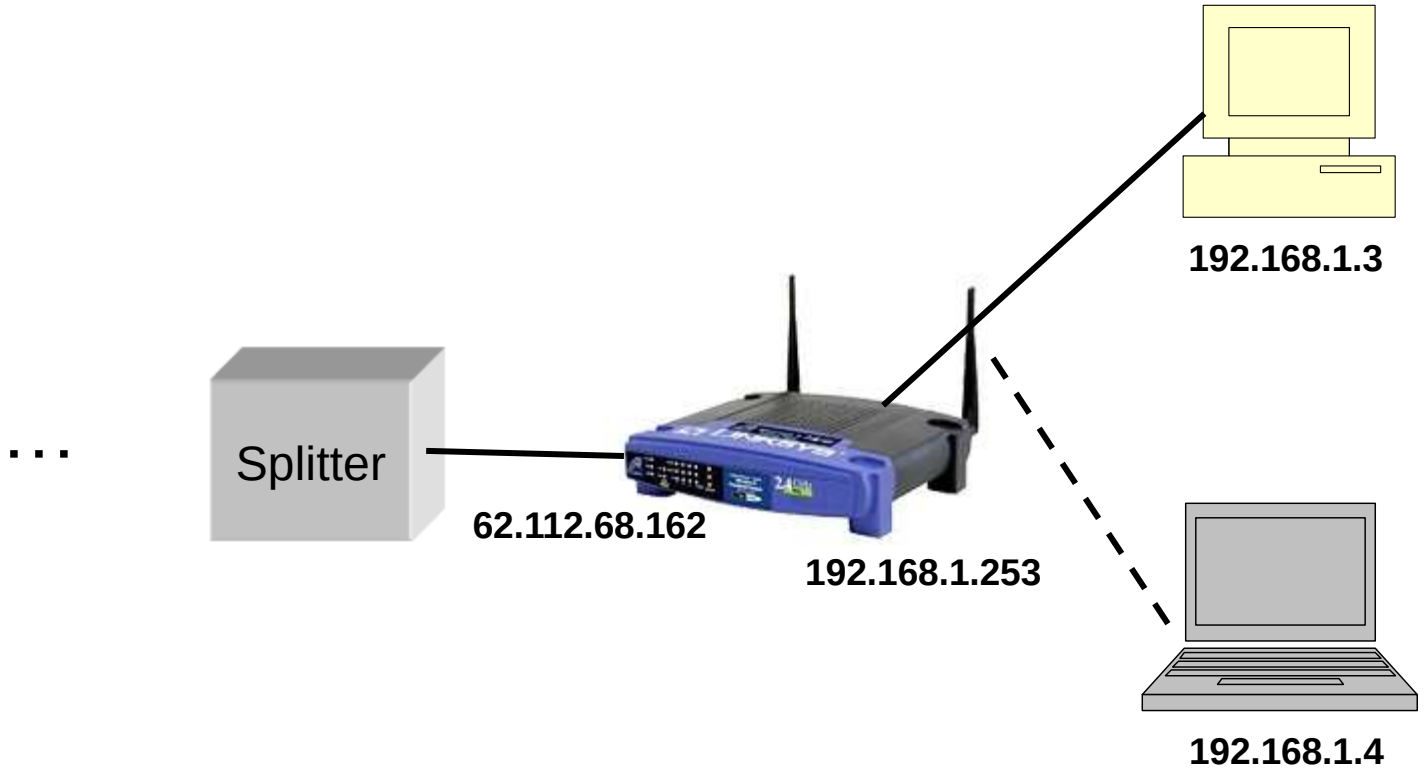
- Internet Assigned Numbers Authority (IANA) reserved three blocks for "private Internets" [RFC 1918]:
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- Hint: Have a look at your Windows TCP/IP Settings



How to get an IP Address

- Bootstrap Protocol (Bootp)
  - used by diskless devices
  - IP Adresses are statically assigned to hosts
- Dynamic Host Configuration Protocol (DHCP)
  - "dynamic bootp"
  - dynamic assignment of IP address range to hosts
  - Time-based assignment ("lease time")

IP Address Translation



What are Ports?

- Ports are conceptual “points of entry” into a host computer.
- They do not correspond with real hardware.
- Usually a service is associated with a port (e.g. http on port 80).
- Servers “listen on a port” for connection attempts.
- Ports provide one level of Internet security.
- Generally, low level ports are reserved for special services.

-> Firewall

TCP Ports

- Adressing of Applications
- Defined Port Numbers:

ftp 21/tcp File Transfer [Control]
telnet 23/tcp Telnet
smtp 25/tcp Simple Mail Transfer
smtp 24/tcp any private mail system
time 37/tcp Time
time 37/udp Time
rap 38/tcp Route Access Protocol
rap 38/udp Route Access Protocol
nicname 43/tcp Who Is
login 49/tcp Login Host Protocol
xns-time 52/tcp XNS Time Protocol
dns 53/tcp Domain Name Server
sql*net 66/tcp Oracle SQL*NET
bootpc 68/udp Bootstrap Protocol Client
tftp 69/udp Trivial File Transfer
gopher 70/tcp Gopher

http 80/tcp World Wide Web HTTP
pop 110/tcp Mail abholen
nntp 119/tcp Network News Transfer Protocol
imap2 143/tcp Interactive Mail Access Protocol v2
https 443/tcp https MCom
microsoft-ds 445/udp Microsoft-DS
login 513/tcp remote login a la telnet
irc 6665-6669/tcp chatting

Exercise 1.3