Welcome to

Networking, TCP/IP and Security for Beginners

PROSA Nov 2024

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

Slides are available as PDF, kramse@Codeberg

basic-tcpip-and-security.tex in the repo security-courses

Contact information

- Henrik Kramselund, he/him internet samurai mostly networks and infosec
- Network and security consultant Zencurity, teach at KEA and activist
- Master from the Computer Science Department at the University of Copenhagen (DIKU)
- Email: hlk@zencurity.com Mobile: +45 2026 6000
- Run a small network for fun AS57860

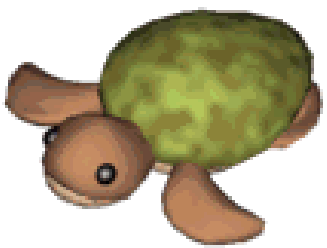
You are welcome to drop me an email

Goals for today

- Introduce basic TCP/IP terminology
- Show various network configurations with common protocols
- Describe how you can connect a router or switch to the network
- Describe basics of TCP/IP in 30 minutes
- Let you get some hands on with IP protocols

Photo is NWWC camp at BornHack 2024, next year 16-23rd of July 2025

Time schedule



- 17:00 - 18:15 Introduction and basics – with my network
- 18:45 - 21:00 Connect to the network, play with TCP/IP, switches and routers. Mix of presentation and exercises

Note: even though I talk a lot about Unix and Linux, you can definitely run a lot of tools on Windows and Mac OS X. The basic tools are available like the built-in ones and Nmap. Command line tools are sometimes used in the slides, as they only show text where a GUI screenshot can be cluttered with a lot of information, feel free to find GUI tools and web sites with same functionality

Exercises are completely optional

We will use a combination of your systems, my networking hardware and my systems.

There might be live sniffing done on traffic!
Don't abuse information gathered if you sniff data

We try to mimic what you would do in your own networks during the exercises.

- Try ping and traceroute
- See your own IP settings
- Borrow a USB Ethernet and connect to a switch or router
- Borrow a router

Linux is a toolbox I will use and participants are recommended to research virtual machines

Course Materials

- This material is in multiple parts:
- Slide show - presentation - this file
- Exercises - PDF which is used for this and other workshops
- Additional resources from the internet are linked throughout
- Wikipedia has a LOT of nice pages about IP protocols, for example:

> Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. The protocol is widely used in applications such as email, instant messaging, and voice over IP, but its use in securing HTTPS remains the most publicly visible.

Source: https://en.wikipedia.org/wiki/Transport_Layer_Security

Prerequisites

If you are interested in TCP/IP you are welcome

If you want to be an expert in IP and network security I recommend doing exercises

It is recommended to use virtual machines for the exercises

Network security and most internet related security work has the following requirements:

- Network experience
- TCP/IP principles - often in more detail than a common user
- Programming is an advantage, for automating things
- Some Linux and Unix knowledge is in my opinion a **necessary skill** for infosec work
  – too many new tools to ignore, and lots found at sites like Github and Open Source written for Linux

Wifi Hardware

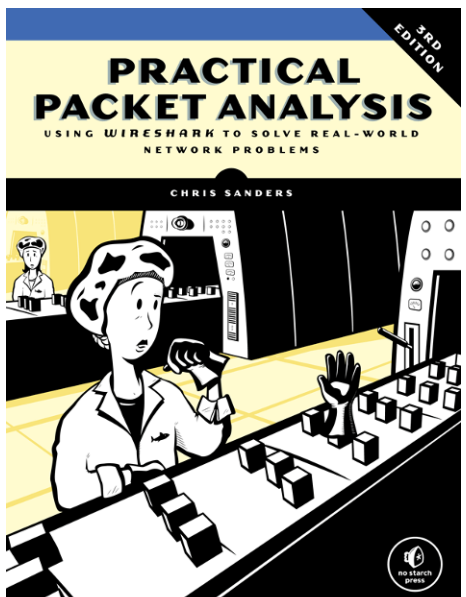
If you want to do sniffing of wireless it will be an advantage to have a wireless USB network card. Make sure to play nice, and dont abuse knowledge!

- The following are two recommended models:
- TP-link TL-WN722N hardware version 2.0 cheap but only support 2.4GHz
- Alfa AWUS036ACH 2.4GHz + 5GHz Dual-Band and high performing
- Both work great in Kali Linux for our purposes, but are older models by now

Unfortunately the vendors change models often enough that the above are hard to find. I recommend using your favourite search engine and research which cards work with Kali Linux and airodump-ng.

I have some available you can borrow

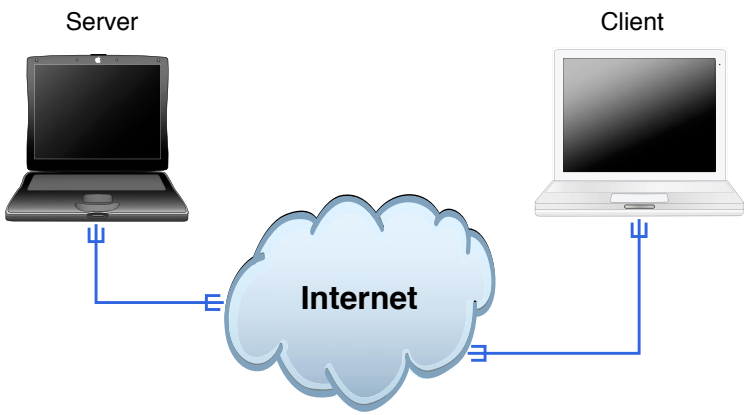
Book: Practical Packet Analysis (PPA)



Practical Packet Analysis, Using Wireshark to Solve Real-World Network Problems by Chris Sanders, 3rd Edition April 2017, 368 pp. ISBN-13: 978-1-59327-802-1 https://nostarch.com/packetanalysis3

I recommend this book for people new to networking, it has been in HumbleBundle book bundles multiple times

Internet Today



Clients and servers, roots in the academic world

Protocols are old, some more than 20 years

Very few protocols where encrypted, today a lot has switched to HTTPS and TLS

Internet is Open Standards!

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments (RFC) – a series of documents spanning decades

RFC, BCP, FYI, informational – first ones from 1969!

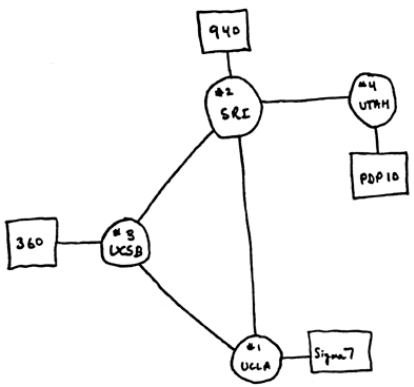
Are not updated but status is changed to Obsoleted when new versions are published

Standards track:
Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard

Internetworking: history

1961 L. Kleinrock, MIT packet-switching theory
1962 J. C. R. Licklider, MIT - notes
1964 Paul Baran: On Distributed Communications
1969 ARPANET 4 nodes
1971 14 nodes
1973 Design of Internet Protocols started
1973 Email is about 75% of all ARPANET traffic
1974 TCP/IP: Cerf/Kahn: A protocol for Packet Network Interconnection
1983 EUUG $\rightarrow$ DKUUG/DIKU Denmark
1988 About 60.000 systems on the internet - The Morris Worm hits about 10%
2002 About 130 million Internet hosts
2010 IANA reserved blocks 7% (Maj 2010) - http://www.potaroo.net/tools/ipv4/

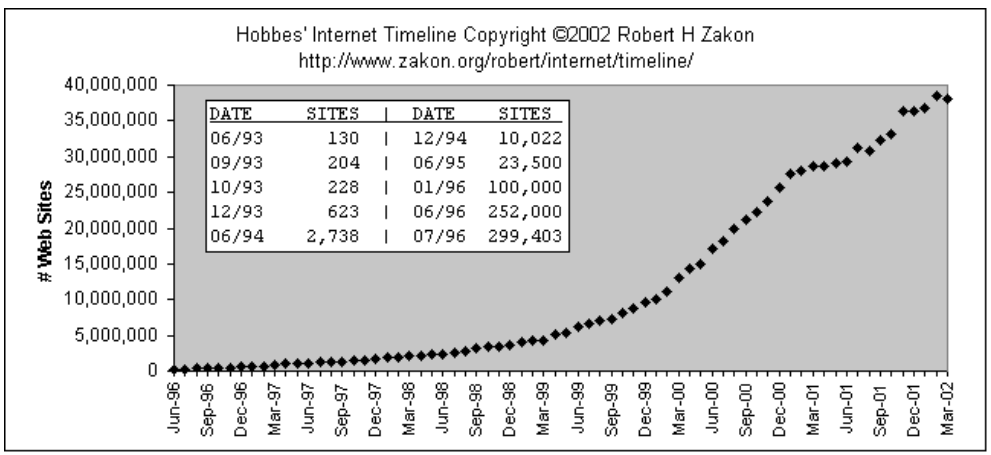
Internet historically set - anno 1969



- Node 1: University of California Los Angeles
- Node 2: Stanford Research Institute
- Node 3: University of California Santa Barbara
- Node 4: University of Utah

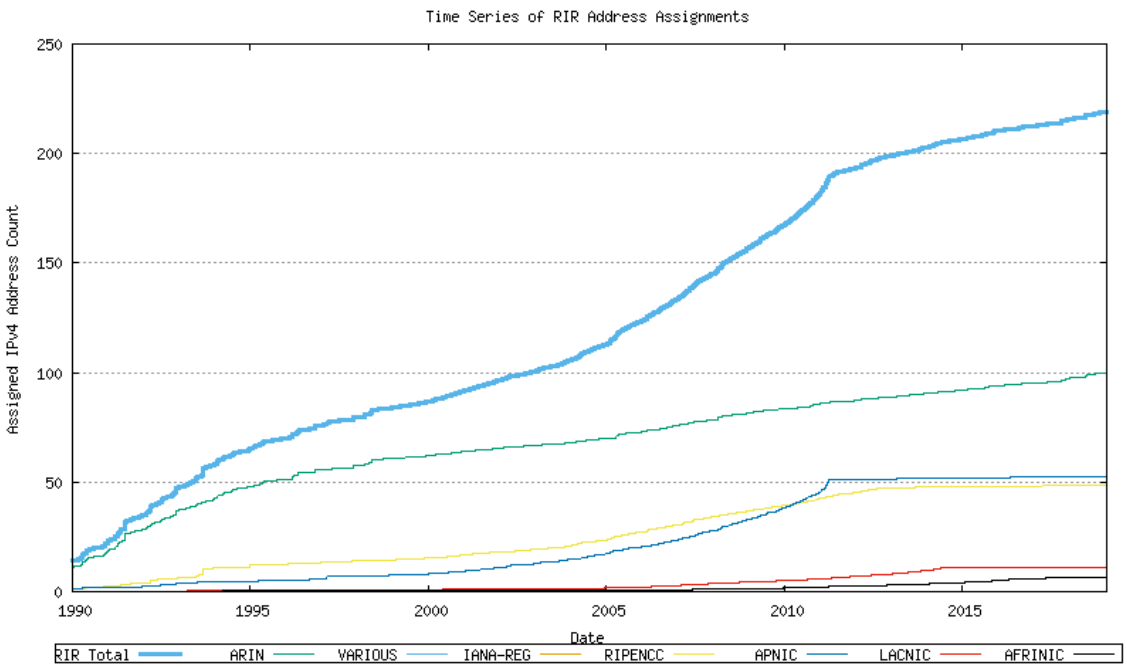
What are Internet hosts

World Wide Web servers



Source: Hobbes' Internet Timeline v5.6 http://www.zakon.org/robert/internet/timeline/

What are Internet hosts



Cumulative RIR address assignments, per RIR

Source: IPv4 Address Report http://www.potaroo.net/tools/ipv4/

What is the Internet

Communication between humans - currently!

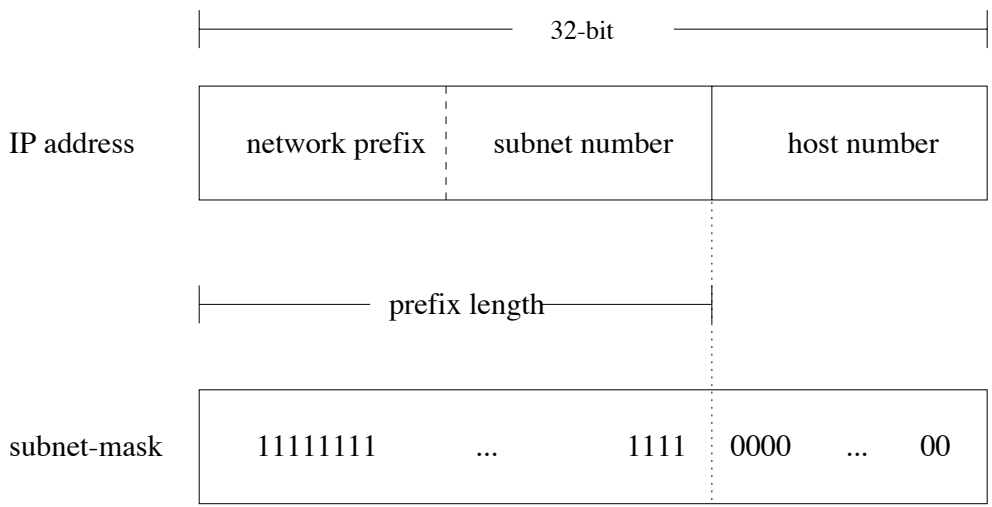
Based on TCP/IP

- best effort
- packet switching (IPv6 calls it packets, not datagram)
- *connection-oriented* TCP
- *connection-less* UDP

RFC-1958:

> A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set"of rules that generates a large, varied and evolving space of technology.

Common Address Space



- Internet is defined by the address space
- IPv4 based on 32-bit addresses, example dotted decimal format 10.0.0.1
- IPv6 very similar to IPv4 without NAT, 128-bit addresses in hex ::1, 2a06:d380:0:101::80

How to use the Internet Protocols (IP)

Names are used by humans

www.kramse.org

hlk@kramse.org

Computers use the addresses

```
www     IN      A       185.129.63.130
        IN      AAAA    2a06:d380:0:102::80
mail    IN      A       217.157.63.115
        IN      AAAA    2a06:d380:0:102::25
```

IPv4 address

```
hlk@bigfoot:hlk$ ipconvert.pl 127.0.0.1
Adressen er: 127.0.0.1
Adressen er: 2130706433
hlk@bigfoot:hlk$ ping 2130706433
PING 2130706433 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.135 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.144 ms
```

IP-adresser typically written as decimal numbers with dots

dot notation: 10.1.2.3

IP-adresser as bits

```
IP-adresse: 127.0.0.1
Heltal: 2130706433
Binary: 11111110000000000000000000000001
```

IP-address converted to bits

Computers use bits

Internet ABC

Previously we used classes: A, B, C, D og E

This proved to be a bit inflexible:

- A-klasse has 16 million hosts
- B-klasse about 65.000 hosts
- C-klasse only 250 hosts

Most people asked for B-klasser - starting to run out!

D-klasse used for multicast

E-klasse reserved

See http://en.wikipedia.org/wiki/Classful_network

Stop saying C, say /24

RFC-1918 Private Networks

Der findes et antal adresserum som alle må benytte frit:

- 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)

Address Allocation for Private Internets RFC-1918 adresserne!

NB: man må ikke sende pakker ud på internet med disse som afsender, giver ikke mening

```
The blocks 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2),
and 203.0.113.0/24 (TEST-NET-3) are provided for use in
documentation.

169.254.0.0/16 has been ear-marked as the IP range to use for end node
auto-configuration when a DHCP server may not be found
```

Documentation Prefix, IPv6 updates etc.

Even documentation has its own prefix, RFC5737:

```
The blocks 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2),
and 203.0.113.0/24 (TEST-NET-3) are provided for use in
documentation.
```

IPv6 listed in RFC3849 `2001:DB8::/32`

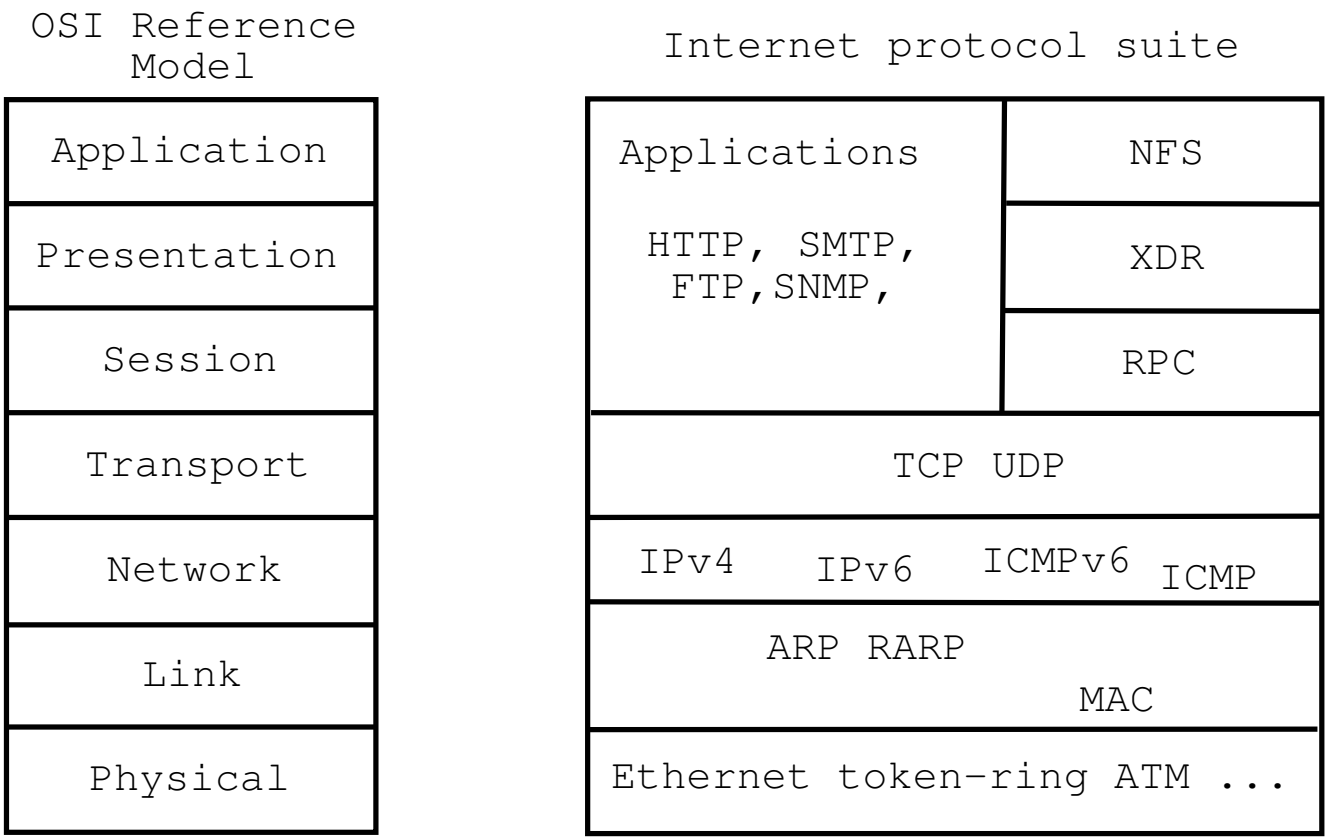
See RFC3330 *Special-Use IPv4 Addresses* which is updated by RFC6890 *Special-Purpose IP Address Registries* which in turn is updated by RFC8190
Use the web version of RFCs to surf back and forth https://www.rfc-editor.org/rfc/rfc8190

CIDR Classless Inter-Domain Routing

Classful routing		Classless routing CIDR	
4 class C networks	Inherent subnet mask	Supernet	Subnet mask
192.0.8.0	255.255.255.0	192.0.8.0	255.255.252.0
192.0.9.0	255.255.255.0		252d=11111100b
192.0.10.0	255.255.255.0		
192.0.11.0	255.255.255.0	Base network/prefix	
		192.10.8.0/22	

- Subnet mask originally inferred by the class
- Started to allocate multiple C-class networks - save remaining B-class
  Resulted in routing table explosion - btw Stop using A, B, C
- A subnet mask today is a row of 1-bit
- Supernet, supernetting
- 10.0.0.0/24 means the network 10.0.0.0 with 24 subnet bits (mask 255.255.255.0)
- 2a06:d380:0:101::80/64 means the network with 64-bit prefix length

Protocols: OSI and Internet models



Ethernet, cables

Show link, and activity – blinkenlights

MAC address

```
00-03-93    (hex)        Apple Computer, Inc.
000393      (base 16)    Apple Computer, Inc.
                         20650 Valley Green Dr.
                         Cupertino CA 95014
                         UNITED STATES
```

Network technologies use a layer 2 hardware address

Typically using 48-bit MAC addresses known from Ethernet MAC-48/EUI-48

First half is assigned to companies – Organizationally Unique Identifier (OUI)

Using the OUI you can see which producer and roughly when a network chip was produced

http://standards.ieee.org/regauth/oui/index.shtml

Bridges

Ethernet is a broadcast technology data transmitted into the ether – a cable

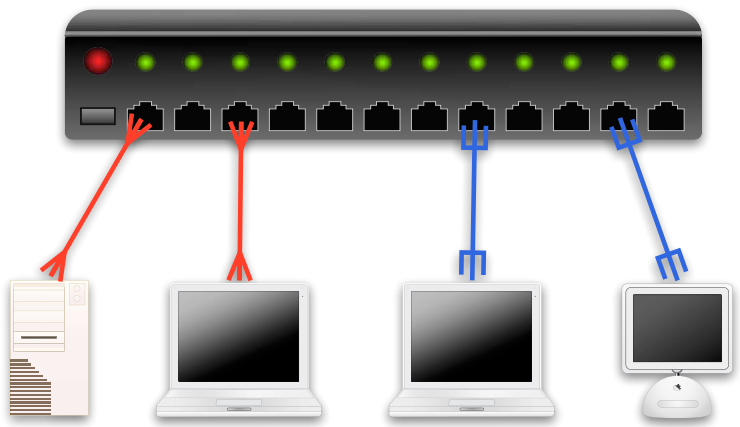
This limits how many devices to connect

Using bridges we can connect segments – which copy between them if needed

It learns the devices on each side (MAC address)

See also http://en.wikipedia.org/wiki/ALOHAnet

A switch



Today we use switches, Don't buy a hub, not even for experimenting or sniffing

A switch can receive and send data on multiple ports at the same time

Performance only limited by the backplane and switching chips

Can also often route with the same speed and mirror packets

Wireless

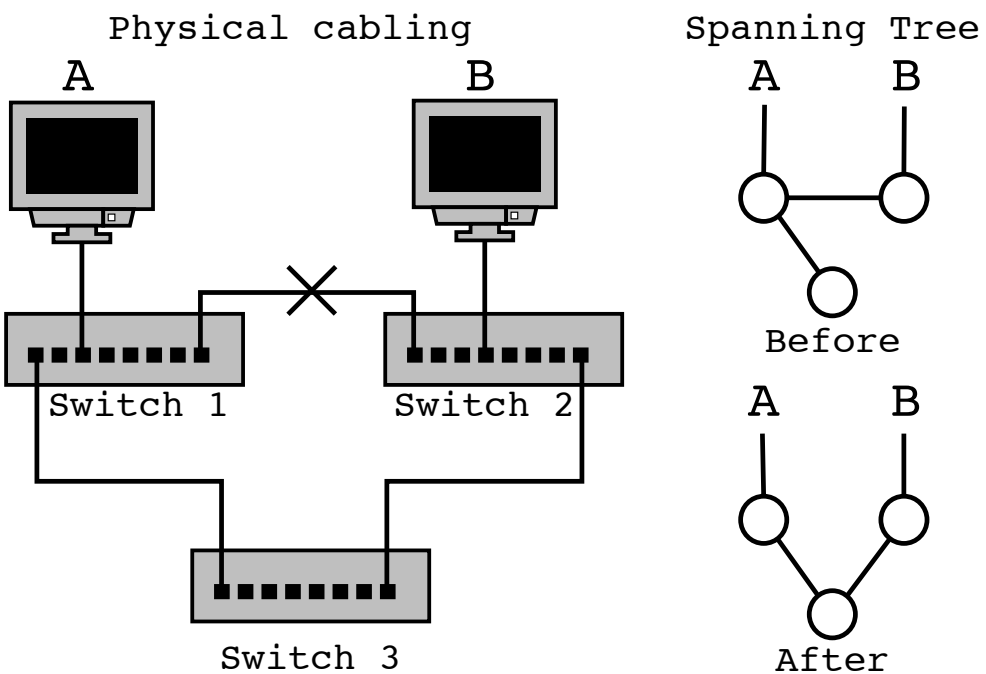
A typical home router would have built-in 802.11 Access-Point (AP) and some Ethernet LAN ports

A modern router

- Opal (GL-SFT1200) is a pocket-sized travel router supporting 1200Mbps wireless, Max. 300 Mbps (2.4GHz) + 867 Mbps (5GHz) Fast Wi-Fi Speeds, Powerful CPU with 3 x Gigabit Ports, Excellent Security with VPN – OpenVPN & WireGuard, IPv6

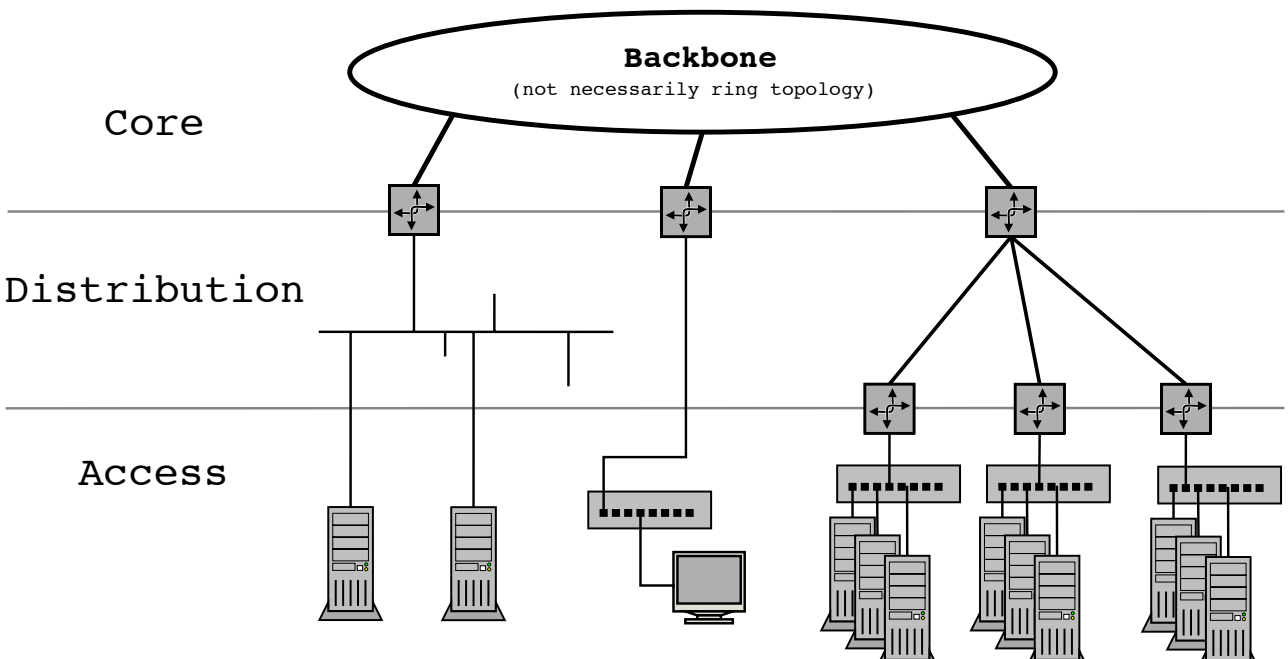
  Source: https://www.gl-inet.com/products/gl-sft1200/

Topologier og Spanning Tree Protocol



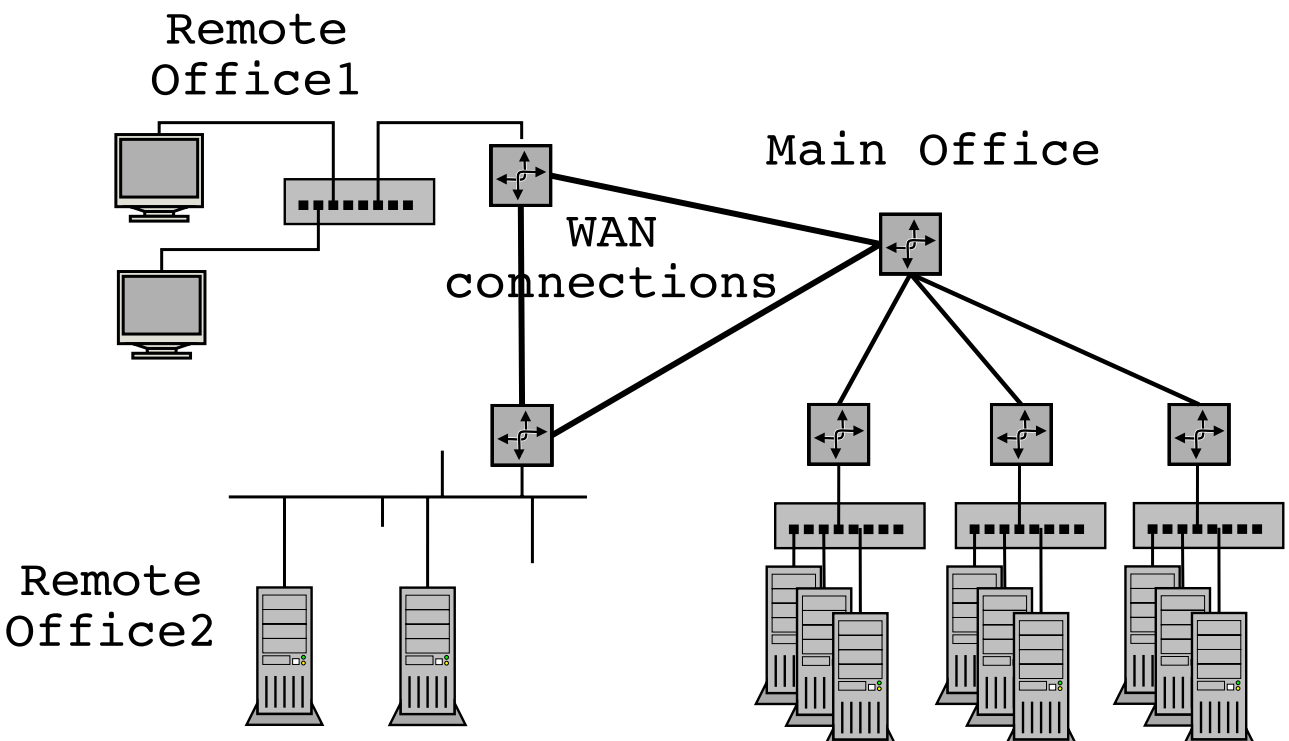
Se mere i bogen af Radia Perlman, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*

Core, Distribution og Access net

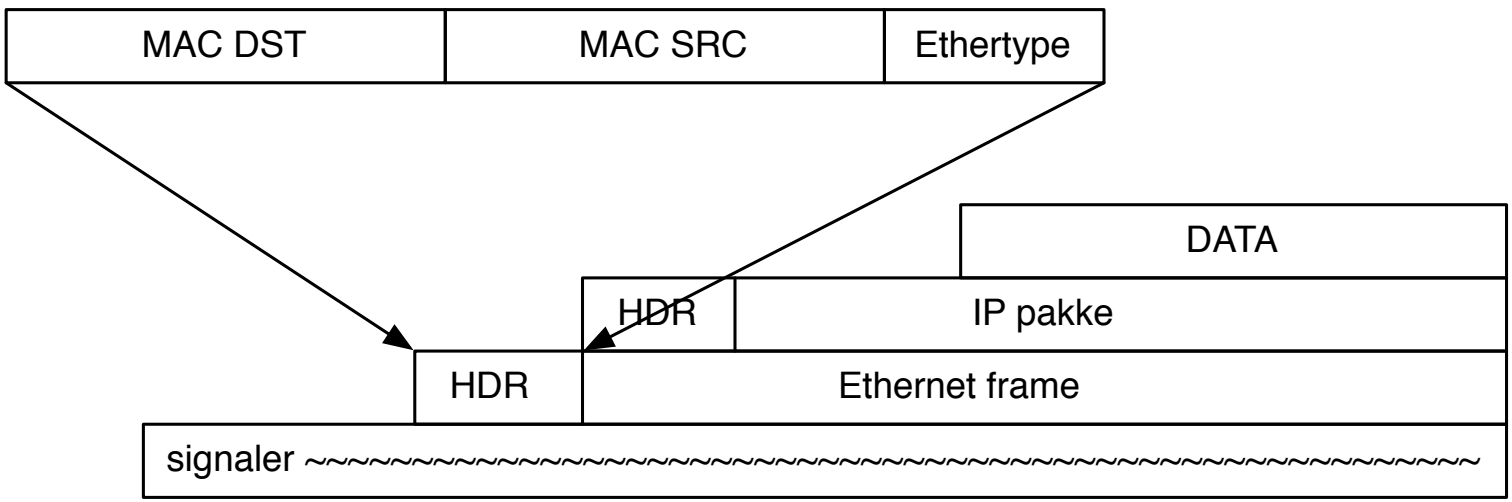


Det er ikke altid man har præcis denne opdeling, men den er ofte brugt

Bridges and routers



Packets across the wire or wireless



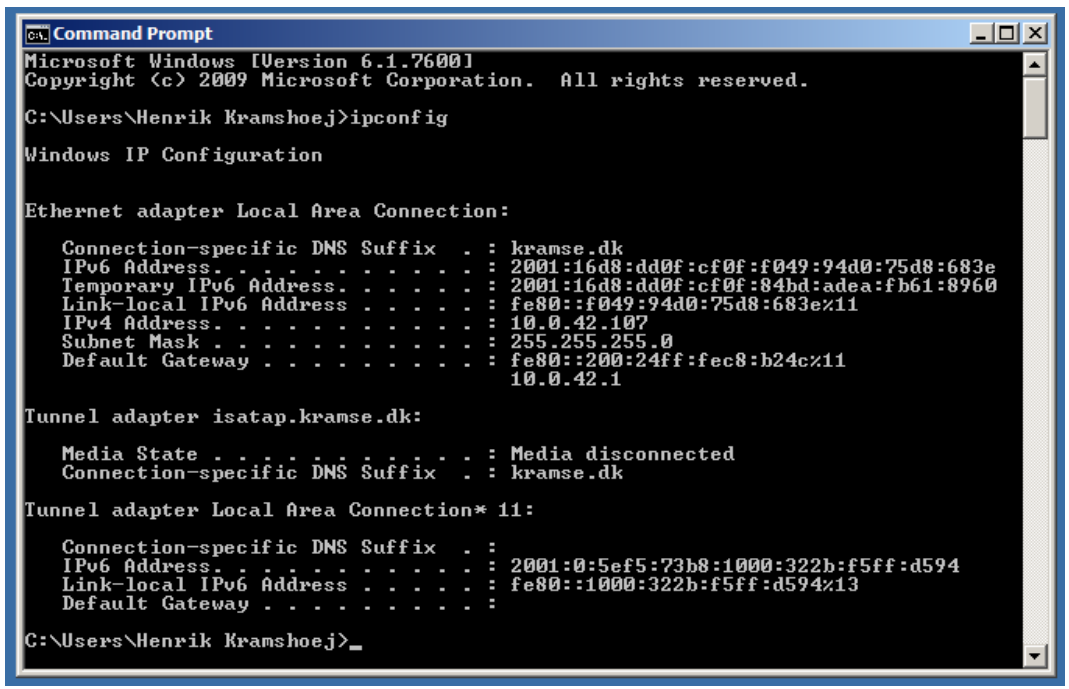
Looking at data as a stream the packets are a pattern laid on top

Network technology defines the start and end of a frame, example Ethernet

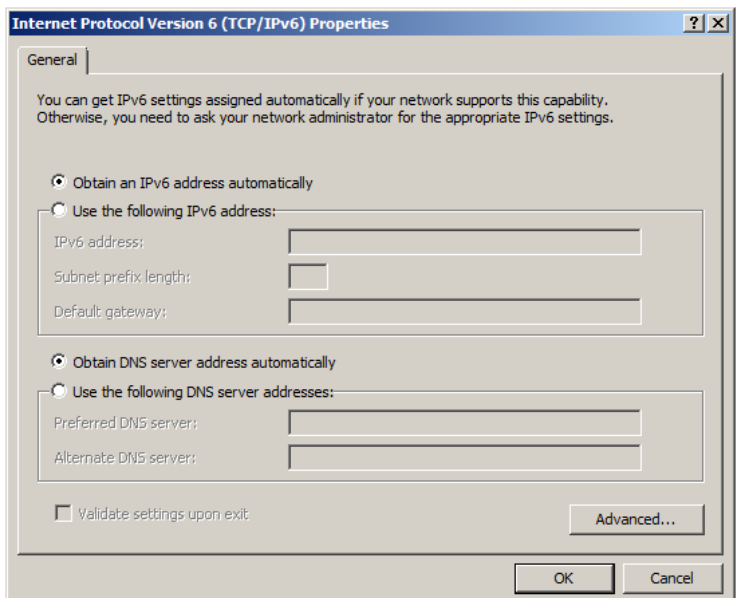
From a lower level we receive a packet, example 1500-bytes from Ethernet driver

Operating system masks a lot of complexity

Windows - ipconfig

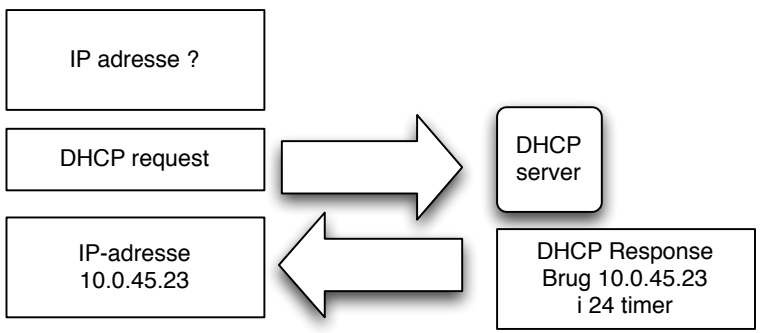


Windows – control panel with DHCP



DHCP is responsible for giving you a dynamic address

DHCP Dynamic Host Configuration Protocol



How does a system get the address?

Typically in IPv4 they will get them from DHCP

System sends a DHCP request, server allocates an address *lease*

IPv6 typically uses Router Advertisement – get prefix, configure their own IPv6 address

Unix - practical examples ifconfig and ping

```
$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6  fe80::216:cbff:feac:1d9f%en0 prefixlen 64 scopeid 0x4
        inet  10.0.42.15 netmask 0xffffff00 broadcast 10.0.42.255
        inet6  2001:16d8:dd0f:cf0f:216:cbff:feac:1d9f prefixlen 64 autoconf
        ether 00:16:cb:ac:1d:9f
        media: autoselect (1000baseT <full-duplex>) status: active

$ ping6 ::1
PING6(56=40+8+8 bytes) ::1 --> ::1
16 bytes from ::1, icmp_seq=0 hlim=64 time=0.089 ms
16 bytes from ::1, icmp_seq=1 hlim=64 time=0.155 ms

$ traceroute6 2001:16d8:dd0f:cf0f::1
traceroute6 to 2001:16d8:dd0f:cf0f::1 (2001:16d8:dd0f:cf0f::1)
from 2001:16d8:dd0f:cf0f:216:cbff:feac:1d9f, 64 hops max, 12 byte packets
 1  2001:16d8:dd0f:cf0f::1  0.399 ms  0.371 ms  0.294 ms
```

Knowledge and insight

- Networks have end-points and conversations on multiple layers
- Wireshark is advanced, try right-clicking different places
- Name resolution includes low level MAC addresses, and IP - names

- Tcpdump format, built-in to many network devices
- Remote packet dumps, like `tcpdump -i eth0 -w packets.pcap`
- Story: tcpdump was originally written in 1988 by Van Jacobson, Sally Floyd, Vern Paxson and Steven McCanne who were, at the time, working in the Lawrence Berkeley Laboratory Network Research Group https://en.wikipedia.org/wiki/Tcpdump

Great network security comes from knowing networks!

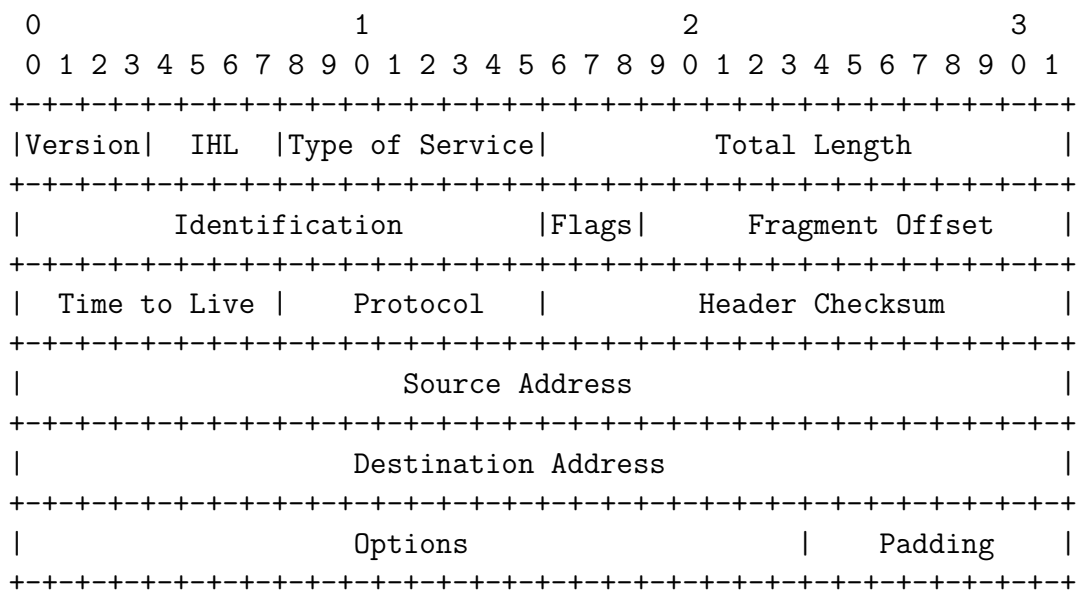
Network Knowledge Needed

To work with network security the following protocols are the bare minimum to know about.

- ARP Address Resolution Protocol for IPv4
- NDP Neighbor Discovery Protocol for IPv6
- IPv4 & IPv6 – the basic packet fields source, destination,
- ICMPv4 & ICMPv6 Internet Control Message Protocol
- UDP User Datagram Protocol
- TCP Transmission Control Protocol
- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System

A little Linux knowledge is also **highly recommended**

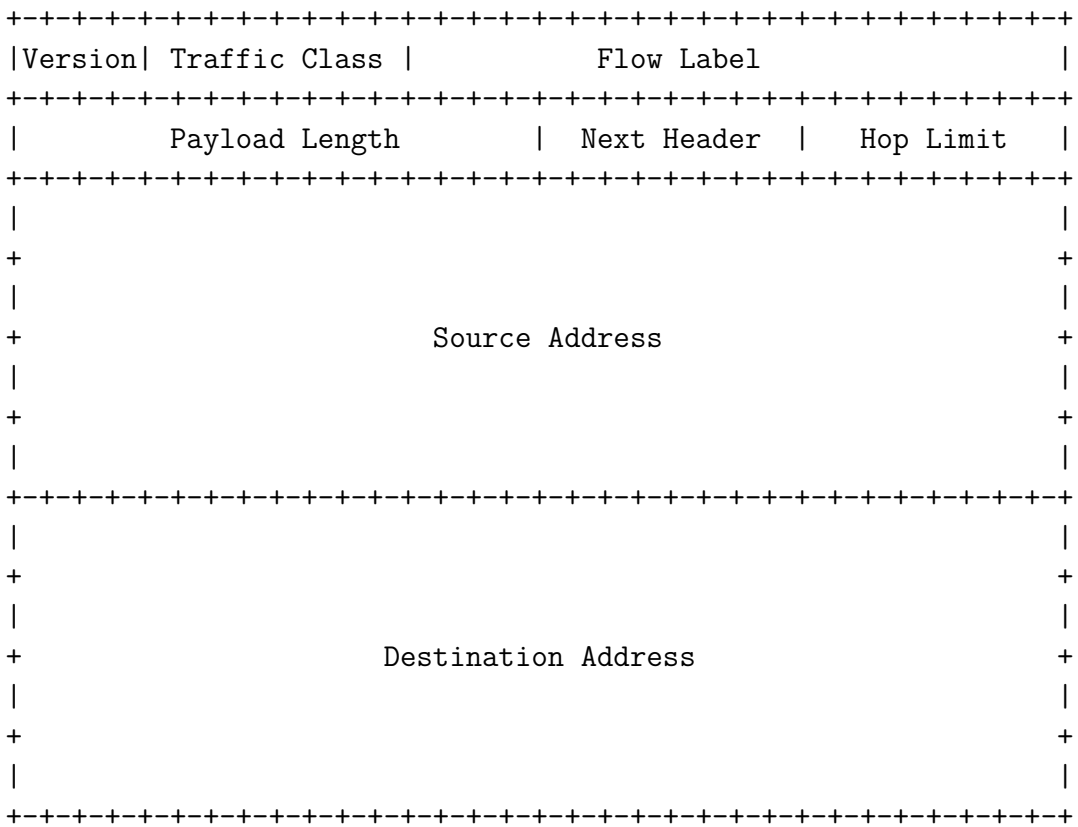
IPv4 header - RFC-791 september 1981



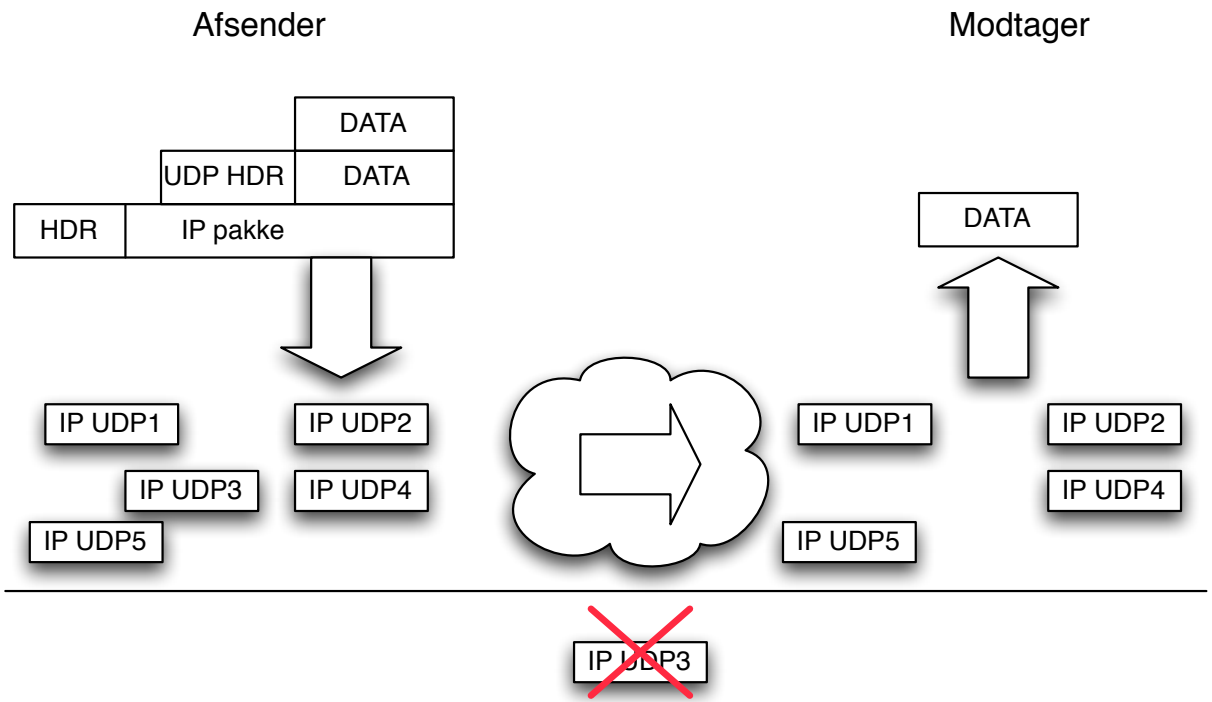
Example Internet Datagram Header

Source: https://datatracker.ietf.org/doc/html/rfc791 and updated later

IPv6 header - RFC-1883 December 1995

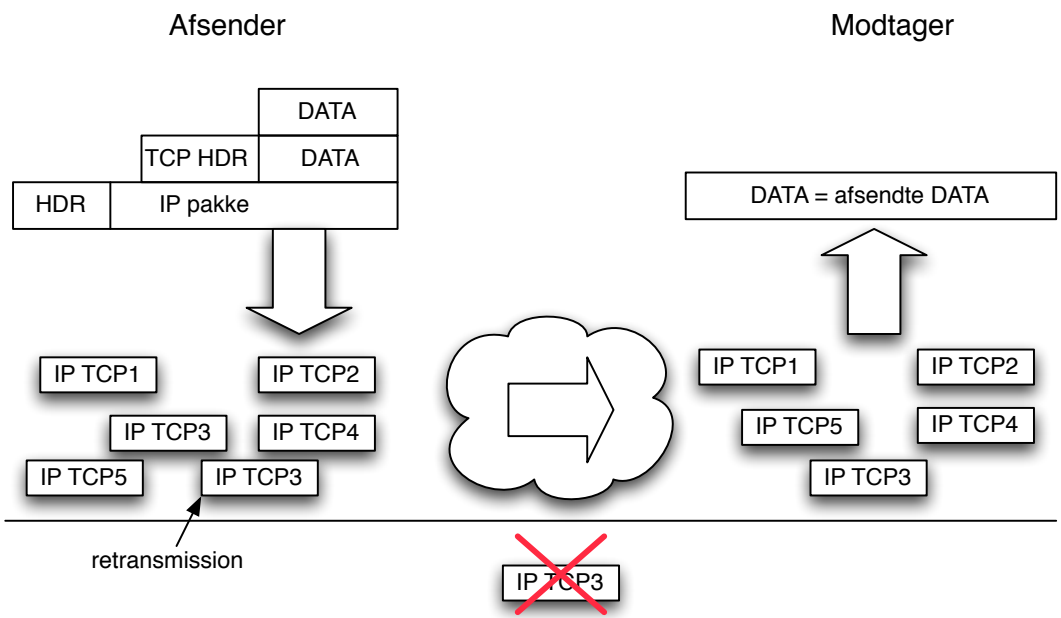


UDP User Datagram Protocol



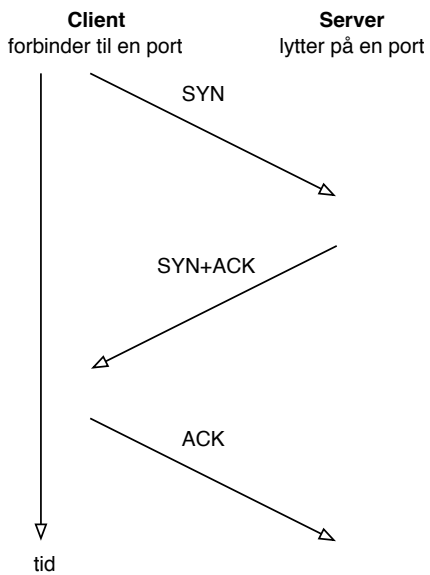
Connectionless https://en.wikipedia.org/wiki/User_Datagram_Protocol

TCP Transmission Control Protocol



Connection-oriented https://en.wikipedia.org/wiki/Transmission_Control_Protocol

TCP three way handshake



- Session setup is used in some protocols
- Other protocols like HTTP/2 can perform request in the first packet

Well-Known Port Numbers

IANA maintains a list of magical numbers in TCP/IP

Lists of protocl numbers, port numers etc.

A few notable examples:

- Port 25/tcp Simple Mail Transfer Protocol (SMTP)
- Port 53/udp and 53/tcp Domain Name System (DNS)
- Port 80/tcp Hyper Text Transfer Protocol (HTTP)
- Port 443/tcp HTTP over TLS/SSL (HTTPS)

Source: http://www.iana.org

Whois – Where do IP addresses come from

A these magical numbers we use on the internet are administered by IANA https://www.iana.org/

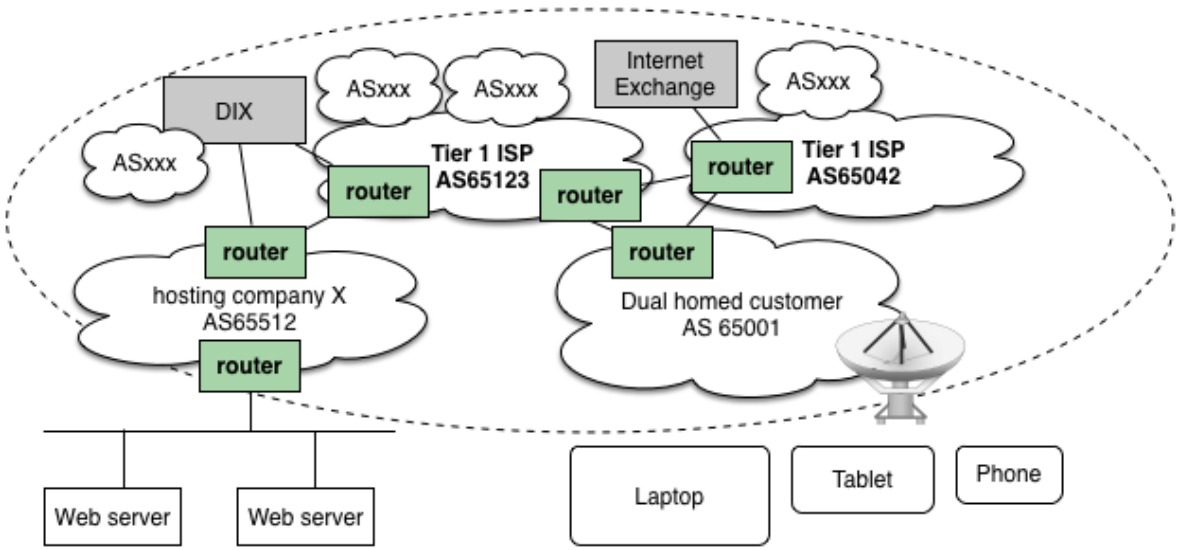
They have handed out portions to the Region Internet Registries (RIR)

- RIPE (Réseaux IP Européens) http://ripe.net
- ARIN American Registry for Internet Numbers http://www.arin.net
- Asia Pacific Network Information Center http://www.apnic.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands

AFRINIC https://afrinic.net/

They are memberbased, and members are called Local Internet Registries (LIRs) og National Internet Registry (NIR)

Hosting and internet providers



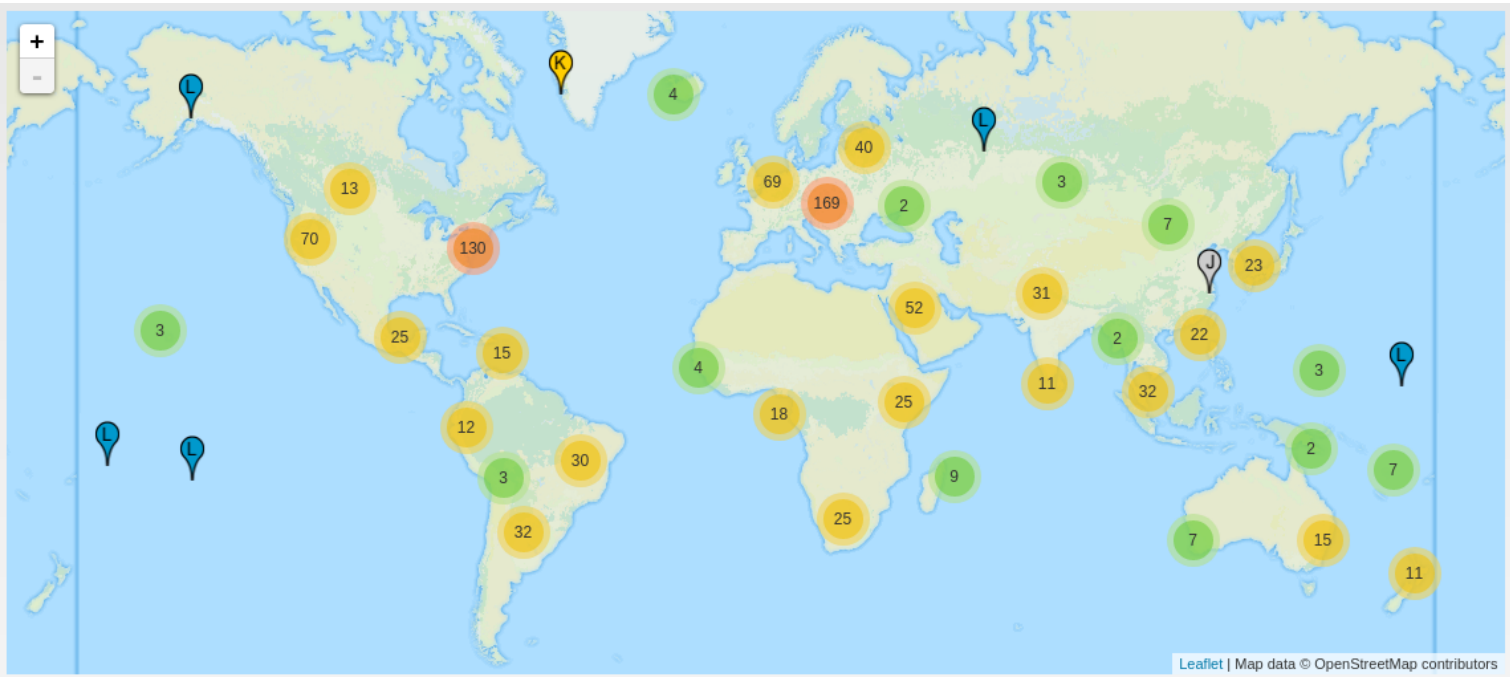
- BGP networks are used for all of the Internet
- New standards like Resource Public Key Infrastructure (RPKI) are underway
- Try RIPE BGPlay https://stat.ripe.net/special/bgplay#bgplay_fetch.resource=185.129.60.1

DNS root – the server addresses

```
a.root-servers.net 198.41.0.4, 2001:503:ba3e::2:30 Verisign, Inc.
b.root-servers.net 170.247.170.2, 2801:1b8:10::b University of Southern California,
Information Sciences Institute
c.root-servers.net 192.33.4.12, 2001:500:2::c Cogent Communications
d.root-servers.net 199.7.91.13, 2001:500:2d::d University of Maryland
e.root-servers.net 192.203.230.10, 2001:500:a8::e NASA (Ames Research Center)
f.root-servers.net 192.5.5.241, 2001:500:2f::f Internet Systems Consortium, Inc.
g.root-servers.net 192.112.36.4, 2001:500:12::d0d US Department of Defense (NIC)
h.root-servers.net 198.97.190.53, 2001:500:1::53 US Army (Research Lab)
i.root-servers.net 192.36.148.17, 2001:7fe::53 Netnod
j.root-servers.net 192.58.128.30, 2001:503:c27::2:30 Verisign, Inc.
k.root-servers.net 193.0.14.129, 2001:7fd::1 RIPE NCC
l.root-servers.net 199.7.83.42, 2001:500:9f::42 ICANN
m.root-servers.net 202.12.27.33, 2001:dc3::35 WIDE Project
```

Source: https://www.iana.org/domains/root/servers, see also https://en.wikipedia.org/wiki/Root_name_server

DNS root servers



As of 2019-01-29, the root server system consists of 933 instances operated by the 12 independent root server operators.

http://root-servers.org/

Metadata – enrichment

Metadata	Metacategory: Data
The DNS lookup occurred at a certain time.	Timestamp: 278621182
The internal host sent a DNS PTR request.	Network protocol: DNS PTR
The internal host had a hostname.	Location: Desktop subnet
	Source IP Address: 1.1.1.2
	Hostname: windowspc22.company.com
The internal host resolved an external host.	Location: External
	Destination IP Address: 255.123.215.3
	Hostname: dgf7adfnkjhh.com
The external host was hosted by a dynamic DNS provider.	Network: Shady DDnS Provider Inc.
	ASN: SHADY232
	Reputation: Historically risky network
The remote hostname appeared randomly generated.	Hostname: dgf7adfnkjhh.com
	Category: Unusual, nonlinguistic

Source: picture from Crafting the InfoSec Playbook, CIP

Metadata + Context

ICMP and Ping

Internet Control Message Protocol (ICMP)

Error conditions are signalled using this

The ping program sends ICMP ECHO request and expect ICMP ECHO reply

```
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=150 time=8.849 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=150 time=0.588 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=150 time=0.553 ms
```

traceroute

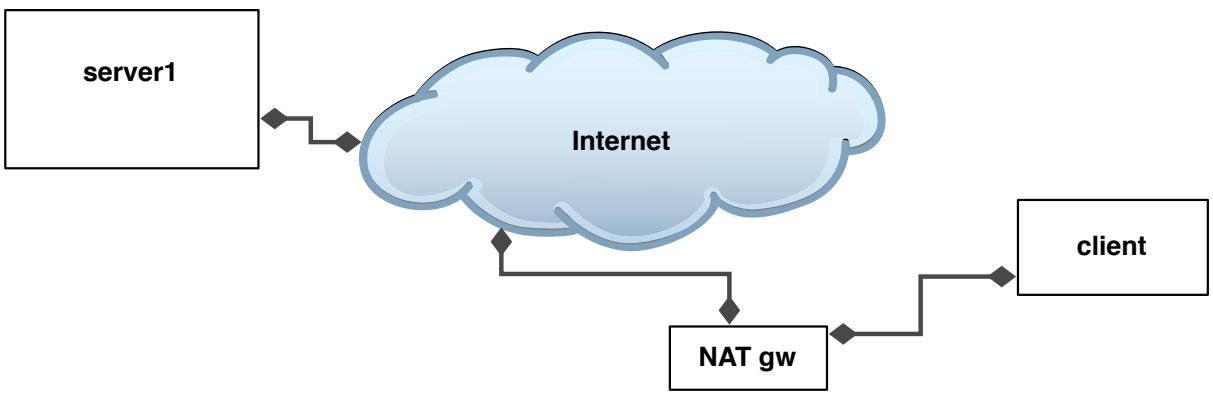
traceroute works using the Time to Live (TTL) or Hop-Count fields

Each router will subtract one from this, and if zero – return ICMP message

Unix uses UDP and Windows usually uses ICMP Echo

```
$ traceroute 185.129.60.129
traceroute to 185.129.60.129 (185.129.60.129),
30 hops max, 40 byte packets
 1  safri (10.0.0.11)  3.577 ms  0.565 ms  0.323 ms
 2  router (185.129.60.129)  1.481 ms  1.374 ms  1.261 ms
```

NAT Network Address Translation



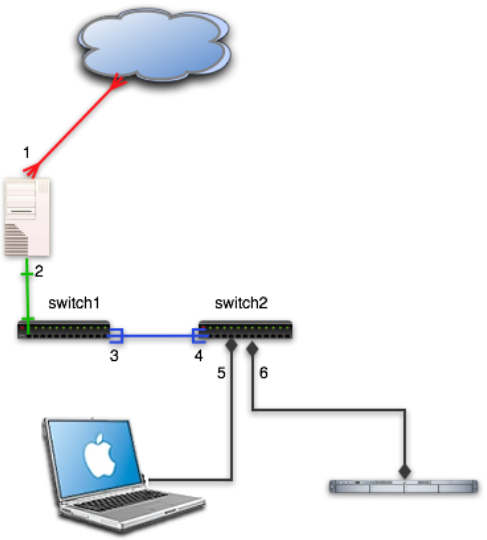
- NAT is used for connecting private networks to the Internet
- NAT gateway replaces source address and forwards packets
- A quick and dirty fix that keeps messing up networks and protocols
- The NAT router/firewall has state tables

Course Network

.

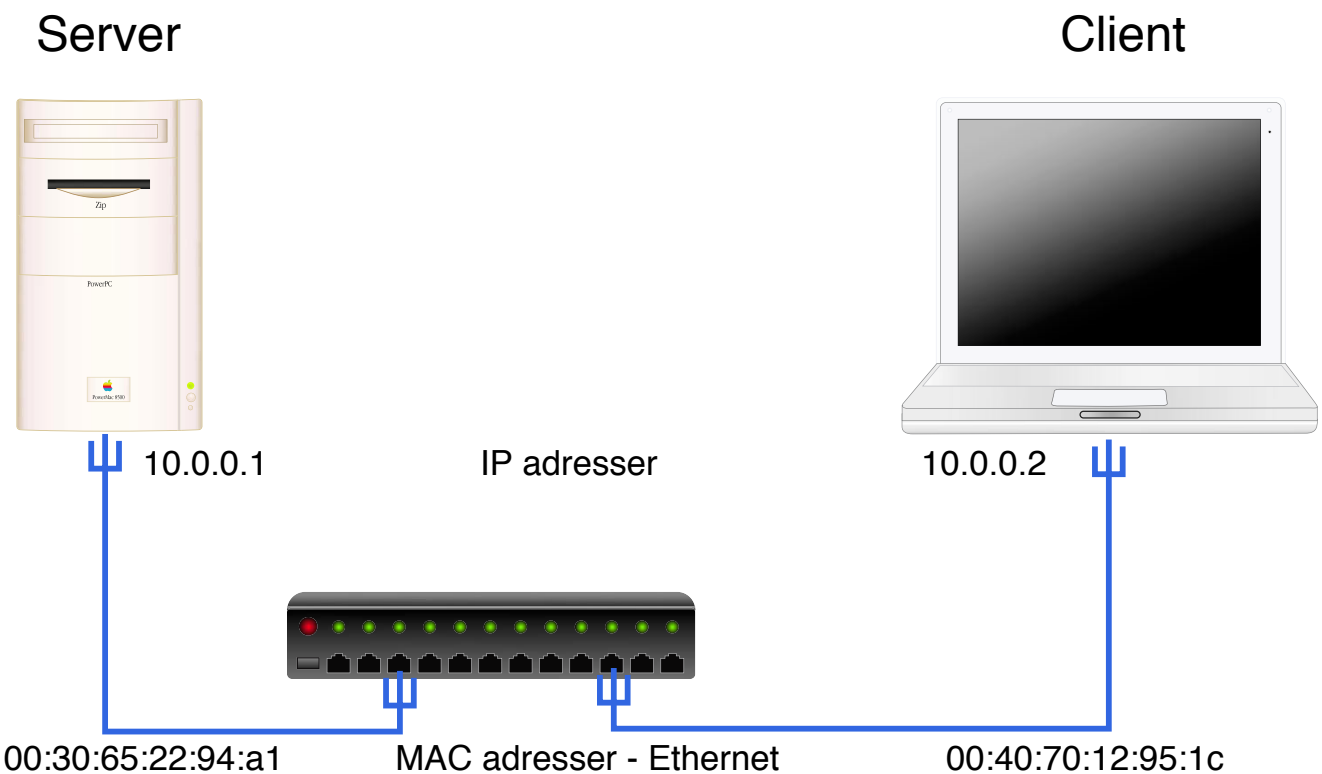
I have a course network with me which has the following information:

- Router APU24D – single board computer with OpenBSD
- Switches Juniper and TP-Link
- wireless access-points Unifi AP https://en.wikipedia.org/wiki/Autonomous_system_(Internet)



You are encouraged to use the network

ARP in IPv4


Server
Client
10.0.0.1
IP adresser
10.0.0.2
00:30:65:22:94:a1
MAC adresser - Ethernet
00:40:70:12:95:1c

ARP request and reply

ping 10.0.0.2 from server

ARP Address Resolution Protocol request/reply:

- ARP request broadcasted on layer 2 - Who has 10.0.0.2 Tell 10.0.0.1
- ARP reply (from 10.0.0.2) 10.0.0.2 is at 00:40:70:12:95:1c

IP ICMP request/reply:

- Echo (ping) request from 10.0.0.1 to 10.0.0.2
- Echo (ping) reply from 10.0.0.2 to 10.0.0.1
- ...

ARP is performed on Ethernet before IP can be transmitted

IPv6 Neighbor Discovery Protocol (NDP)

OSI	IPv4	IPv6
Network	IP / ICMP	IPv6 / ICMPv6
Link	ARP	
Physical	Physical	Physical

Address Resolution Protocol (ARP) is replaced

NDP expands on the ARP concept, similar command `arp -an` compared to `ndp -an`

Can do some things we knew from DHCPv4 still DHCPv6 exist

Note ICMPv6 often need to be added to firewall rules for NDP! 🚩

ARP vs NDP

So at the low level, near the hardware we have protocols connecting IP addreses with MAC addresses, Ethernet and Wi-Fi are commonly found

```
hlk@bigfoot:basic-ipv6-new$ arp -an
? (10.0.42.1) at 0:0:24:c8:b2:4c on en1 [ethernet]
? (10.0.42.2) at 0:c0:b7:6c:19:b on en1 [ethernet]

hlk@bigfoot:basic-ipv6-new$ ndp -an
Neighbor                        Linklayer Address  Netif Expire    St Flgs Prbs
::1                             (incomplete)         lo0 permanent R
2001:16d8:ffd2:cf0f:21c:b3ff:fec4:e1b6 0:1c:b3:c4:e1:b6 en1 permanent R
fe80::1%lo0                     (incomplete)         lo0 permanent R
fe80::200:24ff:fec8:b24c%en1  0:0:24:c8:b2:4c      en1 8h54m51s  S  R
fe80::21c:b3ff:fec4:e1b6%en1  0:1c:b3:c4:e1:b6     en1 permanent R
```

ARP and NDP problems

- This mapping is used in your operating system, keep a dynamic ARP/neighbor cache – a table
- Switches map devices to ports – tables
- Routers remember your IP, so it can send responses back – tables
- A table has a maximum size! This can cause problems 🚩
- This is all done without ANY security – you can lie, attackers can lie
- See ARP spoofing and a sample tool https://en.wikipedia.org/wiki/ARP_spoofing and https://en.wikipedia.org/wiki/DSniff

IPv6 addressing RFC-4291

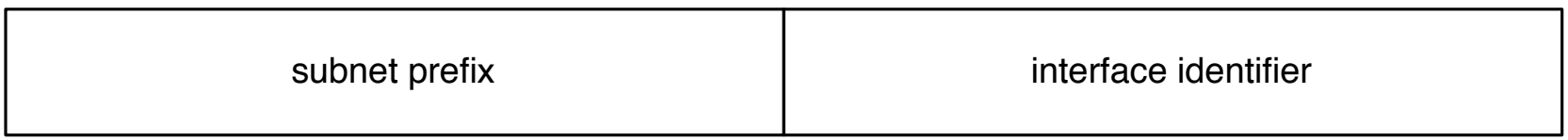
Addresses are always 128-bit identifiers for interfaces and sets of interfaces

Unicast: An identifier for a **single interface**.
A packet sent to a unicast address is delivered to the interface identified by that address.

Anycast: An identifier for a **set of interfaces** (typically belonging to different nodes).
A packet sent to an anycast address is **delivered to one** of the interfaces identified by that address (the "nearest"one, according to the routing protocols' measure of distance).

Multicast: An identifier for a **set of interfaces** (typically belonging to different nodes).
A packet sent to a multicast address is **delivered to all interfaces identified by that address**.

IPv6 addressing RFC-4291, cont.



2001:16d8:ff00:012f:0000:0000:0000:0002
2001:16d8:ff00:12f::2

8 times 4 hex-digits seperated by colon x:x:x:x:x:x:x:x

Written as ipv6-address/prefix-length CIDR notation

Leading zeros can be removed

One or more groups of 16 bits of zeros can be replaced by ::

Examples:

- ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
- Adddress 2001:DB8:0:0:8:800:200C:417A
- Address of loopback ::1
- IPv6 prefix 2a02:09d0:95::1/64, subnet 2a02:09d0:0095:0000::/64
- Address 2a02:09d0:95::1 or 2a02:09d0:0095:0000:0000:0000:0000:0001

IPv6 address - special prefixes

- link-local unicast addresses
  fe80::/10 generated from the interface MAC address EUI-64
- FEC0::/10 site-local - deprecated in RFC-3879
- 2001:0DB8::/32 NON-ROUTABLE range to be used for documentation purpose RFC-3849.
- FC00::/7 Unique Local IPv6 Unicast Addresses RFC-4193
  http://www.simpledns.com/private-ipv6.aspx
  If you do not like to put public addresses on internal network - use this instead

Hello neighbors

```
$ ping6 -w -I en1 ff02::1
PING6(72=40+8+24 bytes) fe80::223:6cff:fe9a:f52c%en1 --> ff02::1
30 bytes from fe80::223:6cff:fe9a:f52c%en1: bigfoot
36 bytes from fe80::216:cbff:feac:1d9f%en1: mike.kramse.dk.
38 bytes from fe80::200:aaff:feab:9f06%en1: xrx0000aaab9f06
34 bytes from fe80::20d:93ff:fe4d:55fe%en1: harry.local
36 bytes from fe80::200:24ff:fec8:b24c%en1: kris.kramse.dk.
31 bytes from fe80::21b:63ff:fef5:38df%en1: airport5
32 bytes from fe80::216:cbff:fec4:403a%en1: main-base
44 bytes from fe80::217:f2ff:fee4:2156%en1: Base Station Koekken
35 bytes from fe80::21e:c2ff:feac:cd17%en1: arnold.local
```

IPv6 autoconfiguration

`Modified EUI-64 format-based interface identifiers`

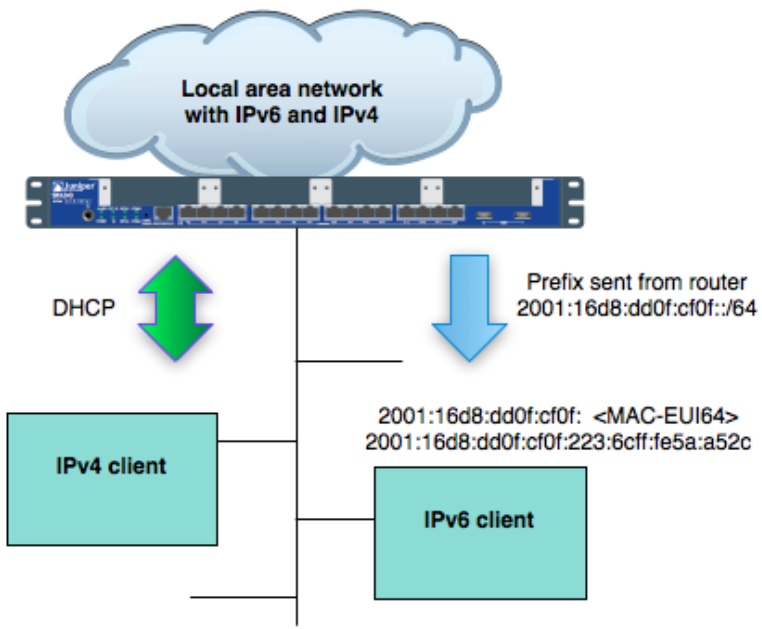
```
ifconfig en1
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 00:23:6c:9a:f5:2c
                00-23-6c-ff-fe-9a-f5-2c  48-bit MAC stretched to become EUI-64
                02-23-6c-ff-fe-9a-f5-2c  inverting the "u" bit (universal/local bit)
                fe80::  +  0223:6cff:fe9a:f52c   add link-local prefix
        inet6 fe80::223:6cff:fe9a:f52c%en1 prefixlen 64 scopeid 0x6
```

DHCPv6 is available, but **stateless autoconfiguration** is king

Routers announce subnet prefix via **router advertisements**

Individual nodes then combine this with their EUI64 identifier

Router Advertisement ICMPv6



Exercise

Now lets do the exercise

ℹ Using ping and traceroute 10 min

which is number **6** in the exercise PDF.

Exercise

Now lets do the exercise

ℹ DNS and Name Lookups 10 min

which is number **7** in the exercise PDF.

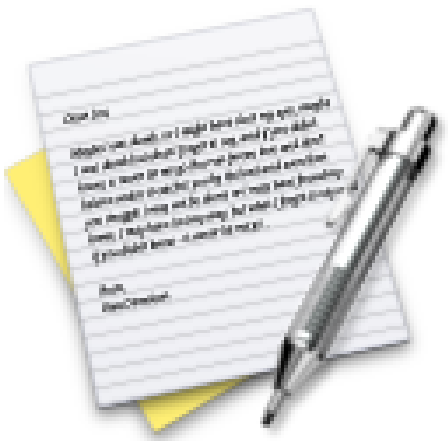
Exercise

Now lets do the exercise

Whois databases 15 min

which is number **8** in the exercise PDF.

Exercise

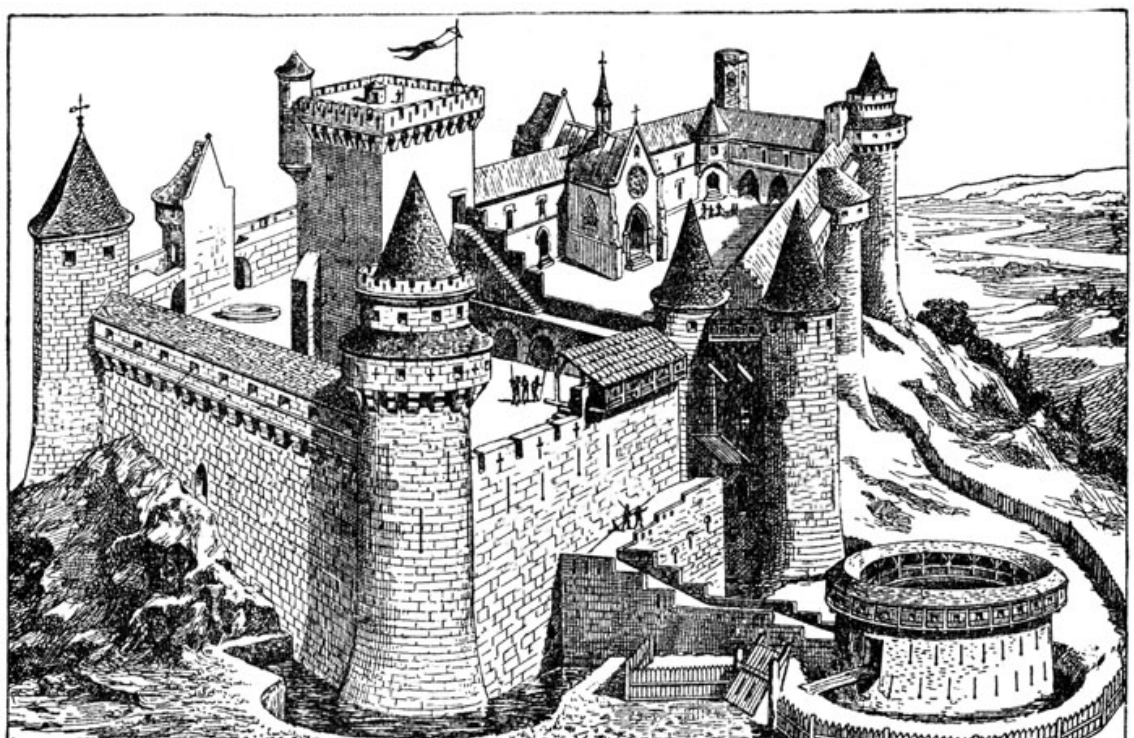


Now lets do the exercise

IP address research 30 min

which is number 9 in the exercise PDF.

Defense in depth



Picture originally from: http://karenswhimsy.com/public-domain-images

Intrusion Kill Chains

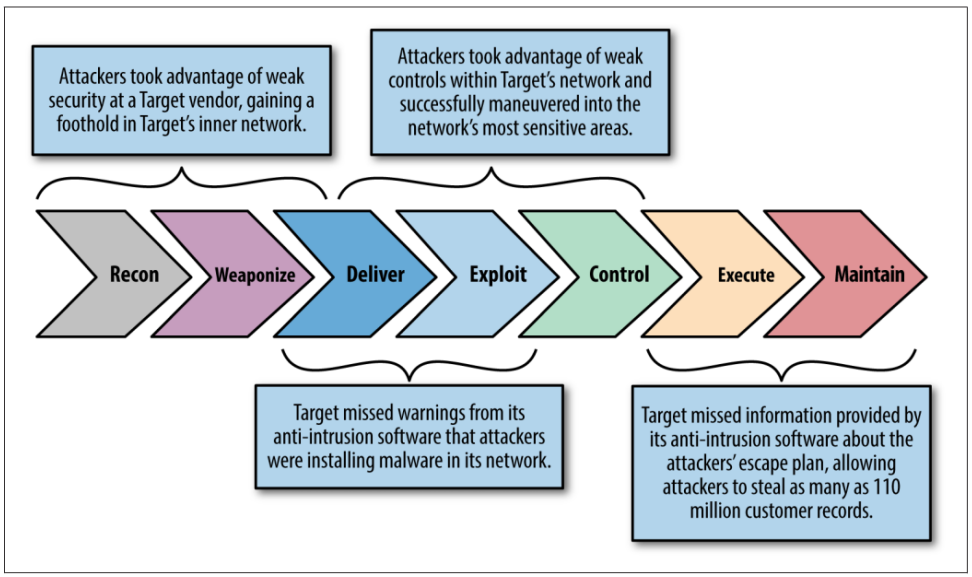


Figure 7-1. The kill chain

- See also *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Eric M. Hutchins , Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corporation

  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

The Spamhaus Don't Route Or Peer Lists

> The Spamhaus Don't Route Or Peer Lists
> DROP (Don't Route Or Peer) and EDROP are advisory "drop all traffic"lists, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by criminals and professional spammers. DROP and EDROP are a tiny subset of the SBL designed for use by firewalls and routing equipment.

http://www.spamhaus.org/drop/

- When your SIEM alerts you, you need tools to block and restrict
- Recommend adding empty blocking access control lists etc. to your network infrastructure
- Add premade blocking to your name servers, proxy servers, recursive servers
- Recommend implementing country lists

Network Segmentation – Firewalls

$ firewall

1. (I) **An internetwork gateway that restricts data communication traffic to and from one of the connected networks** (the one said to be "inside"the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside"the firewall). (See: guard, security gateway.)
2. (O) **A device or system that controls the flow of traffic between networks using differing security postures.** Wack, J. et al (NIST), "Guidelines on Firewalls and Firewall Policy", Special Publication 800-41, January 2002.

Tutorial: A firewall typically protects a smaller, secure network (such as a corporate LAN, or even just one host) from a larger network (such as the Internet). The firewall is installed at the point where the networks connect, and the firewall applies policy rules to control traffic that flows in and out of the protected network.

Source: RFC4949 *Internet Security Glossary, Version 2*

https://datatracker.ietf.org/doc/html/rfc4949 2007

Continued

> **A firewall is not always a single computer.** For example, a firewall may consist of a pair of filtering routers and one or more proxy servers running on one or more bastion hosts, all connected to a small, dedicated LAN (see: buffer zone) between the two routers. The external router blocks attacks that use IP to break security (IP address spoofing, source routing, packet fragments), while proxy servers block attacks that would exploit a vulnerability in a higher-layer protocol or service. The internal router blocks traffic from leaving the protected network except through the proxy servers. The difficult part is defining criteria by which packets are denied passage through the firewall, because a firewall not only needs to keep unauthorized traffic (i.e., intruders) out, but usually also needs to let authorized traffic pass both in and out.

Source: RFC4949 *Internet Security Glossary, Version 2*

https://datatracker.ietf.org/doc/html/rfc4949 2007

- Network layer, packet filters, application level, stateless, stateful
- Firewalls are by design a choke point, natural place
  to do network security monitoring!
- Older but still interesting Cheswick chapter 2 PDF *A Security Review of Protocols: Lower Layers*
  http://www.wilyhacker.com/

Modern Firewall Infrastructures

A firewall blocks traffic on a network

A firewall allows traffic on a network

The interesting part is typically what it allows!

A firewall infrastructure must:

- Prevent attackers from entering
- Prevent data exfiltration
- Prevent worms, malware, virus from spreading in networks
- Be part of an overall solution with ISP, routers, other firewalls, switched infrastructures, intrusion detection systems and the rest of the infrastructure
- ...

Difficult – and requires design and secure operations

Open source based firewalls

- Linux firewalls IP tables, use command line tool ufw Uncomplicated Firewall!
- Firewall GUIs on top of Linux – lots! Some are also available as commercial ones
- OpenBSD PF http://www.openbsd.org
- FreeBSD IPFW og IPFW2 http://www.freebsd.org
- Mac OS X uses OpenBSD PF
- FreeBSD has an older version of the OpenBSD PF, should really be renamed now

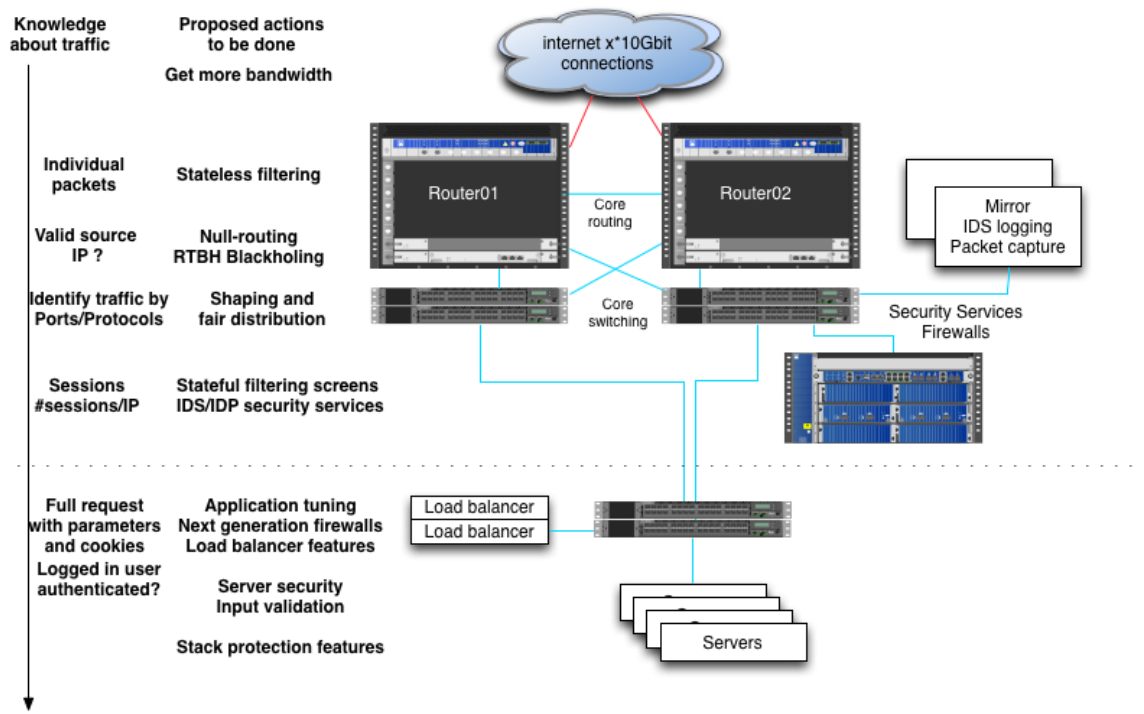
Uncomplicated Firewall (UFW)

```
root@debian01:~# apt install ufw
...
root@debian01:~# ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian01:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian01:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

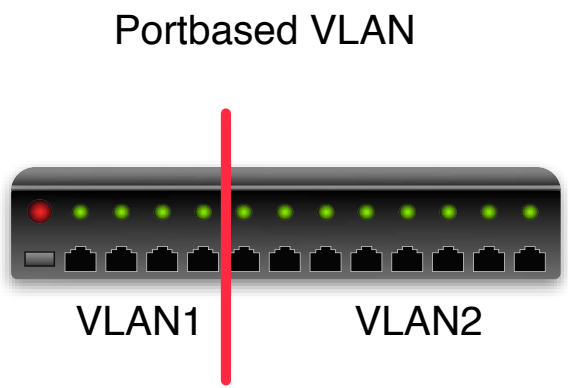
- Extremely easy to use – I recommend and use the (Uncomplicated Firewall) UFW

Firewalls are NOT Alone



Use Defense in Depth – all layers have features

Together with Firewalls - Virtual LAN (VLAN)



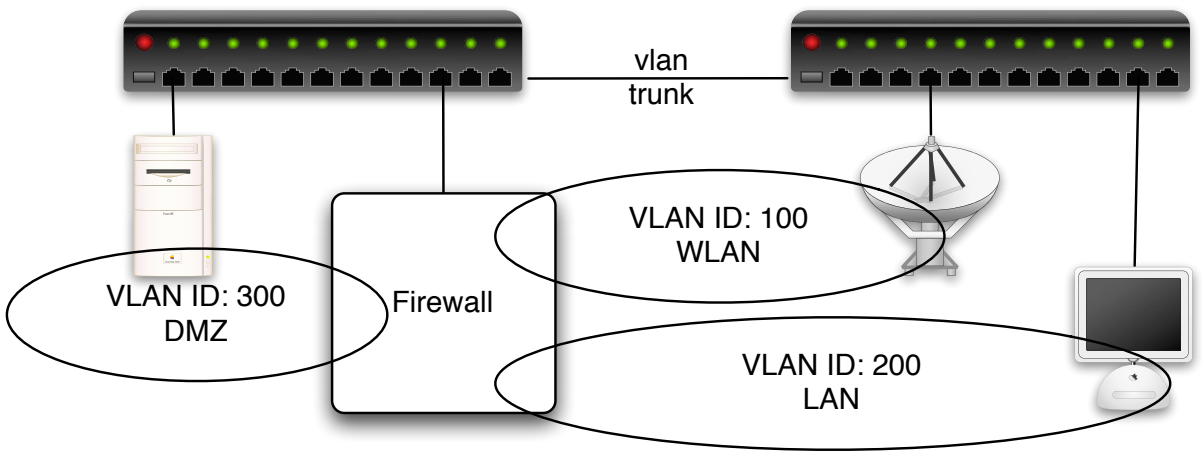
Managed switches often allow splitting into zones called virtual LANs

Most simple version is port based

Like putting ports 1-4 into one LAN and remaining in another LAN

Packets must traverse a router or firewall to cross between VLANs

Virtual LAN (VLAN) IEEE 802.1q



Using IEEE 802.1q VLAN tagging on Ethernet frames

Virtual LAN, to pass from one to another, must use a router/firewall

Allows separation/segmentation and protects traffic from many security issues

Exercise

Now lets do the exercise

Enable firewall - 15min

which is number **4** in the exercise PDF.

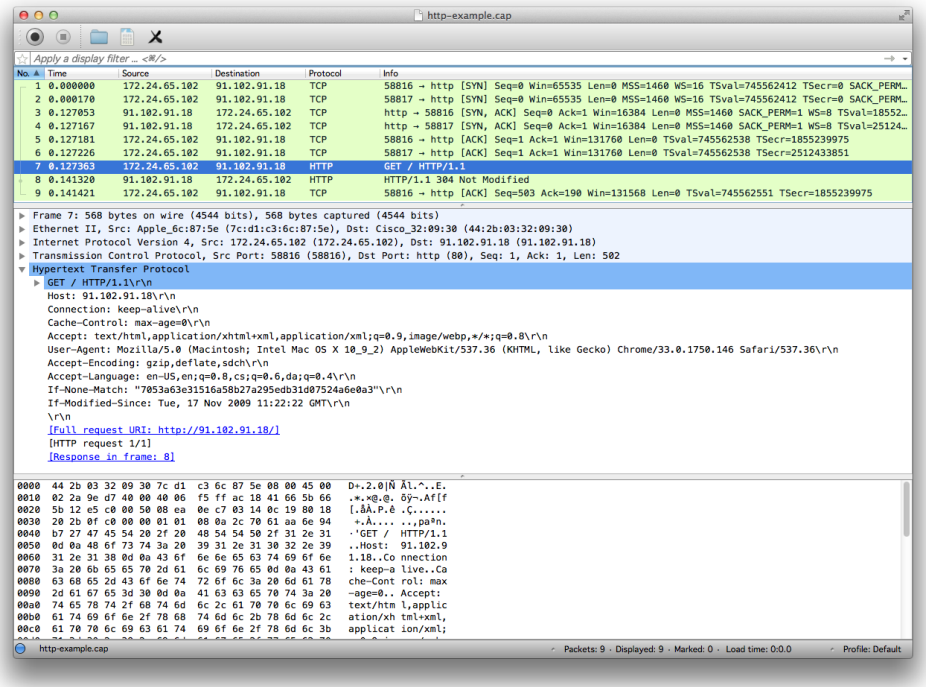
Exercise

Now lets do the exercise

Git tutorials - 15min

which is number **5** in the exercise PDF.

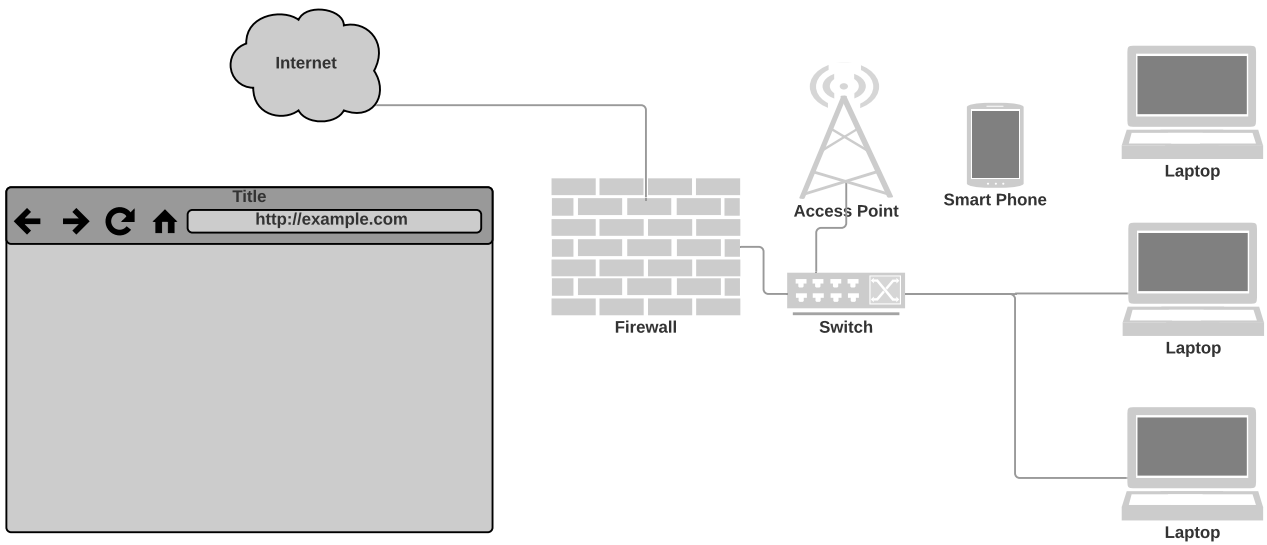
Wireshark - graphical network sniffer



Capture - Options, select a network interface

http://www.wireshark.org

Your Privacy



- Your data travels far
- Often crossing borders, virtually and literally

Exercise

Now lets do the exercise

ℹ Wireshark and Tcpdump 15 min

which is number **10** in the exercise PDF.

Exercise

Now lets do the exercise

Nping check ports 10 min

which is number 11 in the exercise PDF.

Wifi standards IEEE 802.11

IEEE 802.11

- 802.11b 11Mbps
- 802.11g 54Mbps
- 802.11n faster
- 802.11i Security enhancements Robust Security Network RSN

New names soon:
Wi-Fi 6 to identify devices that support 802.11ax technology
Wi-Fi 5 to identify devices that support 802.11ac technology
Wi-Fi 4 to identify devices that support 802.11n technology

Source: http://grouper.ieee.org/groups/802/11/index.html

Wi-Fi Labs Network cards

Varenummer: 2225730

TP-Link TL-WN722N

Hi-Speed USB - 802.11b, 802.11g, 802.11n

På lager, 1-2 dages levering
(Billigste fragt: 0 kr.)
Ret land

Køb

120,00 kr.
(96,00 kr.)

4 stk på lager i Århus
0 stk på lager i Viborg
0 stk på lager i København

Laptop or Netbook, I typically use USB wireless cards
Cheap and easy – keep using your built-in with the host OS

Access Points - get a small selection for testing

Many resources available, books, sites, blogs, etc.

IEEE 802.11 Security fast forward

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by **Fluhrer, Mantin, and Shamir's** paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first **verification of the attack**. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward

The IEEE set up a dedicated task group to create a replacement security solution, **802.11i** (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an **interim specification called Wi-Fi Protected Access (WPA)** based on a subset of the then current IEEE 802.11i draft. These started to appear in products in **mid-2003**. **IEEE 802.11i (also known as WPA2)** itself was ratified in **June 2004**, and uses government strength encryption in the **Advanced Encryption Standard AES,** instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is **WPA2 (AES Pre-Shared Key) and for the Enterprise space is WPA2 along with a RADIUS authentication server** (or another type of authentication server) and a strong authentication method such as EAP-TLS.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11 Security fast forward

In January 2005, the IEEE set up yet another task group "w"to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[24]

In **December 2011**, a security flaw was revealed that affects wireless routers with the **optional Wi-Fi Protected Setup (WPS)** feature. While WPS is not a part of 802.11, **the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours**.

Source: http://en.wikipedia.org/wiki/IEEE_802.11

WPS WTF?! Turn it off – use WPA PSK or WPA Enterprise

WPA3 Security

WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2.[12][13] Certification began in June 2018,[14] and WPA3 support has been mandatory for devices which bear the "Wi-Fi CERTIFIED™"logo since July 2020.[11]

The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode[15] (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

The WPA3 standard also replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, a method originally introduced with IEEE 802.11s, resulting in a more secure initial key exchange in personal mode[16][17] and forward secrecy.[18] The Wi-Fi Alliance also says that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.[2][19]

Protection of management frames as specified in the IEEE 802.11w amendment is also enforced by the WPA3 specifications.

Source: https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- Does not seem to be used much, in Denmark, yet – but coming

IS WPA3 supported?

> A wireless network adapter that supports Wi-Fi 6. To see if your PC supports it, check the documentation that came with it or check the PC manufacturer's website. Tip: You can also check to see if your router supports Wi-Fi 6 by opening the Command Prompt, and then typing the command netsh wlan show drivers. Look next to Radio types supported and see if it includes 802.11ax.

Source: https://support.microsoft.com/en-us/windows/faster-and-more-secure-wi-fi-in-windows-26177a28-38ed-1a8e-7e

- Your devices must support both WPA3 in both operating system and Wi-Fi drivers!
- Windows 10 and 11 does, so try upgrading drivers
- Android does since Android 10 – pretty new still
- Apple devices have support in recent versions

WPA3 on Apple Devices

- iPhone 7 or later.
- iPad 5th generation or later.
- Apple TV 4K or later.
- Apple Watch series 3 or later.
- Mac computers (late 2013 or later, with 802.11ac or later)

Source: https://support.apple.com/da-dk/guide/security/sec8a67fa93d/web

Wi-Fi CERTIFIED WPA3™

WPA3™ provides cutting-edge security protocols to the market. Building on the widespread success and adoption of Wi-Fi security, WPA3 adds new features to simplify Wi-Fi security, enable more robust authentication, deliver increased cryptographic strength for highly sensitive data markets, and maintain resiliency of mission critical networks. All WPA3 networks:

- Use the latest security methods
- Disallow outdated legacy protocols
- Require use of Protected Management Frames (PMF)

Since Wi-Fi networks differ in usage purpose and security needs, WPA3 includes additional capabilities specifically for personal and enterprise networks. Users of WPA3-Personal receive increased protections from password guessing attempts, while WPA3-Enterprise users can now take advantage of higher-grade security protocols for sensitive data networks.

WPA3 is a mandatory certification for Wi-Fi CERTIFIED™ devices.

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3-Personal

WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE). The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

- **Natural password selection**: Allows users to choose passwords that are easier to remember
- **Ease of use**: Delivers enhanced protections with no change to the way users connect to a network
- **Forward secrecy**: Protects data traffic even if a password is compromised after the data was transmitted

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3-Enterprise

WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections.

- **Authentication**: multiple Extensible Authentication Protocol (EAP) methods
- **Authenticated encryption**: minimum 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128)
- **Key derivation and confirmation**: minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA256)
- **Robust management frame protection**: minimum 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)

Source: https://www.wi-fi.org/discover-wi-fi/security

WPA3-Enterprise with 192-bit mode

WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.

- **Authentication**: Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) using Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- **Authenticated encryption**: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- **Key derivation and confirmation**: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- **Robust management frame protection**: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

  The 192-bit security mode offered by WPA3-Enterprise ensures the right combination of cryptographic tools are used and sets a consistent baseline of security within a WPA3 network.

Source: https://www.wi-fi.org/discover-wi-fi/security

2020: Dragonblood

> April 2019 — Modern Wi-Fi networks use WPA2 to protect transmitted data. However, because **WPA2 is more than 14 years old**, the Wi-Fi Alliance recently announced the new and more secure WPA3 protocol. One of the supposed advantages of WPA3 is that, thanks to its underlying **Dragonfly handshake**, it's **near impossible to crack the password** of a network. Unfortunately, we found that even with WPA3, an **attacker within range of a victim can still recover the password**. If the victim uses no extra protection such as HTTPS, this allows an attacker to steal sensitive information such as passwords and emails. We hope our disclosure motivates vendors to mitigate our attacks before WPA3 becomes widespread.
>
> ...
>
> Fortunately, as a result of our research, both the Wi-Fi standard and EAP-pwd are being updated with a more secure protocol. Although this update is not backwards-compatible with current deployments of WPA3, it does prevent most of our attacks.

Source: https://wpa3.mathyvanhoef.com/

- Side-channel leaks
- Full paper Mathy Vanhoef and Eyal Ronen. 2020. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*. In IEEE Symposium on Security & Privacy (SP). IEEE. https://eprint.iacr.org/2019/383

Advanced Subjects

- Nmap
- Zeek
- Suricata

Basic port scanning

What is a port scan

Testing all values possible for port number from 0/1 to 65535

Goal is to identify open ports, listening and vulnerable services

Most often TCP og UDP scan

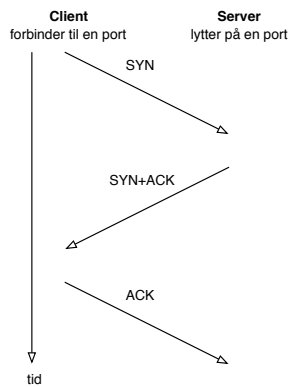
TCP scanning is more realiable than UDP scanning

TCP handshake must respond with SYN-ACK packets

UDP applications respond differently – if they even respond
so probes with real requests may get response, no firewall they respond withb ICMP on closed ports

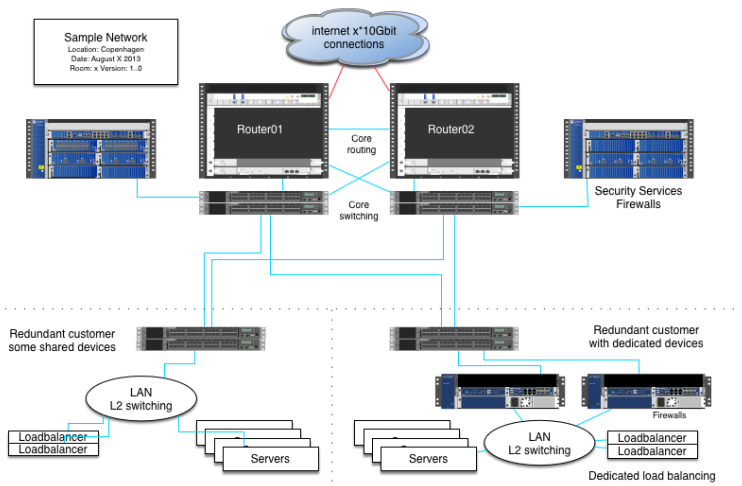
Use the GUI program Zenmap while learning Nmap

TCP three-way handshake



- **TCP SYN half-open** scans
- in the old days systems would only log when a full TCP connection was setup – so doing only half open it was a *stealth*-scans
- Today system and IDS intrusion detection can easily monitor for this
- Sending a lot of SYN packets can create a Denial of Service – **SYN-flooding**

Scope: select systems for testing



- Routers in front of critical systems and networks - availability
- Firewalls – are traffic flows restricted
- Mail servers – open for relaying
- Web servers – remote code execution in web systems, data download

Ping and port sweep

Scans across the network are named sweeps

Ping sweeps using ICMP Ping probes

Port sweep trying to find a specific service, like port 80 web

Quite easy to see in network traffic:

- Selecting two IP-adresser not in use
- Should not see any traffic, but if it does, its being scanned
- If traffic is received on both addresses, its a sweep – if they are a bit apart it is even better, like 10.0.0.100 and 10.0.0.200

Pro tip: a Great network intrusion detection engine (IDS), is Suricata suricata-ids.org

what is Nmap today

> Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

Initial release September 1997; +20 years ago

Today a package of programs for Windows, Mac, BSD, Linux, ... source

Flexible, powerful, and free! Includes other tools!

Lets check release notes, 7.70 pt.
http://seclists.org/nmap-announce/2018/0

Bonus info: you can help Nmap by submitting fingerprints

Nmap port sweep for web servers

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap port sweep for SNMP port 161/UDP

```
root@cornerstone:~# nmap -sU -p 161 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:30 CET
Nmap scan report for 172.29.0.1
Host is up (0.00015s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00011s latency).
PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: 00:0C:29:46:22:FB (VMware)
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

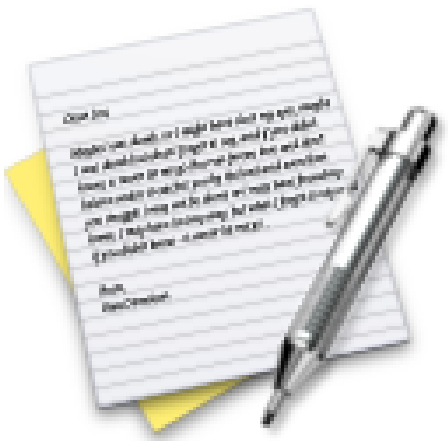
More reliable to use Nmap script with probes like –script=snmp-info

Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Low-level way to identify operating systems, also try/use `nmap -A`
- Send probes and observe responses, lookup in table of known OS and responses
- Techniques known since at least: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

Exercise

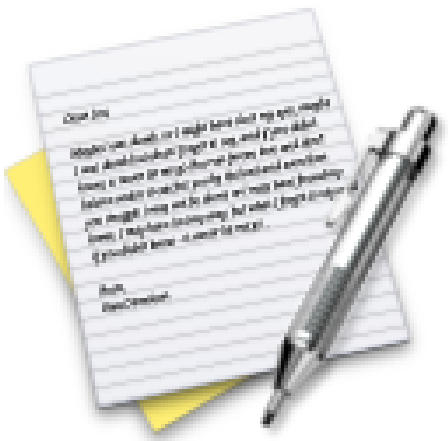


Now lets do the exercise

Discover active systems ping sweep 10 min

which is number 12 in the exercise PDF.

Exercise

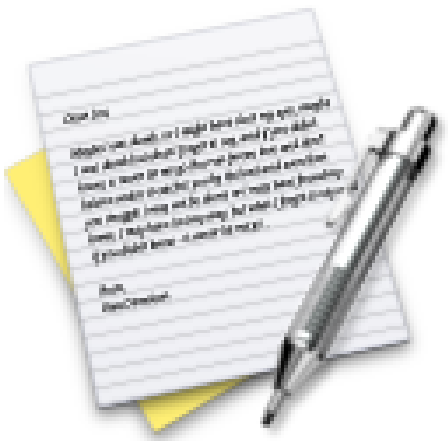


Now lets do the exercise

Execute nmap TCP and UDP port scan 20 min

which is number **13** in the exercise PDF.

Exercise

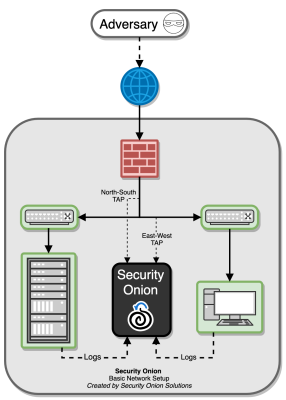


Now lets do the exercise

Perform nmap OS detection 10 min

which is number **14** in the exercise PDF.

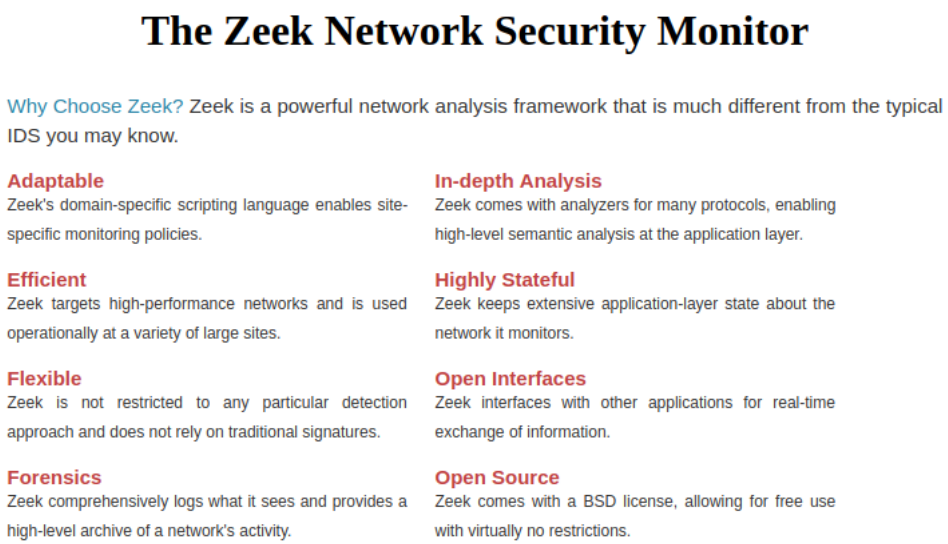
Architecture for packet capture



Source: picture from https://docs.securityonion.net/en/2.3/introduction.html

- Note the terminology North-South – from the internet into the systems
- East-West – horizontal traffic inside the data center
- See also from Security Onion https://docs.securityonion.net/en/2.3/architecture.html#architecture

The Zeek Network Security Monitor



The Zeek Network Security Monitor is not a single tool, more of a powerful network analysis framework. Note: the project was renamed from Bro to Zeek in Oct 2018

Source https://www.zeek.org/

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

http://suricata-ids.org/ http://openinfosecfoundation.org

I often use Suricata and Zeek together

Questions?

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

You are always welcome to send me questions later via email

Mobile: +45 2026 6000

Email: hlk@zencurity.com