Computer Networks Lab

Introduction and Fundamentals
Winter Term 2019

Prof. Dr. Christian Baun
Henry-Norbert Cocos
Maurizio Petrozziello
{christianbaun,cocos,petrozziello}@fb2.fra-uas.de

Computer Science
Faculty of Computer Science and Engineering
Frankfurt University of Applied Sciences

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Inhalt

1. Introduction
2. Command-line tools for networking
3. Basic networking technologies
4. Wireshark
5. References

Introduction

This slide set covers the following topics:

- **Linux Command-line tools for networking**
- **Basics on networks**
- **Basics on Wireshark**

After this introductory slide set you should be able to solve the Lab Exercise Sheet 1!

Linux Command-Line tools

Linux offers some useful Command-line tools for networking

The following list shows some of the most common tools

- `ping` used to send ICMP-Requests to an IP-Address or a domain [1]
- `traceroute` used to list the routers that forward an IP-Packet to the destination [2]
- `dhclient` used to configure the DHCP on an interface [3]
- `lynx` a textbased webbrowser [4]
- `iptables` used to set up rules for a firewall [5]

ping

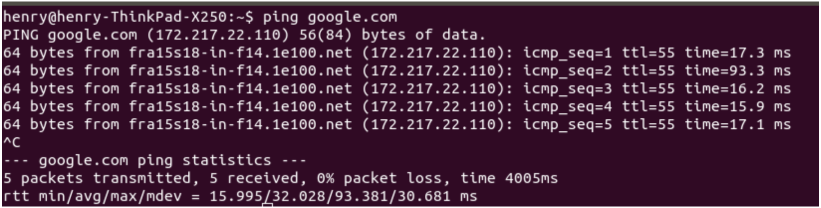
ping is a useful command tool for...

- checking the reachability of a server
- sending and receiving ICMP packets
- checking transmission information (time-to-live, response time, round-trip-time)

ping command-line tool

ping is the most essential tool for network administrators and is the first tool to use when analyzing a network!

ping



```
henry@henry-ThinkPad-X250:~$ ping google.com
PING google.com (172.217.22.110) 56(84) bytes of data.
64 bytes from fra15s18-in-f14.1e100.net (172.217.22.110): icmp_seq=1 ttl=55 time=17.3 ms
64 bytes from fra15s18-in-f14.1e100.net (172.217.22.110): icmp_seq=2 ttl=55 time=93.3 ms
64 bytes from fra15s18-in-f14.1e100.net (172.217.22.110): icmp_seq=3 ttl=55 time=16.2 ms
64 bytes from fra15s18-in-f14.1e100.net (172.217.22.110): icmp_seq=4 ttl=55 time=15.9 ms
64 bytes from fra15s18-in-f14.1e100.net (172.217.22.110): icmp_seq=5 ttl=55 time=17.1 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 15.995/32.028/93.381/30.681 ms
```

Figure: Output of `ping` command for www.google.com

traceroute

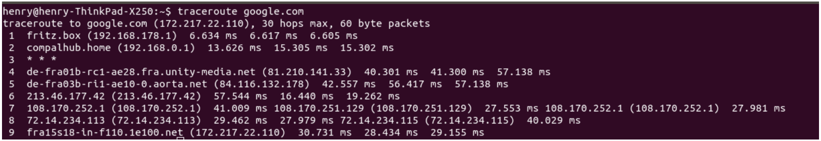
traceroute is a useful command tool for...

- checking the number and IP-Addresses of Servers between sender and receiver
- checking the time consumption for every hop and for the transmission
- sending and receiving ICMP packets

traceroute command-line tool

traceroute is used to identify delays in the connection between sender and receiver. By using traceroute the response time of routers between sender and receiver can be analyzed.

traceroute



```
henry@henry-ThinkPad-X250:~$ traceroute google.com
traceroute to google.com (172.217.22.110), 30 hops max, 60 byte packets
 1  fritz.box (192.168.178.1)  6.634 ms  6.617 ms  6.605 ms
 2  compalhub.home (192.168.0.1)  13.626 ms  15.305 ms  15.302 ms
 3  * * *
 4  de-fra01b-rc1-ae28.fra.unity-media.net (81.210.141.33)  40.301 ms  41.300 ms  57.138 ms
 5  de-fra03b-ri1-ae10-0.aorta.net (84.116.132.178)  42.557 ms  56.417 ms  57.138 ms
 6  213.46.177.42 (213.46.177.42)  57.544 ms  16.440 ms  19.262 ms
 7  108.170.252.1 (108.170.252.1)  41.009 ms 108.170.251.129 (108.170.251.129)  27.553 ms 108.170.252.1 (108.170.252.1)  27.981 ms
 8  72.14.234.113 (72.14.234.113)  29.462 ms  27.979 ms 72.14.234.115 (72.14.234.115)  40.029 ms
 9  fra15s18-in-f110.1e100.net (172.217.22.110)  30.731 ms  28.434 ms  29.155 ms
```

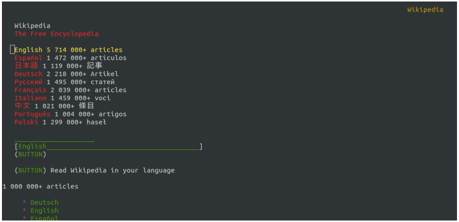
Figure: Output of traceroute command for www.google.com

lynx webbrowser

lynx webbrowser is...

- one of the oldest webbrowsers
- a textbased webbrowser for static websites
- is used for screenreaders and braille terminals

lynx webbrowser



```
                                                                    Wikipedia

  Wikipedia
  The Free Encyclopedia

  English 5 714 000+ articles
  Español 1 472 000+ artículos
  日本語 1 119 000+ 記事
  Deutsch 2 218 000+ Artikel
  Русский 1 495 000+ статей
  Français 2 039 000+ articles
  Italiano 1 459 000+ voci
  中文 1 021 000+條目
  Português 1 004 000+ artigos
  Polski 1 299 000+ haseł


  ____________________
  [English______________________________________]
  (BUTTON)

  (BUTTON) Read Wikipedia in your language

1 000 000+ articles

     * Deutsch
     * English
     * Español
```

Figure: lynx webbrowser on the command-line for www.wikipedia.org

Figure: A braille terminal for blind persons

Image Source:

https://de.wikipedia.org/wiki/Braillezeile

Basic network technologies

This section will cover...

- some basic network technologies
- some basic network protocols

Only some basics!

However this section only covers some fundamental technologies necessary for understanding the Lab exercises.

More details!

A more detailed view on the technologies is presented in the lectures!

ICMP

The Internet Control Message Protocol (ICMP) is used to exchange diagnosis information inside a network

Here is a list of some important message types [1]:

0	Echo Reply
3	Destination Unreachable
8	Echo Request
11	Time Exceeded
30	Traceroute

`ping` command-line tool

The command-line tool `ping` uses ICMP-Requests to check the reachability of a machine. If the machine is reachable and supports the ICMP protocol it answers with an ICMP-Reply.

[1] The message type is specified by the code inside the header field

ICMP

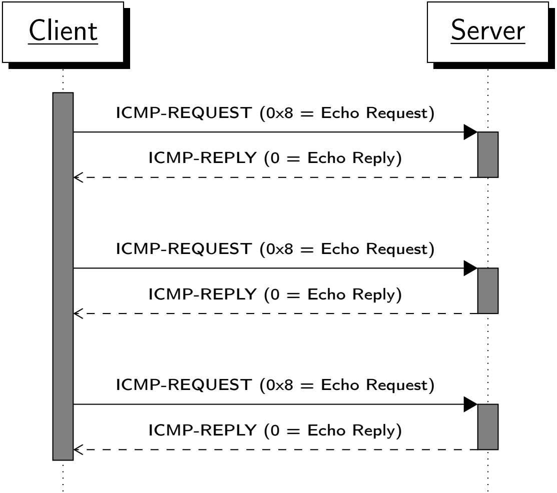

Client
Server
ICMP-REQUEST (0x8 = Echo Request)
ICMP-REPLY (0 = Echo Reply)
ICMP-REQUEST (0x8 = Echo Request)
ICMP-REPLY (0 = Echo Reply)
ICMP-REQUEST (0x8 = Echo Request)
ICMP-REPLY (0 = Echo Reply)

Figure: Message Sequence Diagram (MSC) `ping`

DHCP

The Dynamic Host Control Protocol (DHCP) is used to control the assignement of IP-Adresses

The assignment of IP-Addresses and network configurations is managed by a DHCP-Server

The DHCP-Server in a private network is usually the Router/Gateway

DHCP vs bootp

The Bootstrap Protocol (bootp) is the core protocol for dynamically assigning IP-Addresses, netmasks, and gateways. However in large private networks additional information is needed. Therefore DHCP was invented which is an extension of the Bootstrap Protocol. The flow of bootp is shown in the next slide.

DHCP

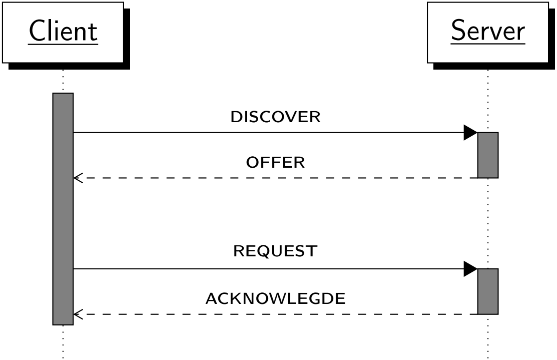


Figure: MSC for IP-Address renewal using DHCP

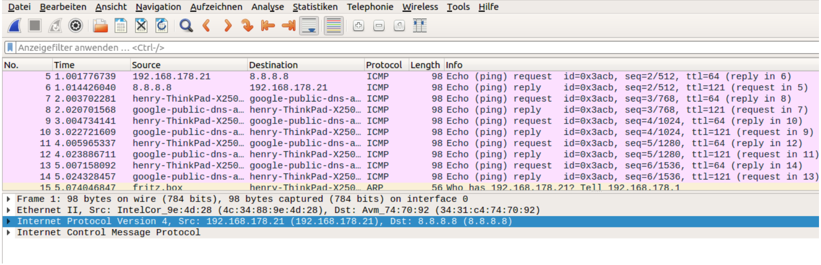
Wireshark

Wireshark is an open-source tool for network analysis

Wireshark features the following functions:

- Graphical user interface
- Collection of transmited data
- Detailed view of each packet and protocol
- Enables a detailed analysis of network traffic

Wireshark



Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
Anzeigefilter anwenden … <Ctrl-/>

```
No.     Time         Source               Destination          Protocol Length Info
      5 1.001776739  192.168.178.21       8.8.8.8              ICMP       98 Echo (ping) request  id=0x3acb, seq=2/512, ttl=64 (reply in 6)
      6 1.014426040  8.8.8.8              192.168.178.21       ICMP       98 Echo (ping) reply    id=0x3acb, seq=2/512, ttl=121 (request in 5)
      7 2.003702281  henry-ThinkPad-X250… google-public-dns-a… ICMP       98 Echo (ping) request  id=0x3acb, seq=3/768, ttl=64 (reply in 8)
      8 2.020701568  google-public-dns-a… henry-ThinkPad-X250… ICMP       98 Echo (ping) reply    id=0x3acb, seq=3/768, ttl=121 (request in 7)
      9 3.004734141  henry-ThinkPad-X250… google-public-dns-a… ICMP       98 Echo (ping) request  id=0x3acb, seq=4/1024, ttl=64 (reply in 10)
     10 3.022721609  google-public-dns-a… henry-ThinkPad-X250… ICMP       98 Echo (ping) reply    id=0x3acb, seq=4/1024, ttl=121 (request in 9)
     11 4.005965337  henry-ThinkPad-X250… google-public-dns-a… ICMP       98 Echo (ping) request  id=0x3acb, seq=5/1280, ttl=64 (reply in 12)
     12 4.023886711  google-public-dns-a… henry-ThinkPad-X250… ICMP       98 Echo (ping) reply    id=0x3acb, seq=5/1280, ttl=121 (request in 11)
     13 5.007158092  henry-ThinkPad-X250… google-public-dns-a… ICMP       98 Echo (ping) request  id=0x3acb, seq=6/1536, ttl=64 (reply in 14)
     14 5.024328457  google-public-dns-a… henry-ThinkPad-X250… ICMP       98 Echo (ping) reply    id=0x3acb, seq=6/1536, ttl=121 (request in 13)
     15 5.074046847  fritz.box            henry-ThinkPad-X250… ARP        56 Who has 192.168.178.21? Tell 192.168.178.1
```

```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: IntelCor_9e:4d:28 (4c:34:88:9e:4d:28), Dst: Avm_74:70:92 (34:31:c4:74:70:92)
▸ Internet Protocol Version 4, Src: 192.168.178.21 (192.168.178.21), Dst: 8.8.8.8 (8.8.8.8)
▸ Internet Control Message Protocol
```

Figure: Wireshark Desktop

Wireshark Installation

Perform the following steps in order to install Wireshark [6]:

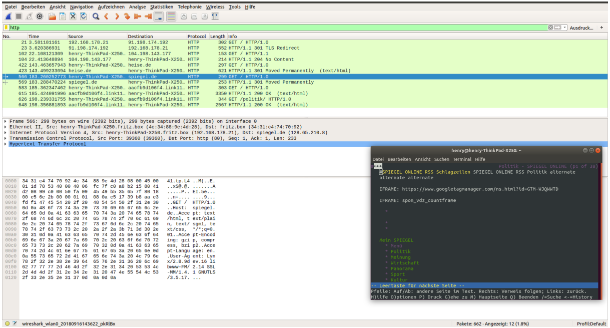
1. download and install the package:
   - `sudo apt-get install wireshark`
2. enable access to interfaces without root privileges and add Wireshark to user group:
   - `sudo dpkg-reconfigure wireshark-common`
   - `sudo adduser $USER wireshark`
3. log out user and afterwards log in to save changes
4. use Wireshark for network analysis

Adding Wireshark to User Group

The commands presented in step 2 are necessary in order to use Wireshark. Otherwise Wireshark has to be used with root privileges, which is considered a security hazard!

An Example on Using Wireshark

The picture shows Wireshark collecting data for a HTTP-connection using `lynx` to access `www.heise.de`.


Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
http
Ausdruck…
+
Datei Bearbeiten Ansicht Suchen Terminal Hilfe

```
No.  Time          Source                  Destination             Protocol Length Info
  21 3.581181161   192.168.178.21          91.198.174.192          HTTP      302 GET / HTTP/1.0
  23 3.620386931   91.198.174.192          192.168.178.21          HTTP      552 HTTP/1.1 301 TLS Redirect
 102 22.108121309  henry-ThinkPad-X250…    104.198.143.177         HTTP      153 GET / HTTP/1.1
 104 22.413648894  104.198.143.177         henry-ThinkPad-X250…    HTTP      214 HTTP/1.1 204 No Content
 422 143.463657943 henry-ThinkPad-X250…    heise.de                HTTP      297 GET / HTTP/1.0
 423 143.499233094 heise.de                henry-ThinkPad-X250…    HTTP      621 HTTP/1.1 301 Moved Permanently  (text/html)
 566 183.260252773 henry-ThinkPad-X250…    spiegel.de              HTTP      299 GET / HTTP/1.0
 569 183.288470224 spiegel.de              henry-ThinkPad-X250…    HTTP      253 HTTP/1.1 301 Moved Permanently
 583 185.362347462 henry-ThinkPad-X250…    aacfb9d106f4.link11…    HTTP      303 GET / HTTP/1.0
 615 185.424091996 aacfb9d106f4.link11…    henry-ThinkPad-X250…    HTTP     3350 HTTP/1.1 200 OK  (text/html)
 626 198.239331755 henry-ThinkPad-X250…    aacfb9d106f4.link11…    HTTP      344 GET /politik/ HTTP/1.0
 648 198.356881893 aacfb9d106f4.link11…    henry-ThinkPad-X250…    HTTP     2567 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 566: 299 bytes on wire (2392 bits), 299 bytes captured (2392 bits) on interface 0
▸ Ethernet II, Src: henry-ThinkPad-X250.fritz.box (4c:34:88:9e:4d:28), Dst: fritz.box (34:31:c4:74:70:92)
▸ Internet Protocol Version 4, Src: henry-ThinkPad-X250.fritz.box (192.168.178.21), Dst: spiegel.de (128.65.210.8)
▸ Transmission Control Protocol, Src Port: 39360 (39360), Dst Port: http (80), Seq: 1, Ack: 1, Len: 233
▸ Hypertext Transfer Protocol
```

```
0000  34 31 c4 74 70 92 4c 34  88 9e 4d 28 08 00 45 00   41.tp.L4 ..M(..E.
0010  01 1d 78 53 40 00 40 06  fc 7f c0 a8 b2 15 80 41   ..xS@.@. .......A
0020  d2 08 99 c0 00 50 fa 09  45 49 b5 35 65 7f 80 18   .....P.. EI.5e...
0030  00 e5 6e 2b 00 00 01 01  08 0a c5 17 39 b8 aa e3   ..n+.... ....9...
0040  fd f1 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 30   ..GET /  HTTP/1.0
0050  0d 0a 48 6f 73 74 3a 20  73 70 69 65 67 65 6c 2e   ..Host:  spiegel.
0060  64 65 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   de..Acce pt: text
0070  2f 68 74 6d 6c 2c 20 74  65 78 74 2f 70 6c 61 69   /html, t ext/plai
0080  6e 2c 20 74 65 78 74 2f  73 67 6d 6c 2c 20 74 65   n, text/ sgml, te
0090  78 74 2f 63 73 73 2c 20  2a 2f 2a 3b 71 3d 30 2e   xt/css,  */*;q=0.
00a0  30 31 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   01..Acce pt-Encod
00b0  69 6e 67 3a 20 67 7a 69  70 2c 20 63 6f 6d 70 72   ing: gzi p, compr
00c0  65 73 73 2c 20 62 7a 69  70 32 0d 0a 41 63 63 65   ess, bzi p2..Acce
00d0  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 0d   pt-Langu age: en.
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4c 79 6e   .User-Ag ent: Lyn
00f0  78 2f 32 2e 38 2e 39 64  65 76 2e 31 36 20 6c 69   x/2.8.9d ev.16 li
0100  62 77 77 77 2d 46 4d 2f  32 2e 31 34 20 53 53 4c   bwww-FM/ 2.14 SSL
0110  2d 4d 4d 2f 31 2e 34 2e  31 20 47 4e 55 54 4c 53   -MM/1.4. 1 GNUTLS
0120  2f 33 2e 35 2e 31 37 0d  0a 0d 0a                  /3.5.17. ...
```

henry@henry-ThinkPad-X250: ~

```
#<<<                                      Politik - SPIEGEL ONLINE (p1 of 38)
  #SPIEGEL ONLINE RSS Schlagzeilen SPIEGEL ONLINE RSS Politik alternate
  alternate alternate

  IFRAME: https://www.googletagmanager.com/ns.html?id=GTM-WJQWWTD

  IFRAME: spon_vdz_countframe

    *


    *
    *

  Mein SPIEGEL
    * Menü
    * Politik
    * Meinung
    * Wirtschaft
    * Panorama
    * Sport
    * Kultur
-- Leertaste für nächste Seite --
Pfeile: Auf/Ab: andere Seite im Text. Rechts: Verweis folgen; Links: zurück.
H)ilfe O)ptionen P) Druck G)ehe zu M) Hauptseite Q) Beenden /=Suche <-=History
```

wireshark_wlan0_20180916143622_pkRlBx | Pakete: 662 · Angezeigt: 12 (1.8%) | Profil:Default

Figure: Data collected with Wireshark using `lynx`

More Information on Wireshark

More details on how to work with Wireshark can be found in [7, 8]!

Lab Exercise 1

This slide set gives a you brief overview of the tools and technologies discussed in Lab exercise sheet 1.

Hopefully this slide set gives you the abillity to solve the tasks of exercise sheet 1!

Lab Exercise 1

Have fun solving the Exercise Sheet and if you have questions, don't be afraid to ask ;-)

References I

[1] ping man page. [accessed: November 21, 2019]. [Online]. Available: https://linux.die.net/man/8/ping

[2] traceroute man page. [accessed: November 21, 2019]. [Online]. Available: https://linux.die.net/man/8/traceroute

[3] dhclient man page. [accessed: November 21, 2019]. [Online]. Available: https://linux.die.net/man/8/dhclient

[4] lynx man page. [accessed: November 21, 2019]. [Online]. Available: https://linux.die.net/man/1/lynx

[5] "iptables man page," [accessed: November 21, 2019]. [Online]. Available: https://linux.die.net/man/8/iptables

[6] "Wireshark – ubuntuusers," [accessed: November 21, 2019]. [Online]. Available: https://wiki.ubuntuusers.de/Wireshark/

References II

[7] “Quick and dirty wireshark tutorial,” [accessed: November 21, 2019]. [Online]. Available: https://www.computerweekly.com/tutorial/Quick-and-dirty-Wireshark-tutorial

[8] Wireshark.org, *Wireshark User’s Guide – Version 2.9.0*, [accessed: November 21, 2019]. [Online]. Available: https://www.wireshark.org/download/docs/user-guide.pdf