Udite 2

jarek.kligl7

June 2024

1 Introduction

Internet - nejvetsi stystem vytvoeryny lidstvem
budeme se snazit vysvetlit ako funguje internet.
Co je to internet (pc sit)?
neni jednoduchy
lze popsat jednotlive casti - jednodusi
skrze jednotlive casti lze snadno popsat co je to sit
budeme popisovat pomoci pojmu sitove infrastruktury

Pocitacova sit - mnozina propojenych pocitacu
historicky nazec, nejsou to jenom pocitace , hostitelsky uzel , konsove systemy ...
muzou byt pripojeny i dalsi zarizeni tablet, mobil, .. tiskarny, skenery
chytra zarizeni .,- zarovky, lednicka ... **IOT** - Internet of things - spojeni i veci co nejsou pocitace
sdileni prostredku a poskytoivani sluzeb

- vypocetni vykon
- pripojene zarizeni
- pristup do site
- software

pocitacova sit obecne

- koncove uzly
  samotne pc
- fyzicky propojeni uzlu (sdilene medium, sitove rozhrani, sitove prvky)
  zarhnuje kabel ale i sitove rozhrani na pc (sitova karta)
  vsechny sitove prvky ktere se nachazeju mezi tema 2 uzlama
- kominikace mezi uzly - **paketovy prenos**
  dulezite bude nas to zajimat

sit - rozhrani mezi pocitacem a venkovnim svetem
sluzba WWW - prohlizeni webovych stranek
emaily

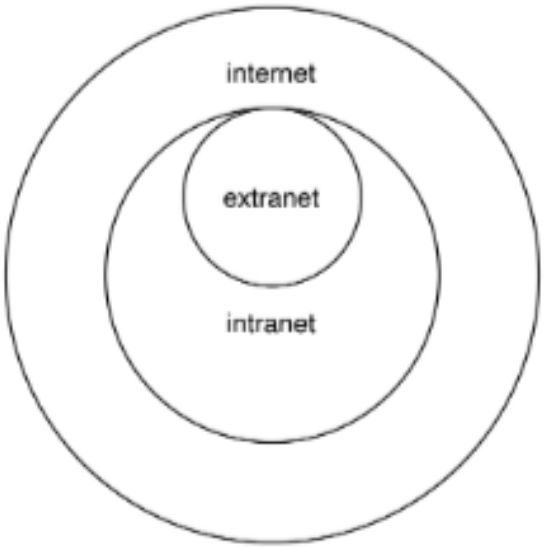


Figure 1: Diagramus

Klasifikace pc siti

1. internet (s malim i)
   - vnejsi sit
   - propojeni vice ruznych sisi
2. intranet
   - vnitrni sit
   - pozadacky na bezpecnost
   - predpoklad ze tam neni nebezpeci
     nezezpeci pochazi z internetu
   - naopak to co posilam z intranetu do internetu je potencionalne nebezpecne
3. extranet
   - cas vnitni site pristupna z internetu
   - router atd ... , pristupovy bod od internetu

Na kazde urovni se pouziva jine bezpecnosti technykusy
duvod rozdeleni: bezpecnost

Klasifikace pc siti (2)

1. dle rozsahu (velikosti)
   - Personal Area Network (PAN)
     do jednotek metru, spojeny s 1 konkretni osobou
     priklad: propojeni telefonu s hodinkami
   - Local Area Network (LAN)
     rozsah do jedne budovy, domaci site, katedra informatiky ma taky lokalni sit
   - Campus Area Network (CAN)
     rozsah do nekolikati budov
     univerzity, firmy s nekolikati budovama
   - Metropolitan Area Network (MAN)
     mestske site, v rozsahu jednoho mesta
   - Wide Area Network (WAN)
     sit Internet , mobilni site
2. dle topologie (propojeni)
   - **hvezdicova**
     jako strom, nejbeznejsi, s**nadna organizace**
     nevyhoda: Centralizace , opadne jeden uzel a rozjebou se uzly vsechny pod nim
   - kruhova
     propojeni do kruhu
   - sbernicova
     mam sbernici ktera je sdilenym mediem
     vyhoda: pokud nejaky uzel zmizi tak se nic nedeje
     nevyhoda: pokud jeden pc komunikuje s druhym tak je to na ukor cele site
     wifi site , sdilene medium = vzduch
   - ...
3. dle prenosoveho media
   - dratova (metalicka, opticka)
     - kroucena dvojlinka
       4 pary navzajem do sebe zakroucenych dratu
       V lokalnich a kampusovych siti
     - opticke vlakno
       svetelna informace
       vyrazne vyssi prenosove rychlosti
       mnohem krehci , kdyby jsme to meli doma tak by sme to asi rozjebaly

- bezdratova (radiovy signal)
  wi-fi , blouetooth, satelitni prenos
  kroucena dvojlinka je rychlejsi

4. dle rychlosti
   vychazi dle prenosoveho media , taky i dle rozsahu mesni rozsah - nutna mesni rychlost

na rucnych urovnich se daji pouzivat jine technologie

Komunikace v pc siti

- Komunikace = zasílání zpráv
  trivialni textove zpravy ktere maji strukturu
- Uzel sítě komunikuje s jedním či více uzly
  - unicast – uzel komunikuje s uzlem
    jeden uzel komunikuje s jednim uzlem
  - multicast – uzel komunikuje se skupinou uzlů
    1 ku n
  - broadcast – uzel komunikuje se všemi uzly v (lokální) síti
    n ku m
    spise technycka role , vimena rezijnich informaci
- Realizace komunikace:
  - přepínání okruhů
    v telekomunikaci
    starsi zpusob, cesta od 1 k 2-hemu, cesta je celou dobu udrzovana
    vyhoda: mam to porad k dispozici
    mam zajistenou kapacitu toho pasma
    nevyhoda: je tam i kdyz neni potreba
    dva pc komunikuji v "jedne" ceste takzde kazdy ma k dipsozici 50 procent
    degradace prenosove kapacity
  - přepínání paketů (Internet)
    nevyhrazuje konkretni cast , ale rozdeluje spravy na mensi casti (pakety), ty pakety se posilaji pak po siti
    vyhoda: vyuziti cele kapacity prenosoveho media
    nevyhoda: pokud sit hodne zahltim , tak dojde k degradaci
- Poznámka: pojem paket budeme používat nepřesně
- Obecně složitý proces → dělení na menší části
  abstrakce nad celym systemem
  casti o sobe nemusi vedet a bude to fungovat

Prenos dat

- Parametry:
  - rychlost
  - spolehlivost
- **Zprávy jsou rozděleny na pakety**.
- Pakety (fyzicky) **přenášeny po bitech**.
- Metoda uloži a odešli:
- pakety se posilaji az jsou v celku (ale pak se poslou po bytech)
  - Dokud neobdržíme celý paket, data ukládáme do bufferu → zpoždění zarizeni by nemuselo mit ani informace co s timi daty ma delat proto cekaji na cely paket tam jsu i informace o tom kam to ma dorazit
  - Více zdrojů = fronta → zpoždění
  - Zaplnění fronty = ztráta paketu
    fronta nema nekonecnou kapacitu
    dochazi k tomu dost casto
- Odbočka: zpoždění šíření - singal degraduje po case musi se opakovat, zpoždění zpracování, ...

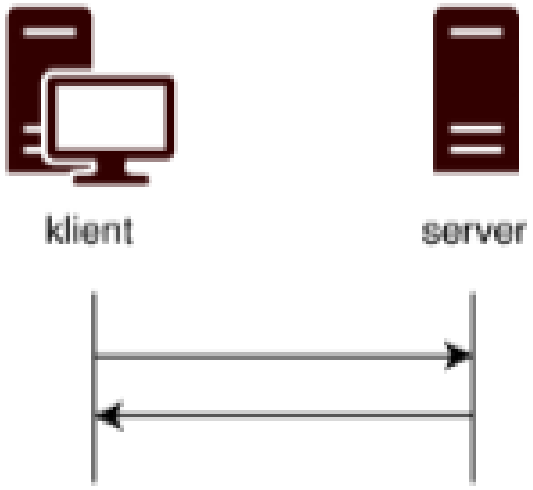


Figure 2: Klient server

Architektury sluzeb v pc siti

klient server
klient zada server o poskytnuti sluzby
nerovnocene role - klient zada o poskytnuti zdroju, server je dodava (server je ten nadrazeny)
bezne : 1 server n klientu
centralizace - slabe misto
proxy server = prostredek mezi klientem a servrem
klient → proxy → server
klient se zepta proxy servery ten se zepta servu tu informaci pak uz ma a muze ji predavat a chovat se jako server
na 1 proxyserver muze byt n klientu
pouziva se to pro odlehceni klient-server archytektury
proxi-server muze zprostredkovat anonimitu - VPN je proxy server
napr. prohlizeni webove stranky
Dos, DDos , velka skupina zahlcuje centralni server
pad serveru
V OS jsou demoni ty servery ktere poskytuji sluzby a mi je o ne zadame (treba sluzba vzdaleneho prihlaseni)

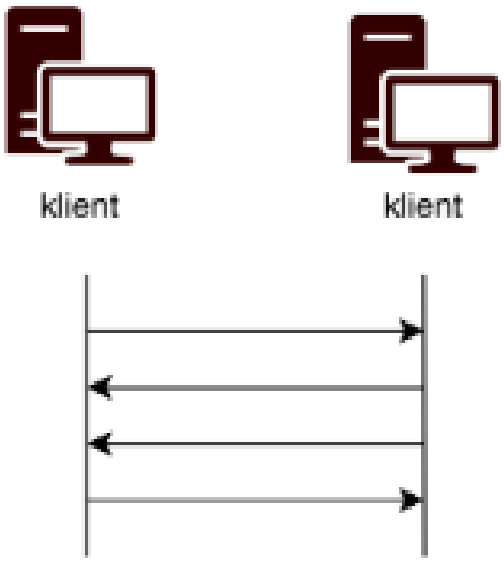


Figure 3: peer-to-peer

peer-to-peer (P2P) se servrem (hybridni) i bez nej
server udrzuje jenom seznam uzlu
rovnocene role uzlu
muze kdokoliv zacit komunikaci s kymkoliv
decentralizace - cim vic uzlu je v siti tim vic je ta sit robustnejsi
napr. sdileni souboru pres tzv. torrent site
stahovani obsahu jak uz legalniho tak nelegalniho
skype byl drive P2P

2 TCP/IP architektura

Sitovy model
Abstrakce nad procesem komunikace
Rozdělení na menší části tzv. vrstvy (obecný designový princip)
abtrakce je dulezita v tom ze to muzeme udelat ve vnitr pak uplne jinak a z venku se nic nezmeni
program nezajima jestli data pujdou po dvojlince nebo wifine

- Vrstva:
  - poskytuje služby vyšší vrstvě
  - používá služeb nižší vrstvy
- Vrstvy popisují různé části komunikace.
- Nejběžnější modely:
  - OSI (abstraktní, referenční)
    nikdo to nedela moc ale je to mozny
  - TCP/IP (Internet)
    bezne i Internet
- Abstrakce:
  - Abstrakce je klíčová.
  - Vrstvy jsou nezávislé → robustnost (implementace vrstvy je nezávislá na ostatních vrstvách).

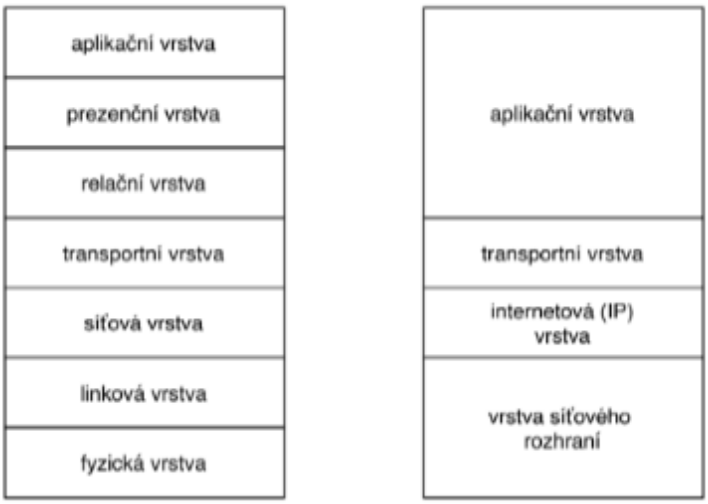


Figure 4: Enter Caption

V levo OSI - 7 vstev
TCP/IP - nejake vrstvy spojuje do 4 vstev
maji mezi sebou korespondenci
da se rict ze TPC/IP archytektura je implementace OSI
Vrstvy mezi sebou komunukiji
pouze "sousedni vrstvy" muzou komunikovat

protokol
Vrstvy jsou tvořeny protokoly.

Protokol = množina jasně daných pravidel.
presne definovany co se ma dit kdyz se neco deje, co se nema dit

Analogie protokolu v lidské komunikaci (např. "dobré chování").

Komunikace pouze mezi sousedními vrstvami.
benefit abstrakce - nemusi aplikacni vrstvu zajimat co dela interentova, nebo sitoveho rozhrani
Standardy a standardizace:
potreba unifikace
to je jak kdyz se potka slovak z francouzem rozumi si picu nechtene!!
Internetové síťové standardy – RFC (Request For Comments), dostupné na `https://www.rfc-editor.org/`
budeme popisovat to co je v tech standartehc

2.0.1 TCP/IP

Transmission Control Protocol/Internet Protocol
pocitacova sit → TCP/IP architektura
TCP/IP se deli na 4 vrstvy

- aplikacni
- **transportni**
- **interentova**
- sitoveho rozhrani

Figure 5: Enter Caption

komunikace Analogie: poslání zprávy mezi aplikacemi na dvou počítačích = poslání dopisu (zpráva) obyvatelem (aplikace) jednoho domu (počítač) obyvateli (jiná aplikace) jiného domu (jiný počítač).
clovek chce poslat zpravu co bydly v dome a chce poslat zpravu jinemu clovekovy v jinem dome
dum = pc
lide = aplikace
musime zavest adresu, format dat

Potřebujeme zajistit (zjednodušeno):

- formát vyměňovaných dat
  infrastruktura ma omezeni , A0 obalka nemuzeme poslat, ceska posta nema tu infrastrukturu
  musime popsat jak ta zprava bude vypadat
- identifikaci (adresaci) komunikujících aplikací
  musim zajstit aby ty data co chtel emailovej klient dostal emailovej klient
- adresaci uzlů v síti
  musi byt jasny kam to chci poslat
- identifikaci konkrétních síťových rozhraní
  konkretni sitova karta (mame vchod ze predu i vchod ze zadu)
- přenos dat skrze síť
  v jake podobe ty jednotlive data pujdou

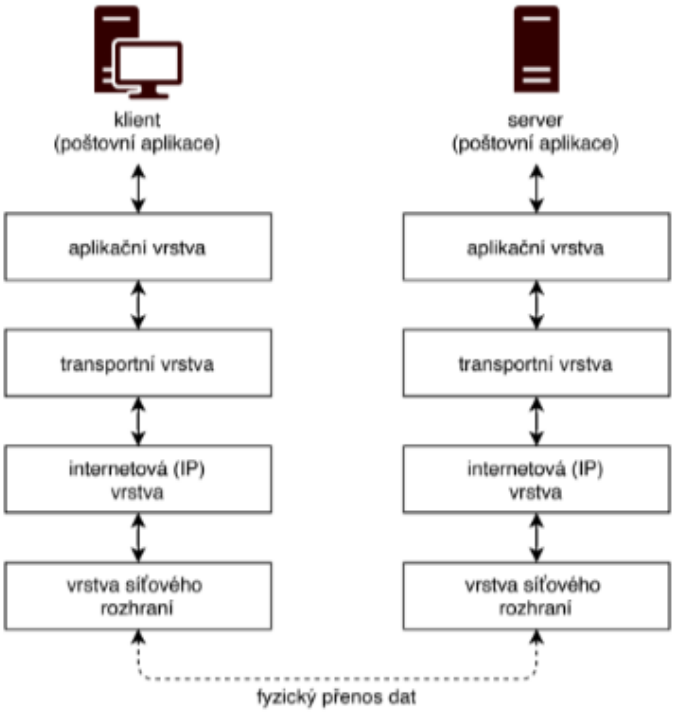


Figure 6: Enter Caption

aplikacni vrstva - resi podobu sprav
transportni vrstva - resi identifikaci a poslani dat, zpusob prenosu
internetova vrstva (ip vsrtva) - adresace v ramci site
vsrtva sitoveho rozhrani - samotny fyzycky prenos dat

pomyslne spojeni mezi stejnyma vrstvama (abstrakce) - aplikacni s aplikacni atd

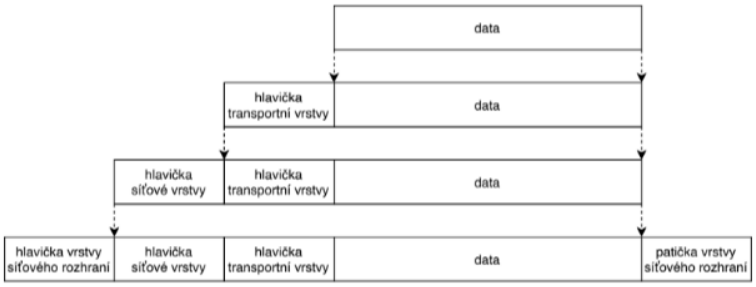


Figure 7: Enter Caption

Komunikace mezi vrstvama hlavicka a paticka = data potrebna pro funkci dane vrstvy
"baleni" a "vybalovani"
na koncovych uzleh **i sitovych zarizenich**
sitove zarizeni nemohou sahnout na hlavicku transporni vrstvy aplikacni vrstva vyproduke data → dostane je transportni vrstva a prida si k tomu rezijni informaci so potrebuje pro sebe → ... → vrstva sitoveho rozhrani prevezme data od sitove vrstve a prida k tomu jak hlavicku tak paticku

3 Aplikacni vrstva

aplikacni protokoly popisuje format (podobu) vymenovanych dat a dalsi
aplikacni protokol = konkretni sluzba

- HTTP(S)
  vymena webovych stranek
- DNS
  Preklad domenovych jmen
- ...

Kazdy z nas jako programatori si muzeme udelat vlastni protokol
popiseme konkretni podobu zpravy jak bude vypadat
kdyz ja pisu program ktery chce komunikovat ze siti potrebujeme API - **SOCKET API** poskytovano OS
jako programator staci nastudovat jak funguje toto API Resi bezpecnost (ostastni vrstvy pouze okrajove)

- TCP/IP puvodne neresila bezpecnost vubec
  puvodne se neprepokladalo ze tam muze byt neco nebezpecneho

- dodatecne "zaplatovano"
- internet je nebezpecny

Priklad emailovy - klient

4 Transportní vrstva TCP/IP architektury

predavani dat mezi jednotlivimi aplikaci (identifikuje aplikaci v ramci uzlu)
port (identifikace)

- cislo 0-65535
- $\leq$ 1023 vyhrazeno pro konkretni konektivitu (privilige)
  pod 80 je port webove sluzbe (doporucene ale nikdo nas nenuti)
- pokud chci napsat vlastni aplikaci tak je pro nas zbytek tech portu az na ty priviligovane

cast socketu je ten port , os ma seznam portu a prideli to aplikac
neco bude pouzivat port 80 , zazadam OS o port 80 , OS odpovi tenhle port je jiz pouzity a nepovoli mi to
dokud je port pouzivan tak je blokovan ten port (je navracen OS)
jedna aplikace muze pouzivat klidne vice portu
sluzba FTP (pro vymenu soubour)- pouziva 2 porty, jeden pro prenos dat a druhy pro rizeni
dva typy sluzeb:

1. TCP (transmission Control Protocol)

2. User Datageam Protocol (UDP)

TCP i UDP identifikujeme pomoci portu , kazdy ma svoje porty: timpadem muze teoretycky bezet 2 x 65535 aplikaci co vyuzivaji sirtovou jkonektivitu
znaceni cislo portu/tcp

Protokol TCP Data ve formě segmentů → segmentace dat.
data vezme a rozdeli je na mensi kusy (segmenty)
Spolehlivá spojová služba:

- navazuje a udržuje spojení mezi uzly (režie, potvrzování) → spojení musí být ukončeno - spojovost
- zajišťuje doručení dat (řeší ztráty segmentů, potvrzení přijetí segmentu a další) - spolehlivost

Klient-server architektura
klinet posle data a server posle ja jsem ty data prijal (rezijni informace potvrzeni ze jsem ty data prijal) - diky tomu se zajisti ze se ty data poslou znovu pokud neprisli
s potvrzenim muze poslat i nejaka data klient zadata o webowou stranku a server spolu s tim potvrzenim posle i informace o webove strance

- zajišťuje řízení toku sítě
- zajišťuje integritu dat → kontrolní součet
  tohle se jedna o kontrolu ale ne o bezpecnost
  kazdy si muze ten kontrolni soucet udelat sam a pozmenit si to at to sedi predchazi se poskozeni z prenosu

Hlavička protokolu: zdrojový a cílový port- adresa aplikace kde to musi byt ulozeni, číslo segmentu - semgenty jsou cislovany abych vedel do jakeho poradi je mam poskladat, číslo potvrzeného segmentu, příznaky (a další) - jestli se jedna o zahajeni komunikace, potvrzeni (to se nachazi v te hlavice)

segmentace
vezmu data rozsekam je do mensich dat a kde pridam tu hlavicku

Protokol UDP
Data ve formě datagramů (nutnost manuálního dělení na aplikační vrstvě).
dela to programator
Nespolehlivá nespojová služba:

- nevytváří spojení
- nezajišťuje doručení dat
  nevim jestli dojdou nebo ne
- nelze řídit tok dat

Nízká režie.
zadna kontrola dojiti
Hlavička protokolu: zdrojový a cílový port (a další) ale moc toho tam neni.
Potrebuji takovou sluzbu ???
ano - treba stream nedava smysl zobrazit ten obraz zpatky
pocitacove hry

Navazani spojeni (TCP):
Klient posle serveru segment ktery ma priznak SYN + nahodne vygenerovane cislo X
server odpovi s priznakem SYN + Jine nahodne cislo Y , potvrzeni urceno priznakem ACK X + 1
klient potvrdi segment s priznakem ACK Y + 1
.
Tri fazovy hand shake

spojeni smaotne kdyz uz je navazano: pak posilame zpravy s treba s cislem Z a server posle zpatky Z+1

Ukonceni:
Klient pouzije priznak FYN, server potvrdi priznak FYN
Server posle priznak FYN, je zvykem a slusnosti ze Klient mu to potvrdi (ale je to sumak)

ctvir-fazove rozlouceni

5 IP vrstva TCP/IP architektury

Identifikace uzlů v síti → IP adresa.
kazdy uzel musi mit globalne nejakou identifikaci

Směrování mezi nesousedními uzly **(skrze internet)**.

Data se přenáší ve formě (IP) paketu. - hlavicka IP vsrtvy

Služební protokoly pro hlášení chyb a diagnostiku (ICMP).

IP adresa
IP adresa je uložena v hlavičce IP protokolu.
Musi tam byt ulozena jak ip adresa odesilatele i prijemce
ip adresu musi mit vsechny zarizeni v siti
IPv4 (32 bitů) - starsi, vice pouzivana
IPv6 (128 bitů).
lisi se protokolem, hlavne se lisi **DELKOU ARESY**
Příklad (phoenix.inf.upol.cz):

- 158.194.80.13
- 2001:718:1401:50:0:0:0:0d, zkrácený formát 2001:718:1401:50::0d

To rozdeleni po 8 bytech je jenom at se to lepe lidem pamatuje jinak je to v pc
32 bytu vedle sebe
255.255.255.255 - nejvetsi mozna ip adresa

budeme to tady vysvetlovat na IPv4

Internet je síť sítí → hierarchie.

Lokální adresy (používané v lokálních sítích) a veřejné adresy (ostatní).

IP adresa sítě a IP adresa uzlu:

- logické a praktické rozdělení
- hierarchické směrování

Maska sítě = rozdělení na adresu sítě a adresu v síti (adresa síťového rozhraní).
32 nebo 128 bytove cislo
obsahuje jednicky z leva do nejakeho bodu v pravo a pak to pokracuje nulami:
$[1][1][1][1][1][0][0][0][0][0]..[0]_{32}$
Příklad:

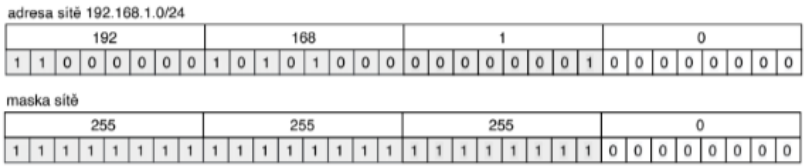


Figure 8: Enter Caption

- adresa sítě: 192.168.1.0
- maska sítě: 255.255.255.0
- adresy v síti: 192.168.1.1 – 192.168.1.254
- 192.168.1.255 vyhrazena pro broadcast

1. Vezme se adresa site a maska site

2. provede se logicky soucin ($\wedge$) ip-adresy site a masky site

tou maskou nechame prostor na nejakou "lokalni sit"
pri masce 255.255.255.0:
nejmensi adresa je adresa site jako celku
kdyz jem max (255) - broadcastova adresa

Používanější CIDR (Classless Inter-Domain Routing) formát: 192.168.1.0/24. udava pocet jednicek - 24 = 255.255.255.0 Maska rozdeluji adresu na netwokvou cast a hostovou cast

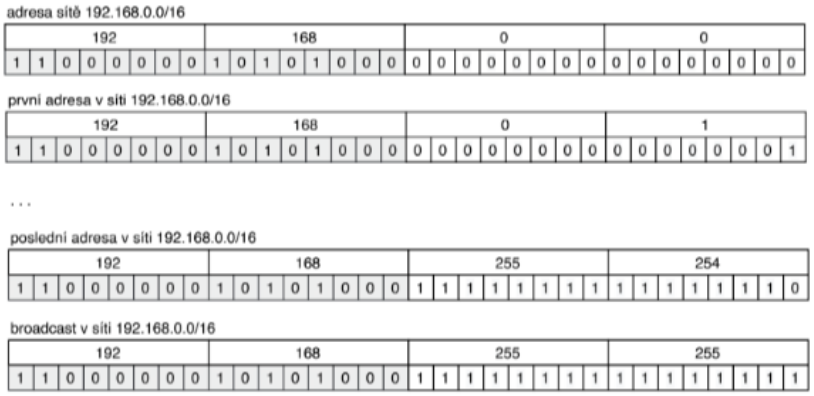


Figure 9: Enter Caption

Princip tvorby podsiti

Sítě lze dále dělit na podsítě.

Sítě lze spojovat do větších sítí (agregace).

Manipulace s maskou sítě. - prida se cast na adresu podsite
pri defaultni masce 255.255.0.0 muzeme upravit masku na 255.255.192.0 a tim rozdelime sit na 4 podsite

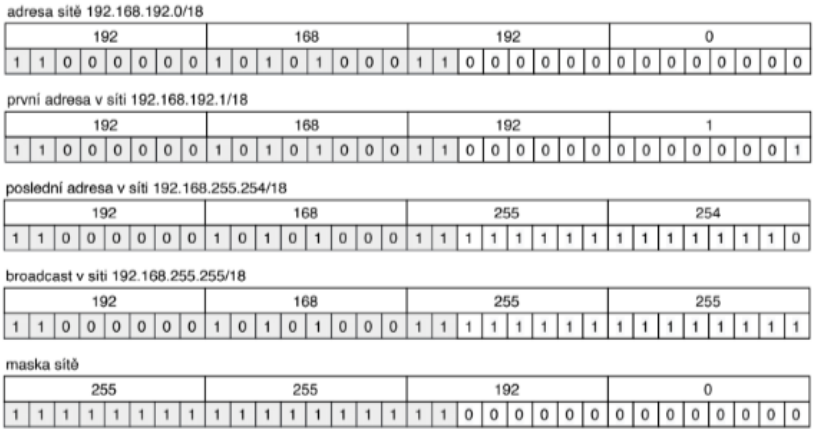


Figure 10: Enter Caption

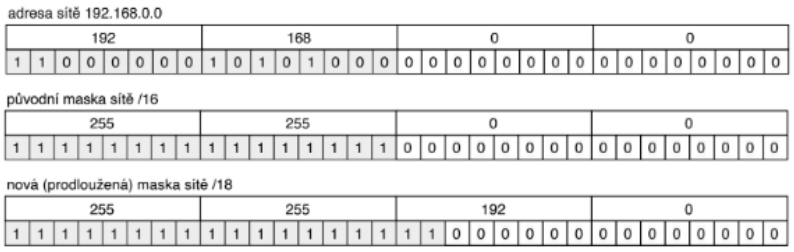


Figure 11: Enter Caption

IP adresa	popis
127.0.0.1	zpětná smyčka (loopback)
10.0.0.0/8	adresa lokální sítě
172.16.0.0/12	adresa lokální sítě
192.168.0.0/16	adresa lokální sítě
192.168.0.0/24	adresa lokální sítě

Figure 12: Enter Caption

Specialni IP Adresy

loopback - chceme poslat informaci sami sobe (localhost) : mame k dyspozici fucking 16 milionu adress xddd, protoze maska loopbacku je 255.0.0.0
Lokalni site- neboli private ip (kdo vi ten vi kdo nevi googly on to ani moc nevysvetlovat)

Omezeni IPv4
je jenom 2^{32} IPv4 asress , pro lokalni site dostatecne

- Internet Assigned Numbers Authority (IANA)
  vlastni vsechny ip adresy, uvolnuje je podregistrum
  on uz nema IPv4 Adresy
- Regional Internet Registry (RIR)
  tady jiz tady dosly taky, jedine kde jeste jsou sou v africe organizace pro EU
- Provideři

IPv4 adresy již došly (na několika úrovních).

IPv6:

- obtížně zapamatovatelné
- IP adresy vnitřní a vnější sítě lze oddělit - (neni nutnost IPv6)**(NAT)**
  oddeleni vnitrni site od venkovni , ty lokalni mame doma a verejnou ma domacnost vetsinou jenom jednu , (router) ten si to preklada a usmernuje
- poskytovatelé neinvestují do infrastruktury

Poznámka: IPv6 nepoužívá masku, ale délku prefixu (zkráceně prefix), jinak stejné.
Nepodstatne pro nas ale v sitich to pak asi bude

Prideleni IP adresy uzlu

1. staticke
   - manualni konfigurace
   - v topologich co se nemeni treba router doma
2. dynamicke
   - DHCP protokol
     dinamicke prideleni adressy (ip adresy a subnet masky)
   - klinet-server sluzba
     v domacich siti to dela router, klient se zepta jestli je v siti DHCP protokol, server odpovi ano jsem tu uwu, tu mas ip a masku
   - server zasle uzlu udaje pro konfigurace sitoveho rozhrani

6 Vrstva síťového rozhraní TCP/IP architektury

zajmava pro lidi co se chcou zaajimat o HW, ne pro nas ale musime si to popsat

Řeší fyzický přenos dat a přenosová média.

Linková část (přenos v rámci LAN pomocí rámců) a fyzická část (přenos signálu po jednotlivých bitech).
to co prijde od IP vrstve tak se ty data pak zaobali do Linkoveho rance, adresace v lokalni siti
Různé typy přenosu (analogový, digitální).

Identifikace fyzického rozhraní: **MAC adresa**.
na svete by nemeli existovat 2 zarizeni ktere maji stejnou MAC adresu
cast adresi je pridelena na jednotlive vyrobce, a ten si to rozdeluje aby nebyly 2 stejne
Například 01:23:45:67:89:ab, lze změnit. (hexadecimalni cislice)
muzu si to menit softwarove abych treba mohl maskovat po sobe stopy kdyz jsem hacker
nebo kdyz mam pristup nekam po moji mac adresou pak mi zhori sitova karta tak az si koupim novou tak si tam dam tu moji puvodni mac adresu
Přenosové médium (fyzicka cast):

- kroucená dvojlinka (Cat 5e, Cat 6, Cat 6a, Cat 7 a další, **konektor RJ45 - vypada to jako kostka cukru (takova mensi ochuzena)**)
  lisi se to konktretnim standartem , a prenosover rychlosti
  zajisteno lepsim stinenim vetsi mechanicke odolnosti
- optické vlákno
  mnohonasobne drazsi
- prostor (WI-FI)

Struktura Pocitacove site

- Uzly site
  pocitac na ktrem je OS
- Prenosove medium
- switche
- huby
- repeatry
- bridge

- routery
- modemy
- ...

Bridge (most)

ma vstupni porty, premostuje 2 libovolne sitove rozhrani
jakykoliv PC co ma 2 sitove karty se muze chovat jako bridge
(Spojuje 2 site)

HUB (rozbocovac)

Jakakoliv informaci ktera tam prijde tak jde automaticky na vsechny porty ktere jsou pod nim
Vzdycky to posle na vsechny
nebezpeci odposlechu !!!!
nepromiskujitni rezim - ten defaultni
kdyz zjisti ten uzel ze ta informace neni pro me tak ji zahodi promiskujitni rezim sitoveho rozhrani - bere si vsechny informace
muzeme pak poslouchat vsechno co se na te site deje

Switch

rizene odboceni komunikace na bazi MAC adressy
lze to nastavit, switch se to sam nauci na jakem portu je jaka MAC adresa
switch se v prvnim okamziku chova jako hub a ty uzly mu odpovi a tim zjisti jaka je jaka MAC adresa
Udrzuje tabulku MAC adress

Router (smerovac)

obsahuje obvykle switch, hub, bridge
rizeni na zaklade IP adressy + mac adressy
umozneni smerovani mimo lokalni sit
jak poznam ze posilam neco mimo sit??? - s masky site a adressy!!

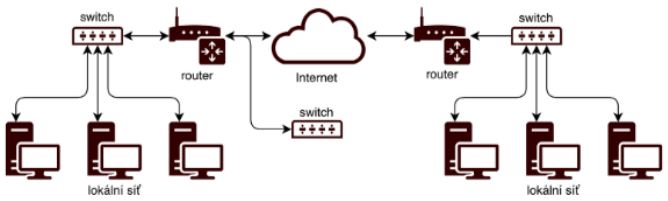


Figure 13: Enter Caption

komunikace v siti
Data - popise aplikacni vrstva
smerovani v lokalni siti

- mam pocitac ten ma IP Adresu
- kdyz chci nekam poslat musim znat IP Adresu 2. pocitace
- o smerovani se stara Sitova Vrstva (Linkova vrstva)
  ta ale vi jenom o MAC adrese
- ARP protocol - Pc se zepta kdo ma Ip adresu at mi rekne svoji MAC adresu
  posle to vsem na Localni siti - staci mi bohate switch
- IP-adresa je pouizita pro logickou indexaci, ale pri samotnym smerovanim je pouzita pouze MAC adresa

smerovani mimo lokalni sit:

- nutne potrebujeme IP vrstvu
- nutne potrebuji Linkovy ramec a ramec IP vrstvy
- na zaklade IP adresi jsem schopen urcit ze posilam mimo lokalni sit
- **next-hop** kdyz nevim tak to posilam nekam (do gate nadsite)
  do extranetu
- **smerovaci-tabulka** - pekna analogie je letiste vystoupim z letadla kouknu se na tabuli kam mam jit a letim dal
  informace: jenom od kud to prislo a kam to ma jit
- staticka smerovaci tabulka - v ramci lokalni site
- dinamicka smerovaci tabulka - sit se nauci sama ty cesty

Pripojeni pocitacu do lokalni site

Fyzicke propojeni - router , kabel ..
stejna adresa site - ta cast pod tou maskou site musi mit stejnou IP
ruzne MAC adresy
pristup k internetu , musi mit nastavenou gateway (vetsinou router)
preklad domenovych jmen

Lokalni site

FireWall

- **Filtrace sitove komunikace**
- bud na zaklade IP adresy
  zablokujeme nejakou IP firewall zahodi tu informaci a k uzivateli se nedostane
- na zaklade cisla portu
  muzeme treba povolit jenom port 80, nebo to jde delat sofitikovane: na zaklade vymeni segmentu treba kdyz mi prijde packet s priznakem SIN atd...
- obvykle soucast OS, pripadne specialni zarizeni

Nejbezpecnejsi lokalni sit nepripojovat vubec k internetu (u Policie)
ale muze se stat ze uklizecka prinese sussy USBcko ale s tim nejde nic delat
NAT - preklad sitovych addres
mame (internet) - (router) - (intranet)
soucasti routeru je ta NAT sluzba
pozmeni hlavicku ip protocolu , router ma verejnou ip adresu , zameni adresu vnitrni site za hlavicku verejne site
diky tomu muzeme recyklovat ipv4 adressy (ty lokalni) , taky zajistuje to ze nevi nikdo ako mame nastavenou vnitnrni sit (dojem bezpecnosti)
i zpatky to funguje
Velkou roly v tom hraje TCP prtotocol - muzeme povolovat jenom konverzaci ktera byla zahajena
Bezpecnost NATU jde obejit ale je potreba nejaky inpulz z vnitrni site prvne treba uklizecka ze SUSSY usbckem

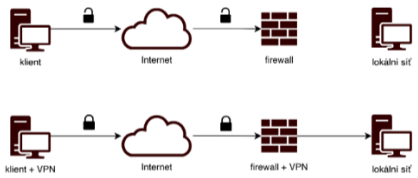


Figure 14: Enter Caption

VPN (virtual private Network)
Zpusob jak pripojit klinetu do vnitrni site mimo z te vnitrni site
dost casto je vyhodne aby uzivatel mel z pc pristup k infrastrukture lokalni site

Šifrované propojení sítí či klienta a sítě skrze nebezpečnou síť.
VPN je software na strane Klienta ktery zasifruje tu komunikace

Klient je součástí lokální sítě → výhody.

Komunikace je šifrována (nikoliv anonymní).
jsem schopny zjistit kdo se tam pripojuje (na zaklade IP adresy)
Vlastní, případně řada poskytovatelů (pozor na bezpečnost).
on poskytuje sifrovani dat , ale on si je schopny desifrovat

7 Konfigurace Wi-Fi routeru

WIFI (tohle asi patri i do predchoziho tematu)
WLAN - wireless local area network
z pohledu TCP/IP - Vrstva sitoveho rozhrani
jiny typ ramce
sdilene medium - vzduch (radiovy signal)
sbernicove medium

- problem s kolizemi - muzeme to zahltit
- runze metody reseni - minimalizace skody
- odmlceni na nahodnou (kratkou) dobu (periodicky zapinani a vypinani)

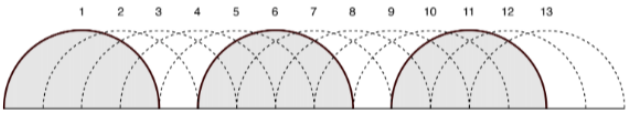
protokol: 802.11 ruzne verze (napr b,g,n,ac,ax) rychlost, parametry site, podpora zarizeni
udava ze se jedno o bezdratovy router
rychlost , bezpecnost
Chi to nejnovejsi protoze rychlost a bezpecnost ALE zpetna podpora zarizeni

Bezny nastaveni WIFI routeru
router = Acces point (AP)
bezdratove sitove rozhrani
bezna zarizeni
ruzna kvalita, ruzna cena - i levnejsi zarizeni umi toho hodne
pocet klientu - nejdulezitejsi faktor
zakladni Wifi-routery → rozsahle nastaveni

- jmeno site
- parametry site (prenos, sifrovani)
- dynamicka konfigurace (DHCP server)
  prideluje ip adresy za nas
- firewall
  odfiltrovani venkovni komunikace
  zablokovani MAC adressy

Nazev site
SSID - jmeno site (treba DomacisitJarmili69)
nazev site jde skryt , uzivatel musi znat, aby se pripojil (moznost hide SSID)
Skryte SSID neni zabezpeceni

velice jednoduse jde zjisti skryte jmeno site



Obrázek: Rozložení kanálů v 2.4 GHz.

Figure 15: Enter Caption

Parametry site (fyzciky prenos) Pásmo:

- 2,4 GHz - nejbeznejsi pasmo, 5 GHz - novejsi , 6 GHz - nedavno standartizovana
- vyšší frekvence = rychlejší přenos, menší dosah, náchylnější na rušení
- Stnadardy musi projit homologaci - prislusny urad v zemi poda povoleni k pouzivani
- vyzsi frekvence hure prochazeji zdemi (Kompromis, zalezi na prostredi)
- vyzsi frekcence jsou ruseny pocasi

pasmo , je rozdelene na kanaly
pocet kanalu je zavysle na zemi
V Japonsku 14 kanalu, v USA 12

Kanál:

- počet kanálů závisí na zemi
- 2,4 GHz, 13 **překrývajících** se kanálů
  v celym pasmu jsou jen 3 kanaly co se neprekryvaji
- 5 GHz, (CR) 25 **nepřekrývajících** se kanálů

Výběr → chceme volný kanál, nepřekrývající se kanál, kanál s co nejméně AP.
pokud je moc wifi siti na jednom kanalu dochazi k ruseni

Šířka kanálu: 20 MHz, 40 MHz, 80 MHz (5 GHz), 160 MHz (6 GHz), větší šířka → větší propustnost, některé zařízení nemusí podporovat.
kdyz nastavim vetsi sirku tak dojde k vice prekryvum

Výkon vysílače (ne vždy lze ovlivnit).
tpl-link bezne to umi
cim vetsi vykon tim muze dojit k vice kolizim

Signál/šum (jednotka -dBm, 0–100), typicky: -60 dBm / -90 dBm, čím blíže 0 tím lépe (u šumu naopak).
dBm - decibely na milivat cosi (nepodstatne)
degradace sygnalu

Kvalita signálu (SNR) rozdíl mezi signálem a šumem (jednotka dB): 40 dB a více kvalitní signál (čárky na ikoně).
neni mozne dosahnout naprosto idelani hodnoty - router rusi sam sebe

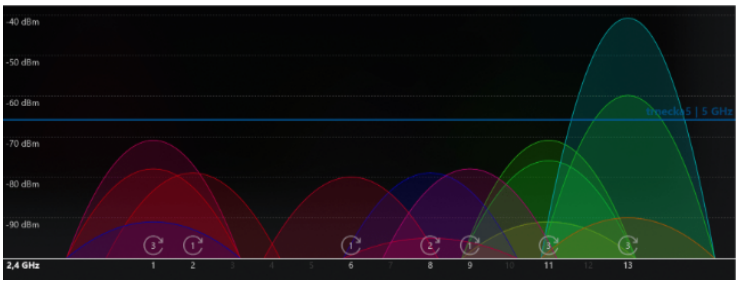


Figure 16: Wifi site v pasmu 2,4 GHz

Ukazka
Wifi-Analuzer (Windows)
rada nastroju pro ruzne OS (Windows, Linux, macOS, Android, ...)
specializovany hardware - presnejsi

Parametry site (bezpecnost) Šifrování:

- žádné (veřejné Wi-Fi) → velmi nebezpečné
  kdokoliv muze komunikaci odposlechnout, rade hezkuch utoku od zahlceni po ukradnuti informaci
- WEP → prolomitelné = nedostatečné
  uz je skoro nenabizene, je v nem matematycka chyba , statistickym utokem se za to heslo prolomit
- WPA → bezpečnostní problémy, lze prolomit slovníkovým útokem
  radove par minut za predpokladu ze mame heslo ve slovniku
- WPA2 → bezpečnostní problémy, lze prolomit slovníkovým útokem
  bezpecnostni standart (defaulni u vetsiny , jinak to jsou retardi), jde to hur prolomit ale stejne jde
- WPA3 → malá podpora, bezpečnostní problémy
  v okamziku kdy bylo zverejnene tak do 14 dny to bylo 2krat ruzne prolomeno pak se to fixlo ale jeste to neni tolik ozkousene

Heslo - zrovna jaka sifra je pouzita:

- TKIP (WPA)
- AES (WPA2)

lze to zamenovat ale neni to dobry, nejlepsi je AES
Autentifikace:

- PSK (heslo)
  predzdileny klic, musime to heslo rict nekomu
- EAP (autentifikační server, obvykle firemní infrastruktura, některé Wi-Fi routery nepodporují)
  uzivatel musi mit vlastni jmeno a heslo
  mnohem bezpecnejsi ale doma to clovek nevyuzije
  potreba autentifikacniho serveru (jeden pc ktery se stara jen o prihlasovani a odhlasovani)

WPS

Tlačítko na Wi-Fi routeru (ze zadu nebo z boku):
zjednoduseni pro bezne uzivatele

Automatické připojení do Wi-Fi sítě pomocí PIN.

Velice nebezpečné (zejména u starších routerů) → lze odposlechnout a prolomit.
zlomeni PINU hrubou silou (+ dost casto je tam chyba ktera to jeste zjednodusi)

Jak Vylepsit Signal?

- opakovace - specialni zarizeni (acces point)
  poslouchaji signal na ktery je nastavima a pak ho opakuji
  potreba delat s rozumem opakovanim signalu nastavaji kolize
  musi bezet na stejnem kanale
- roaming
  propojeni dvou acces pointu do unifikaniho signalu, navzajem si predaji informaci o tech uzivatelych
  musi mit vsechny pristup do internetu
- mesh
- kabel
  kabel ma lepsi prenosove vlastnosti na ukor mobility, neni nejak extra rusenej
- elektrycke rozvody
  jenom na novejsich rozvodech - hlavni pojistky to utnou , neni mozny se dostat pres proudovy chranic (pica nejsem fyzik k cemu mi to je ja jsem rad ze jsem se jeste nezabil tou elektrinou)

8 Systém DNS

IP adresy:

- obtížně zapamatovatelné
- **zachycují fyzickou strukturu**

Logická struktura → doménové jméno.
lepe zapamatovatelne, ale pouziva se IP adresa a Mac Adresa
Příklad: `phoenix.inf.upol.cz`
Služba DNS (soucast aplikacni vrstvy):

- překlad doménového jména na IP adresu (a obráceně, bezpečnost)
- `phoenix.inf.upol.cz` → 158.194.80.13
- decentralizovaná služba (systém DNS)
  existuje milion severu po celim svete
  kdyz by existovalo jenom jedno misto tak v moment vyrazeni by prestal fungovat internet (kind of, bezny uzivatel nezna ip-adresu fb, dokonce jich exituje vice)
- řeší **resolver** (součást OS), který předává řízení DNS resolver serveru
  uzivatel se zepta OS - ten bud vi nebo nevi pokud nevi zepta se DNS resolver serveru

Struktura: standardně ASCII znaky, omezená délka, oddělovač: `.` (tečka), běžně: 1. řádu, 2. řádu, ...
podle tecek se oznacuje rad domeny
je tam i tecka na konci (korenova domena (0 radu) - ale nepise se je tam automaticky
Nákup doménových jmen. - pronajime si ji na nejakou dobu

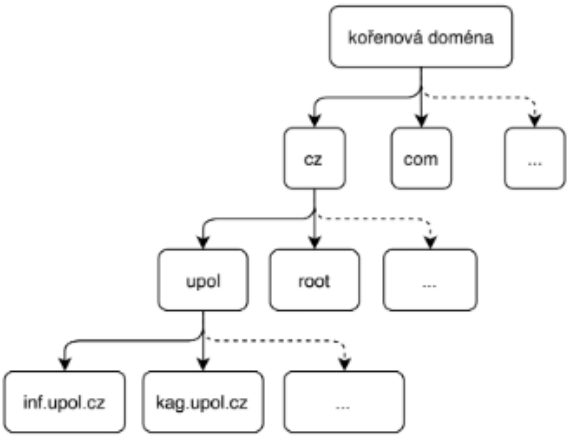


Figure 17: Enter Caption

Hiearchye domenovych jmen domena (zona) spravovana name serverem pocitac v siti jenz udrzuje informace o existujicich domenach 2 radu jenz se tam nachazeji
Vyhrazena (genericka) domenova jmena: edu - vzdelavani, com, gov - vlada, org, info
lze koupit jen volna domena

DNS servery Primární:

- každá doména má právě 1 primární server
- autoritativní odpověď o dané doméně
  zkutecne ma tu informaci o tom ulozenou

Sekundární:

- záloha primárního
  umisteny na ruznych mistech aby kdyz treba vybouchne ta mistnost tak ho to neposkodi
- každá doména má alespoň 1 sekundární server
- autoritativní odpověď o dané doméně

Cache:

- často součástí primárních a sekundárních, ale mohou být i samostatné
- neautoritativní odpověď
  informace je zastarala mozna
- zrychleni prekladu dramaticke

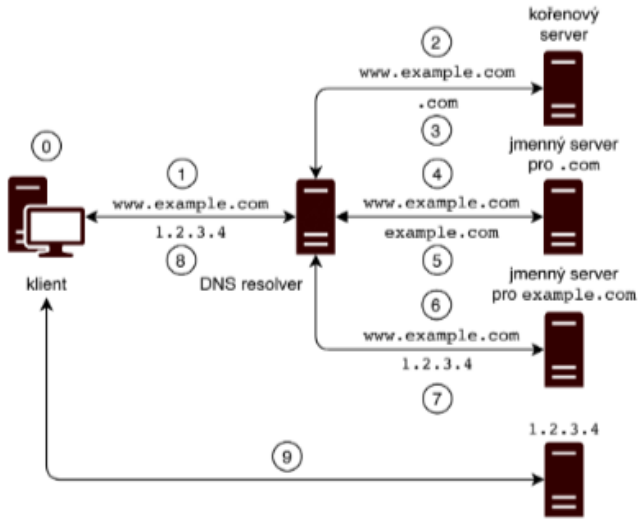


Figure 18: Enter Caption

Preklad domenoveho jmena na IP

Formou dotazu:

Dotazování:

- klient (řeší resolver)
- klient žádá DNS resolver server

Dva typy dotazů:

- rekurzivní (vyřešení dotazu)
- nerekurzivní (předání na jiný server)

Pocitac ma svoji vlastni cashe (muze ji znat)
pokud ji nezna tak vznese rekurzivni dotaz na DNS-server, ten musi byt nutne k dispozici jinak to vyhodi chybu
Druha casta chyba: v cashe mame neplatnou informaci, reseni: vymazani cashe
Servrovy Resolver se snazai vyrezit dotaz, **musi znat adresu korenovyho serveru**
nerekurzivni dotaz na domenu . ale vi kdo je zodpovedny za domenu ".com"
on se zepta na stejny dotaz serveru co je zodpovedny za domenu ".com"
ten nevi ale vy kdo je zodpovedny za domenu "example.com"
tu vrati a DNS-resolver se zepta "example.com" a je vracena IP

TU ip si ulozi ten DNS-resolver do cashe a tu posle zpatky clientovy a ten si ji taky ulozi do cashe

Preklad jmena (reseni dotazu)

Klient chce zjistit IP adresu ke jménu `www.example.com`. Klient prohledá svoji cache, zda nezná odpověď.

1. Klient pošle **rekurzivní dotaz** na DNS resolver (musí být nastaven), pokud DNS resolver zná odpověď (má ji v cache), pošle ji klientovi.
2. Pokud lokální jmenný server nezná odpověď, pošle **nerekurzivní dotaz** na kořenový jmenný server.
3. Kořenový jmenný server nezná odpověď, ale ví, kdo je zodpovědný za doménu `com` v dotazu, pošle DNS resolveru jeho adresu.
4. DNS resolver pošle **nerekurzivní dotaz** na jmenný server spravující doménu `example.com`.
5. Jmenný server zodpovědný za doménu `example.com` nezná odpověď, ale ví, kdo je zodpovědný za doménu `example.com`, pošle DNS resolveru jeho adresu.
6. DNS resolver pošle **nerekurzivní dotaz** na jmenný server spravující doménu `example.com`.
7. Jmenný server spravující doménu `example.com` zná odpověď (`1.2.3.4`) a pošle ji DNS resolveru.
8. DNS resolver předá `1.2.3.4` klientovi a uloží si údaje do cache.
9. Klient uloží `1.2.3.4` do cache a kontaktuje `1.2.3.4`.

Realne

Korenovych domenovych serveru je 13 (A - M) (C se preskakuje)
na kazdem serveru je ulozenej senzma domen 1. radu (dlouhej seznam ale zvladnutelnej)
tech serveru neni realne 13 ale je 13 IP adress a tech je miliony kopii po celim svete v praze jsou 3 (K , L a neco)
Vzdycky musim kontaktovat korenovy server
Velke organizace, velke firmy maji kopie vlastnich korenovych serveru z duvodu vypadky
dotaz je vzdy vznesen na nejblizsi korenovy server
slozitej proces na vyjednani kopie korenoveho serveru

kdyby byl tak brzo spadne , byl by prehlcen
k jednomu domenovymu jmenu muze byt vice IP adress - duvod rozdeleni zateze

- Řada typů jmenných serverů
- Časové omezení na vyřešení dotazu
- Update informací na serverech
  neustala aktualizace tech serveru (vymena nekdy trva i 3 minuty)
- Problém s cache

Dns vyuziva protocol bezne UDP , jde i TCP (port :53)

Veřejné DNS resolvery:
vetsinou poskytuje i internetovy provider

- `8.8.8.8` (Google)
- `1.1.1.1` (Cloudflare)
- `193.17.47.1` a `185.43.135.` (cz.nic)

9 Aplikacni vrstva (2)

Jednotlive protokoly v aplikacni vrstve

Elektronicka posta
odesílání a příjem e-mailu
mailbox
odeslání: **SMTP(S)** (Simple Mail Transfer Protocol) - protokol pro odesilani posty, S - jako secure
příjem: **IMAP4(S)** (Internet Message Access Protocol), zastaralý POP3 (Post Office Protocol) - u IMAP4 zustava kopie na serveru , organizaci do slozek, POP-3 Tohle neumoznuje
hlavička e-mailu - skrita uzivately , odesilatel , prijemce + detailni informace kudmy ten email sel (v g-mailu je tam ... zobrazit original)
bezpečnost, spam

Vzdalene prihlasovani
SSH (Secure SHell)

- ssh [user@]hostname[:port]
- PuTTY (pro Windows)
- pouzte se da s tim pripojit na Linux zarizeni
- vzdalene prihlaseni
- negraficka zalezitost

SCP (Secure **Copy**)

- pouzti: scp zdroj cil
- i na windows a linux

RDP (Remote Desktop Protocol, Windows), vzdalena plocha, graficky
VNC, vzdalena plocha, grafickt (klient - server) , funguje na jak Win tak Linux jsou i placeny = lepsi podpora vetsinou

Zakladni nastroje

- PING
  - odezva uzlu v siti
  - muze byt blokovan
  - ping .ip nebo domenove-jmeno.

  - ICMP protocol - Protocol na vrstve IP (sluzebni protocol)
  - dost casto windows blokuje ICMP protokol xddd (Windows moment)

- traceroute (Linux) , tracert (Windows)
  - analyza cesty v siti
  - priklad je to ze si otevri cmd nebo terminal a zkus to lool (nejlepsi vec na nauceni)

10 Odbocka tohle patri spis zas kte Vrstve sitoveho rozhrani

CESNET2
narodni vysokorychlostni pocitacova sit pro vedu a vzdelavani
www.cesnet.cz
prvni linie proti utokum a popripade protiutokum

CZ.nic
spravce CZ domeny
nic.cz
Jde lze koupit jakakoliv ceska domena (ktera je k dispozici)
provozuji 3 korenove servery
aktivni se zajimaji o vyvoj o DNS - Knot Resolver je cesky server a je i na dosti korenovych serverech