




Welcome to

The Newcomers' Guide to Networking: *Textbooks for the Next Generation*

RIPE86 Community Plenary

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, [kramse@Github](#) 
newcomers-guide-to-networking.tex in the repo security-courses

Problem statement

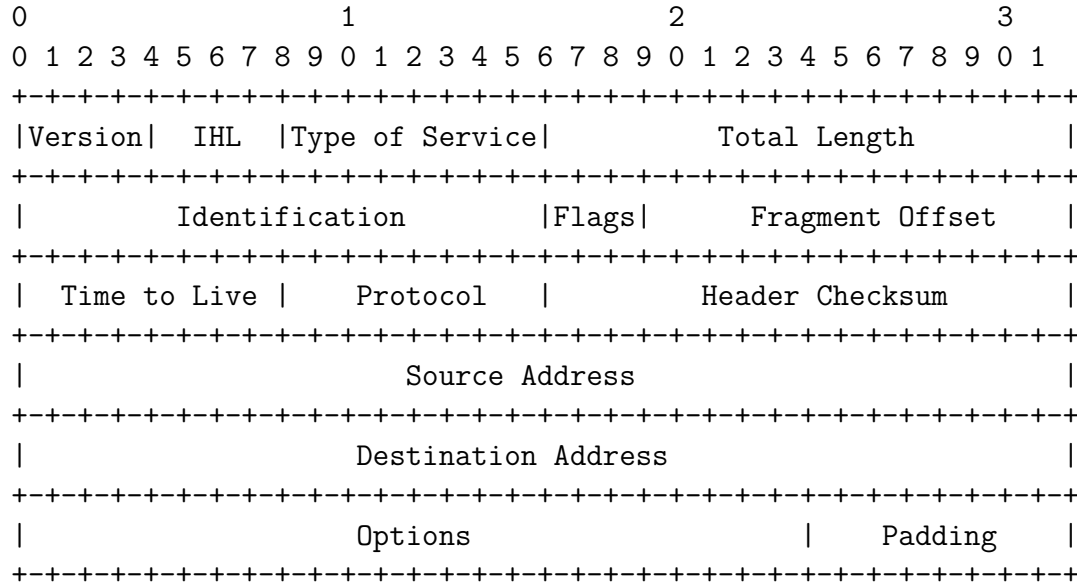


Your co-worker has a question: *You work in networking, so can you give me some pointers for my friend that wants to *get into networking*?!*

How can we **attract more newcomers** to our **networking communities**? I work in **education**, and I learnt about networking the **old school way** in the 1990s, with large **500 page textbooks**, and this is still sometimes the case. Can we **crowdsource interesting and useful sources of knowledge for the next generation**? Can we create a "**newcomers**' guide to networking"?

- A small call for resources, send me your best links, resources, books, papers, and interesting resources I will add them here =====> <https://github.com/kramse/learning-paths>
- May contain opinionated content, beware
- BTW *my slides are boring!*

First of all Thank you!



- Thank you to all the authors of the books I have learnt from. Thank you all that wrote RFCs, I enjoy them a lot
- Unfortunately they are not beginner friendly, if I was a newcomer today I would probably NOT read them
- Many resources are very structured, but become a bit boring, sorry

Prerequisite knowledge



Plan: You want to learn Port Scanning and Nmap!
Usefull in both defense and attack scenarios!

- Knowledge level: What is a port scanner
Need to know TCP/IP, IP address, ports and services – example HTTP 80/tcp, TCP session setup

So a newcomer should get this sorted out first, otherwise they cannot understand what Nmap does, and output returned

Skills are needed



```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-10-27 06:50 CET
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 06:50
Scanning 192.168.0.128 [1 port]
Completed ARP Ping Scan at 06:50, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:50
Completed Parallel DNS resolution of 1 host. at 06:50, 0.10s elapsed
Initiating SYN Stealth Scan at 06:50
Scanning 192.168.0.128 [1900 ports]
Discovered open port 3306/tcp on 192.168.0.128
Discovered open port 53/tcp on 192.168.0.128
Discovered open port 139/tcp on 192.168.0.128
Discovered open port 23/tcp on 192.168.0.128
Discovered open port 22/tcp on 192.168.0.128
```

- Skills level: Running a port scanner
Need to have operating system – luckily Nmap supports Mac, Windows, Linux, ...
- My recommendation: create a virtual machine with Kali Linux
BTW ... what is a Virtual Machine?! And so it keeps on

Small set of Recommended networking technologies to learn



So to accomplish the goal of using Nmap efficiently you need some basics

Networking: Basic Protocols from the Internet Protocols suite IP/TCP, or TCP/IP

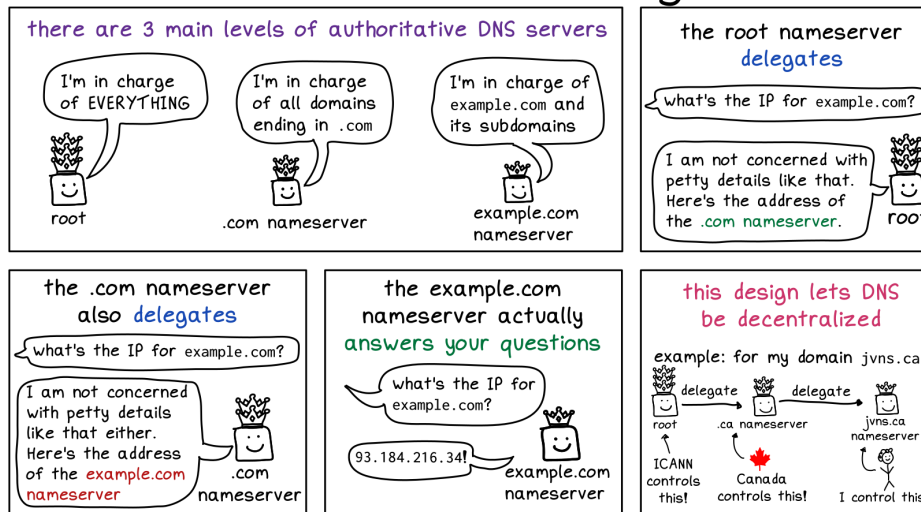
- Network Layer: Ethernet, Address Resolution Protocol (ARP), IPv4 and ICMP
Later add Wi-Fi and IPv6
- Transport Layer: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
- Common upper layer: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP)
Later add the encrypted/secure versions like Hypertext Transfer Protocol Secure (HTTPS) which uses Transport Layer Security (TLS)

Enough to be able to go to other resources, and a connected path from ARP to TLS

What am I looking for – easier entry ways into networking



the DNS hierarchy



Source: *The DNS hierarchy* by Julia Evans

<https://wizardzines.com/zines/dns/samples/1-dns-hierarchy.png> ❤️

Tools that help present real world data



zone	server	port	recursion	query type	protocol	dnssec	
kramse.dk	8.8.8.8	53	true	A	udp	true	digish

Answer

```
<> DiGiSH <> kramse.dk
;; global options: +cmd
;; Got answer:
;; ->HEADER<< opcode: QUERY, status: NOERROR, id: 48718
;; flags: qr aa tc rd ra z ad cd; QUERY:1, ANSWER:2, AUTHORITY:0, ADDITIONAL:1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
kramse.dk.                IN      A
;; ANSWER SECTION:
kramse.dk.                21600  IN      A      185.129.60.130
kramse.dk.                21600  IN      RRSIG  A 13 2 43200
1682669561 1685088761 4046 kramse.dk. 4ZVGmeGEN3I00FsdL9SFAj99vF5sCWsUja8GBcQnwUpKx+
f41211VdUgoy93R8aeGxuC9CVQE+j9mLoKMY8AQ==
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
.                        32768  IN      OPT
;; Query time: 1197 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun May 21 15:40:42 CET 2023
;; MSG SIZE rcvd: 179
```

Tip!

Copy and paste this line into your terminal

```
dig @8.8.8.8 -p 53 A kramse.dk
```

Info section

dig is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. Other lookup tools tend to have less functionality than dig.

digish is not dig.

- at the DNS hackathon I saw this cool tool, EduDIG <https://edudig.se/> ❤️

Books that are fun and educational



The Map of the Internet

The internet isn't actually one big, unified network. Instead, it's a network made out of tens of thousands of smaller networks called **autonomous systems (AS)** belonging to universities, internet service providers (ISPs), or telecommunications companies.

An internet user is always part of one such autonomous system.

Autonomous systems are so named because they're administered independently from each other.

When these networks interconnect, they constitute the internet as we know it. There are currently about 94,000 such ASs.

If the internet is a map of the world, ASs are like villages, cities, or countries on the map. They're relatively well interconnected, in ways similar to street networks. Some routes on the map are bigger and therefore faster to travel on; other routes require you to pay to use them.

28 Chapter 4

Border Gateway Protocol (BGP)

The protocol that makes this interconnection possible is the **Border Gateway Protocol (BGP)**, the de facto routing standard on the internet.

BGP defines how information about IP packet routes are exchanged between ASs throughout the internet, making it possible to calculate the shortest and cheapest possible path from one place to the next, ultimately reaching the packet's destination.

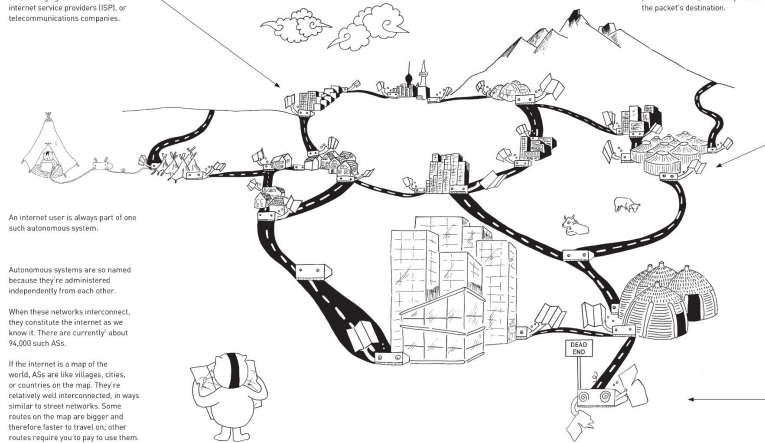
With BGP, each AS controls its own map of the internet and references routes and distances to other networks from its own point of view. Very few BGP servers have a complete global map of all possible routes through the internet.

An AS is made up of many computers connected to each other through routers. Routers that act as entry and exit points of the whole AS are called **BGP routers**.

The BGP routers of different ASs talk to one another regularly, and when they initiate a talk, known as a session, they become neighbors. Whenever neighbors meet to talk, they exchange maps of all routes they know about and want to share. An AS uses BGP to keep track of routes in a table and calculates their priorities based on various attributes. BGP tends to favor an AS's own map relative to its own point of view, because an extra hop to a neighbor makes the path longer.

This system is very clever, but as you can guess, it's also quite prone to mistakes. For example, if a neighbor shares the wrong map, or pretends to know how to get from one place to another when it actually doesn't, this can create an impasse or traffic congestion.

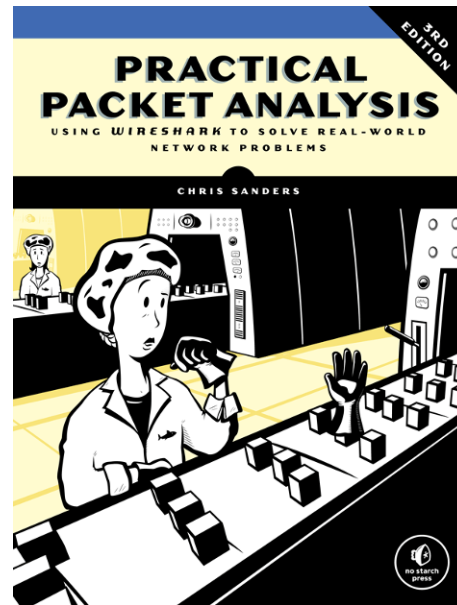
How Does Information Travel on the Internet? 29



Source: *How the Internet Really Works An Illustrated Guide to protocols, privacy, censorship, and governance* by catnip19

<https://catnip.article19.org/>

Real books are also welcome



- *Practical Packet Analysis - Using Wireshark to Solve Real-World Network Problems*, 3rd edition 2017, 368 pp
Chris Sanders ISBN: 9781593278021

Send me your best resources for newcomers



- Send your best links and resources to me h1k@kramse.org
- I will collect it and probably make an *awesome list* – there are awesome lists for just about any topic on Github
- Github repo added <https://github.com/kramse/learning-paths> – pull requests welcome

I am also very happy to discuss learning with you in breaks, I am here until friday.