

Computer Networks Lab

Introduction and Fundamentals

Winter Term 2018

Henry-Norbert Cocos
cocos@stud.fra-uas.de
henry-norber@fb2.fra-uas.de

Computer Science
Faculty of Computer Science and Engineering
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 flrtz.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 fra15s10-tn-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
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 1 259 000+ hasła]

[English
(OUTGO)]

(OUTGO) Read Wikipedia in your language

1 000 000+ articles
- Deutsch
- English
- Français
  
```

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.

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

ICMP

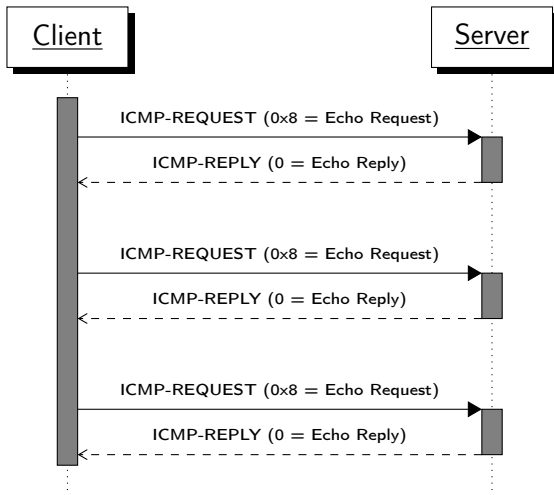


Figure: Message Sequence Diagram (MSC) ping

DHCP

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

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

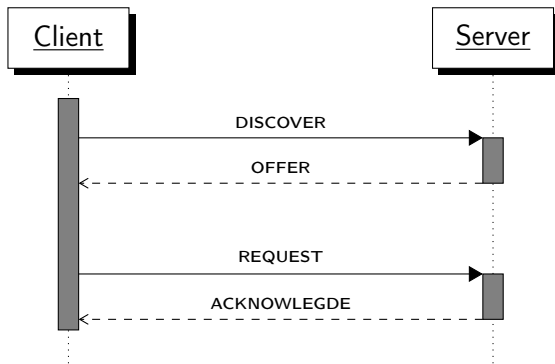


Figure: MSC for IP-Address renewal using DHCP

Wireshark

Wireshark is an open-source tool for network analysis

Wireshark features the following functions:

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

Wireshark

The screenshot shows the Wireshark desktop application. The menu bar includes: Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telefonie, Wireless, Tools, Hilfe. The toolbar contains various icons for file operations and network analysis. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 15) is an ARP request from fritz.box to henrv.ThinkPad-X256.

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	4.023806711	google-public-dns-a...	henry-ThinkPad-X250...	ICMP	98	Echo (ping) reply id=0x3acb, seq=5/1280, ttl=121 (request in 11)
13	5.007150092	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	henrv.ThinkPad-X256	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.

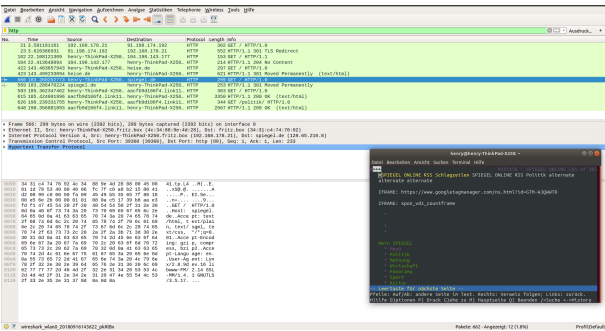


Figure: Data collected with Wireshark using lynx

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 ability 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 ;-)

- [1] ping man page. [accessed: October 29, 2018]. [Online]. Available: <https://linux.die.net/man/8/ping>
- [2] traceroute man page. [accessed: October 29, 2018]. [Online]. Available: <https://linux.die.net/man/8/traceroute>
- [3] dhclient man page. [accessed: October 29, 2018]. [Online]. Available: <https://linux.die.net/man/8/dhclient>
- [4] lynx man page. [accessed: October 29, 2018]. [Online]. Available: <https://linux.die.net/man/1/lynx>
- [5] “iptables man page,” [accessed: October 29, 2018]. [Online]. Available: <https://linux.die.net/man/8/iptables>
- [6] “Wireshark – ubuntuusers,” [accessed: October 29, 2018]. [Online]. Available: <https://wiki.ubuntuusers.de/Wireshark/>

- [7] “Quick and dirty wireshark tutorial,” [accessed: October 29, 2018]. [Online]. Available: <https://www.computerweekly.com/tutorial/Quick-and-dirty-Wireshark-tutorial>

- [8] Wireshark.org, *Wireshark User's Guide – Version 2.9.0*, [accessed: October 29, 2018]. [Online]. Available: <https://www.wireshark.org/download/docs/user-guide.pdf>