Technische Universität Berlin

IPv4 I – Networking Basics

Training for Afghan System Administrators

Networking Basics

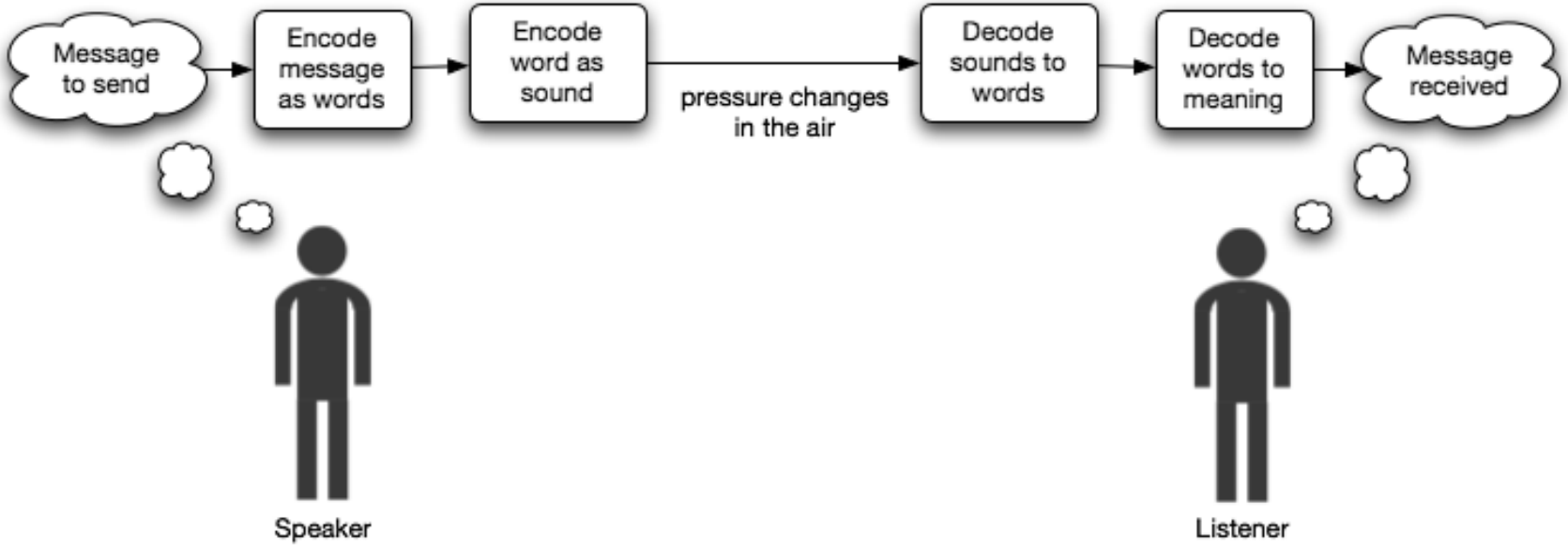
This is the simplified Ramadan version of the simplified introduction to TCP/IP Networking

Networking

The main reason why computers are so dominant in our life is that computers are able **to communicate with other computers**

Computers communicate with other computers within their homenetworks (Intranet) and computers outside,in the **Internet.**

Communication



The whole history of the Internet (in a nutshell)

The Internet was designed once somewhere as a decentralized, hardware independent network under the assumption that all its members are friends.

The 'language' of the Internet: TCP/IP

The Internet uses a whole family of protocols, called TCP/IP suite:

- HTTP, SMTP, IMAP,SSH,FTP…….
- TCP, UDP
- IP,ARP
- Ethernet, Token Ring, FDDI, PPP, PPPoE

Protocol(s) Example: Sending a letter

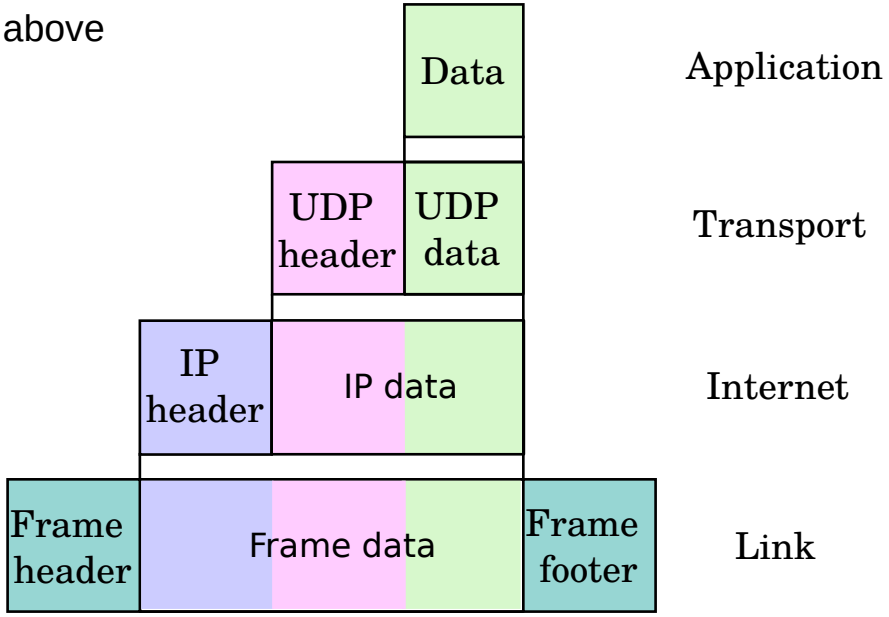
1. Write the letter
2. Put the letter in an envelope
3. Write receiver's address and return address on the envelope
4. Glue an official stamp on the envelope
5. Put the envelope in a letter box

Note: This protocol says nothing about driving a car or flying a plane.

Encapsulation: TCP/IP Protocol Stack

Idea:

- The family of TCP/IP Protocols is organized in four different hierarchical layers, a more efficient and less strict implementation of the 7 layer ISO/OSI model
- Each layer provides transportation for the layer above
- Each layer has its own functionality



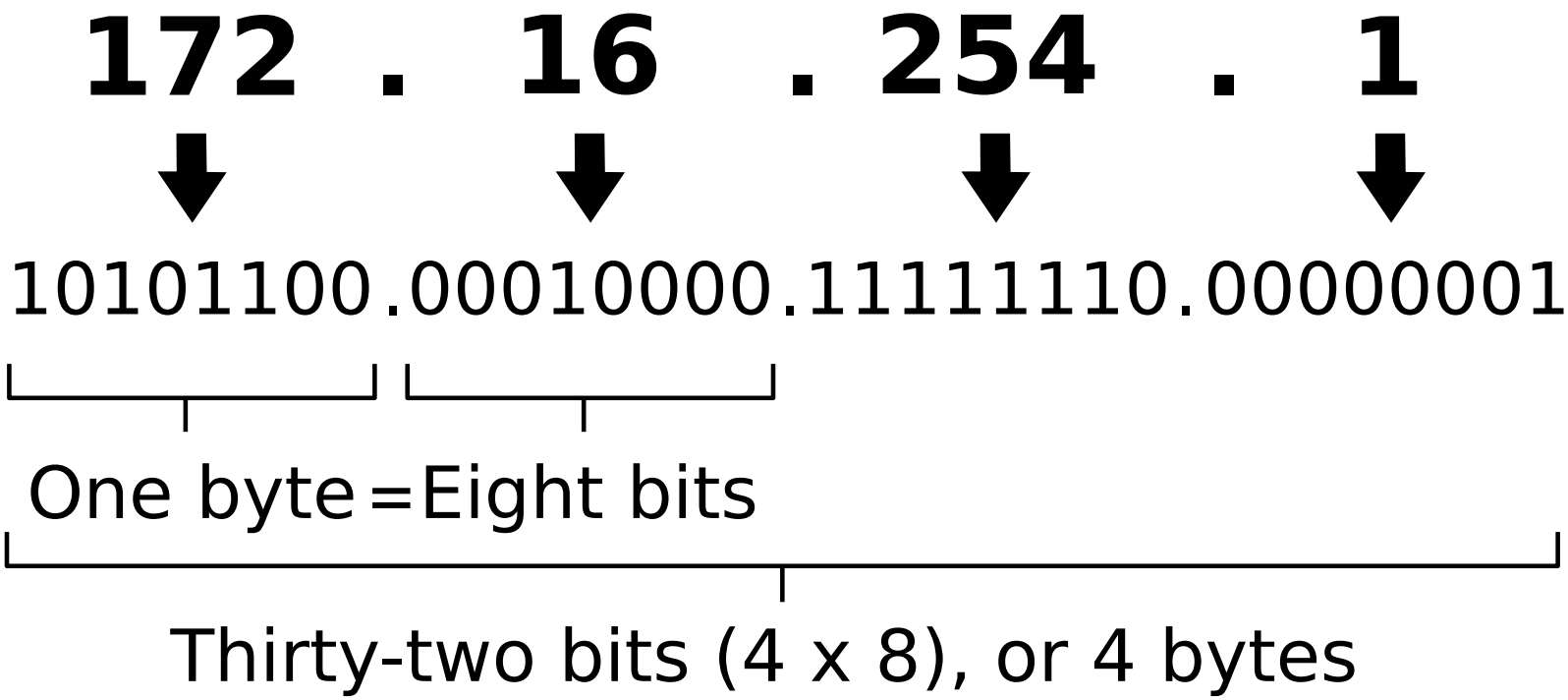
Addressing

Today's focus will be on the link and internet layer. We take a closer look to:

- IP Address

- MAC Address

IP(v4) Address



Technische Universität Berlin

History: Class A,B,C Networks

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

ZIIK

CIDR

- Today any number of bits can be assigned to be network bits
- Human reading friendly notation is /# of networkbit
- We will use standard class a (x.x.x.x/8) or class b (x.x.x.x/16) or class c (x.x.x.x/24) for simplicity

IP Range of ZiiK Subnet

The ZiiK Subnet has the Address **130.149.240.128/26**

What is the IP Range?

How many Computers can be addressed?

Please **do use** some CIDR Calculator!
E.g.: **www.subnet-calculator.com**

Special IP Addresses

- The smallest addr. of a network is the network address (e.g. 192.168.0.0)
- The largest is the networks broadcast address (e.g.) 192.168.0.255)
- 0.0.0.0 meta address (invalid, unknown, all, rest-of)
- 10.0.0.0/8 private class a network
- 127.0.0.0/8 loopback device (own computer)
- 169.254.0.0/16 link-local,
- 172.16.0.0/12 16x private class b network
- 192.168.0.0/16 256x private class c network

IP Configuration

Can be done manually:

- ip addr , ip route
- ifconfig, route
- Edit configuration file
- Network-Manager

Can be done by a service:

- dhcp

DNS Service

Even human read-friendly IP addresses are hard to remember:

DNS Servers offer to address IP addresses by names, like www.yahoo.com

MAC (hardware) address

Unique identifier of 6 bytes (or 48 bits):

000000000000000001101100010001011111111100010111

The human reading-friendly standard is 6 groups of 2 hex digits:

00:00:36:22:ff:17

- ships with the network device
- first 3 bytes identify the vendor, last 3 bytes the device
- Who has assigned the MAC address above?

MAC (hardware) address

It is possible to not use the vendor assigned address. The MAC address can be changed with (**do not** do it):

- ip link
- Ifconfig
- macchanger

Possible reasons to do so:

- Avoiding identification and criminal prosecution
- Circumventing “Accessprotection” (WLAN Routers)
- Both things are not polite things to do

ARP – Mapping IP to MAC Address

A computer gets the corresponding MAC for an IP by broadcasting an ARP request:

- Computer broadcasts his IP and MAC Address and the IP Address for the target
- Target sends his IP and MAC Address to the requesting computer
- Because it is not practical to do this every time, a computer stores ARP replies in the **ARP Cache**

Take a look at your computers ARP cache:
you@yours ~ $ ip neighbor show or

you@yours ~ $ arp -n then

you@yours ~ $ sudo wireshark look if you see any ARP requests

Routing

- On the link layer (e.g. ethernet), only computers in the same physical network can be addressed.
- Communication with other computers has to be relayed by other computers connected to another network as well
- Through a cascade of connected networks, communication will finally reach the target computer
- This process is called **routing**
- The relaying computers are called **routers**

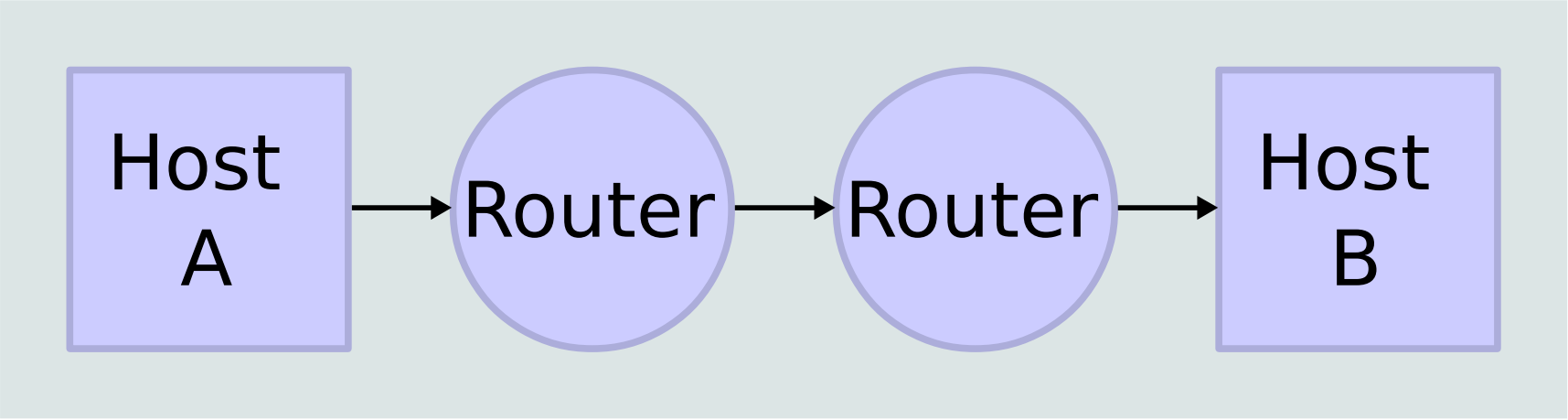
Routing

- The list of routers that will relay communication into other networks is called routing table
- Take a look at your routing table:

you@yours ~$ ip route show

you@yours ~ $ route -n

Network Topology https://en.wikipedia.org/wiki/File:IP_stack_connections.svg



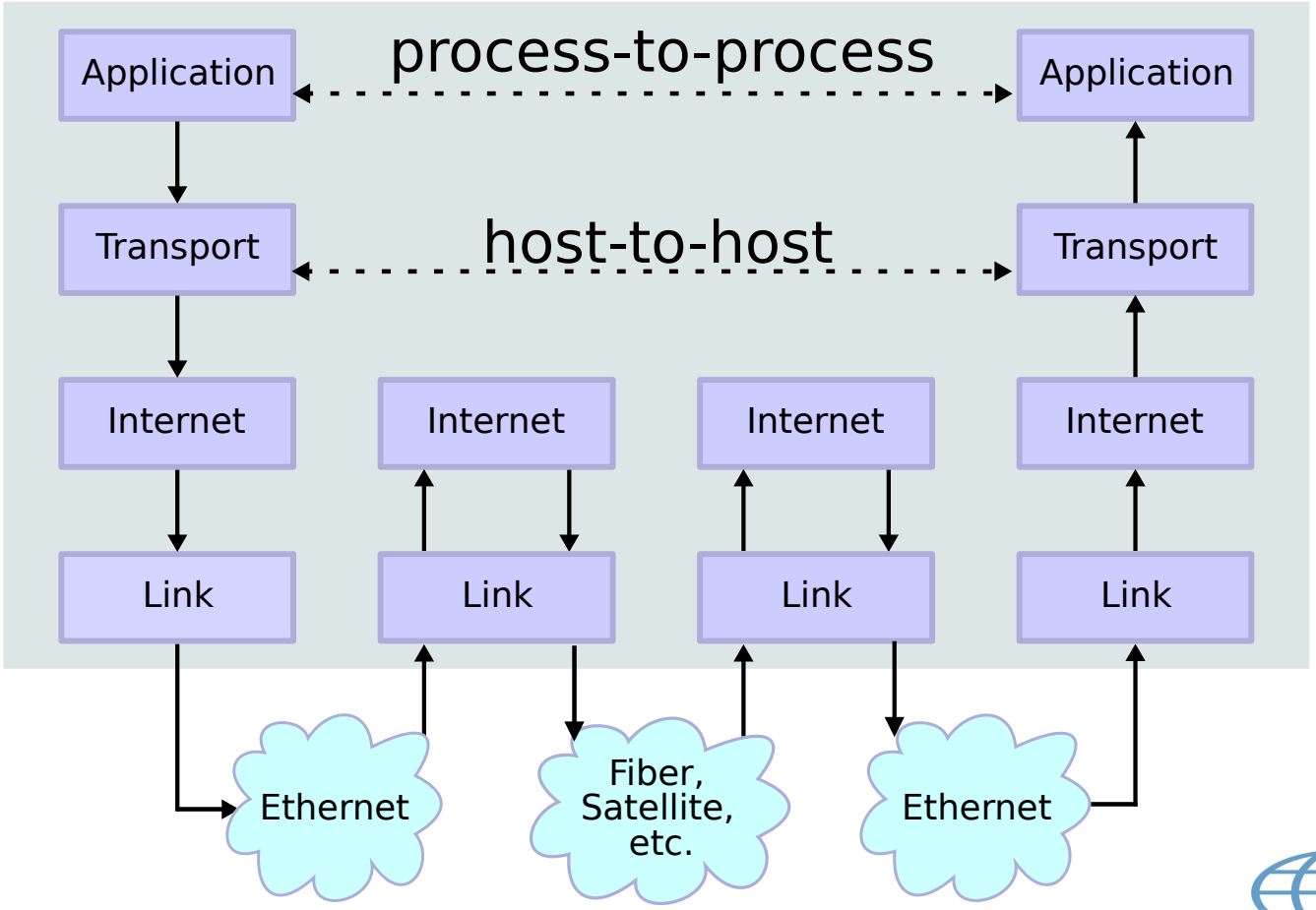
Check some routes, e.g. to google.com:

you@yours ~ $ traceroute google.com

me@mine ~ $ traceroute google.com

```
traceroute to google.com (173.194.32.225), 30 hops max, 60 byte packets
 1  sn-240128.gate.tu-berlin.de (130.149.240.129)  0.603 ms  0.646 ms  0.695 ms
 2  e-n-a.gate.tu-berlin.de (130.149.126.61)  0.569 ms  0.628 ms  0.693 ms
 3  cr-tub1-te0-0-0-15.x-win.dfn.de (188.1.235.117)  0.669 ms  0.738 ms  0.772 ms
 4  google.bcix.de (193.178.185.100)  0.971 ms  0.971 ms  0.961 ms
 5  209.85.249.184 (209.85.249.184)  7.483 ms  7.420 ms  7.440 ms
 6  72.14.232.27 (72.14.232.27)  7.969 ms  7.894 ms  7.938 ms
 7  ber01s09-in-f1.1e100.net (173.194.32.225)  7.689 ms  7.698 ms  7.638 ms
```

Data Flow Chart https://en.wikipedia.org/wiki/File:IP_stack_connections.svg



You should be able to do this now:

- Find out where a connection is broken (in the internet / link layer)
- Circumvent MAC address “protection” based access controls