

Hálózati Alkalmazások

Bemutató:

- Domain Name System (DNS)
- Levélzés: SMTP, POP3, IMAP4, POP3S, IMAP4S
- Távoli elérés protokolljai: Telnet, SSH, SCP
- File Transfer Protokoll: FTP
- Web hozzáférési protokoll: HTTP, HTTPS

Portszám kiosztás

System ports: 0-1023

- általánosan használt szolgáltatások
- privilegizált hozzáférés (pl.: root) (server)

User Ports: 1024-49151

- egyéb szolgáltatások
- igényelhető
- nem kell privilegizált mód (server)

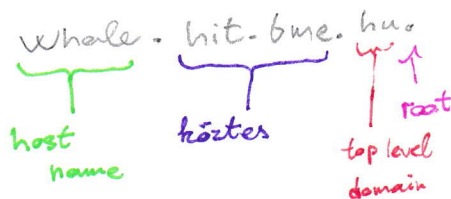
Dynamic/Private/Ephemeral Ports: 49152-65535

- OP osztja

Domain Name System

- IP cím helyett szimbolikus név

Szimbolikus Név



teljes: Fully Qualified Domain Name

- TLD nevek:

- Amerikából indult: .com, .net, .org
- 2 betűs country code: .hu, .sz, stb.

Subdomain

- FQDN középső része
- szabadon definiálható
 - ↳ fel kell tölteni DNS kezelő adatbázisát a zónát képező zónaíjba
- Domain és zóna közti különbség
 - zóna csak függőleges
 - domain: vízszintes is

whale.hit.bme.hu

Domainek:

.bme.hu,
.hit.bme.hu

Zónák:

hit.bme.hu
bme.hu
.hu

Root DNS szerverek

- 13 zóna
- a - m
 - pl: a.root-servers.net
- tárolják a tld szerverek IP-címeit

Névfeloldás

- név → IP-cím
- getaddrinfo() fv.
 - először gépen, utána kiszolga IP-címét
 - ↳ **UDP**
- **recursive query**, amire **authoritative answer**-t vár
 - névszerver: **iterative query** ↔ **referral**
 - néha belső szerverek is inkább authoritative answerrel tér vissza

Reverse Mapping

- IP-cím → szimbolikus név
- egy másik pontot lineárisan új rotnak
 - innen bejárjuk az adott IP címet
 - eltároljuk az eredményt: IP cím októberi fordított sorrendben
- Zónafajl neve (DNS-ben is) **ptr rekord**
- **CNAME**: Canonical Name, alias

Caching

- névszerverek tárolják:
 - **lekérdezett IP-címek** (közben is) (végeredmény is)
 - **negatív eredmény**
- TTL ideig
 - információval együtt ezt is küldi
- válasz üzenet **AA bit** (Authoritative Answer)
 - 1: "friss" info
 - 0: másik névszerver cach-éból
- névkiszolgáló **saját zóna nélkül**
 - csak recursive queryket fogadnak
 - **caching only name server**

Domain Név Regisztráció

- **registry**: TLD-t adminisztrálja
- **registrar**: cég, akihez domain regisztrációval fordulhatunk
- **registration**: folyamat
- **.hu** → ISZT
 - beverő

Domain Név Helyesírása

- a-z, 0-9, és '-' használható két. közt '-'-t határon nem
- már kiterjesztett
 - fordítás ASCII-be

Implementáció

- elterjedt: **BIND**
 - named program (name daemon)

Telnet

- más protokollok vizsgálata
- távoli bejelentkezés: 23-as porthoz csatlakozik
 - Linux: telnetd
 - shell-nek továbbítja a begépelt dolgokat
 - NEM grafikus
 - pl.: telnet localhost 25
 - helyi gép 25-ös portján futó alkalmazás vizsgálata

SMTP

- ASCII kódolás TCP/IP-n keresztül

Feladat

- Mail User Agent (UA) kéri (levelező program)
- UA SMTP-t küld a küldő SMTP-szervernek Message Transfer Agent
- küldő SMTP TCP-vel vevő SMTP-nek (bemenő postaládába ír, utána)
- vevő file-ba írja
- sikertelen → újraküldés, nem végtelenségig
- spam ellen
 - Message Submission Protocol
↳ azonosítást követel (587-es port)
- postaláda_neve@FQDN (nem kötelezően)
- host paranccsal kideríthető

Nem Ascii kódolt információ

- binárisba kódolás
 - uuencode ↔ uudecode
- MIME (Multipurpose Internet Mail Extension)
 - bármit elkódol (kép, stb.)
 - SMTP-t használ
 - megadja: típus és kódolás (pl.: text/plain, base64)
 - részre osztott üzenet
 - válogatható (pl.: nem tud hangot játszani)

SMTP paramerek

HELO	küldő gép
MAIL FROM	feladó címe
RCPT TO	címzett címe, több címzett, többpontosan küldi
DATA	levél tartalma, üzenet vége: olyan sor, ami csak egy.
QUIT	vevő OK válasz és kapcs. vége
RSET	törli a folyamatot
NOOP	no op., vevő OK-t válassza

• SMTP szerver válasza

- nnn szöveges üzenet
 - nnn: 3 jegyű kód
 - 2xx: poz. eredmény "✓"
 - 4xx: transziens hiba "!"
 - 5xx: permanens hiba "X"

Postafiók implementáció

- Unix
 - mbox formátum
 - új levél: sor elején "Mail" ^{space}
 - ha a levélben szerepel → ">Mail"
- sok levél → nagy név → lassú
 - Maildir
 - gyorsabb, hashelhető
 - new, ~~old~~ cur, tmp
 - MTA mindig tmp-be
 - olvasatlan: new

POP3

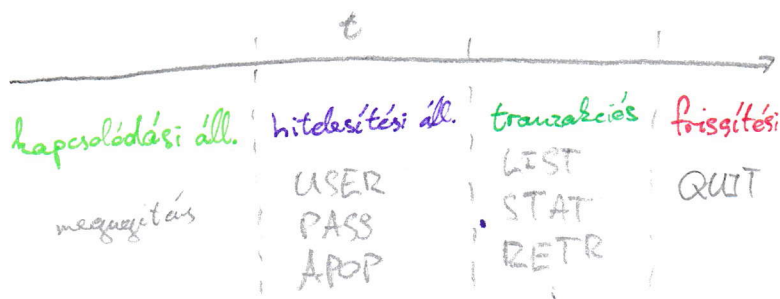
Post Office Protocol 3

Cél

- SMTP fogadó szervernek online kell lennie TCP miatt
- idegton online SMTP szerver
 - kliensek letöltik onnan az üzeneteket (pl.: POP3)
 - felhasználó továbbra is SMTP-vel küld

Használat

- TCP-t használ
- 110-es port
- parancs
 - 4 betűs
- válasz
 - +OK / -ERR



Parancsok

kötelező

STAT

LIST [üzenet-#]

RETR üzenet-#

DELE üzenet-#

NOOP

RSET

QUIT

+OK, üzenetek száma, mérete (oltott)

∃# → üzenet-azonosító, méret (oltott)

→ +OK üzenetek mérete (oltott), n sor szám, méret (oltott)

+OK üzenet mérete (olt.), üzenet (letöltés)

törölés

+OK válasz

törli a törlésre várók figyelését

törli a törlendőket → +OK-Err majd lezár TCP-t

opcionális

USER név

trivial

PASS jelszó

trivial

TOP üzenet-# n

+OK, üzenet fejléce, n sor

UIDL [üzenet-#]

unique id alapján listáz

APOP név digest

név a felhasználó digest jelszó kódolva

POP3S

- SSL3/TLS1 réteg adódik hozzá (Secure Socket Layer 3/Transport Layer Security)
- 995 port
- titkosított csatornán folyik a kommunikáció

IMAP V4

• Internet Message Access Protocol V4

• távoli postafiók kezelésére

• szolgáltatások:

- elérés, szinkronizálás
- crectolmányok állapotának
- levelek letöltése
- synch

• műveletek:

- postafiók add, rename, remove
- új levelek érkezésének figyelése
- levelek eltávolítása postafiókból
- levelek állapotjelzői, törlése
- MIME értelmezése
- keresés, selektív letöltés

• állapotai vannak

- parancsok állapothoz kötve

1. Azonosítás előtt

2. Azonosított

3. Választott

4. Kijelentkezett

Azonosításhoz „olmányokat” kérőjt be
(PreAuth ezt az állapotot kihagyja)

Postafiók kiválasztása, hiba esetén ide
tér vissza

Kiválasztottunk a postafiókát

IMAP4 server bezárja a kapcsolatot

IMAP4S

• SSL 3/TLS 1 réteg +

• 993 port

SSH

Elméleti alapok

- biztonságos hálózati elérés
- szerver-kliens kapcsolat 22-es port
- feltetelek:

- egyenként nyilvános és titkos kulcs
- felhasználónként -11-

- menete:

1. Titkos csatorna létrehozása
2. Felhasználó azonosítása
3. Titkosított kommunikáció

①

- kliens ismeri a szerver nyilvános kulcsát
- kapcsolatkulcs létrehozása, a két fél inentől ezt használja
- sebezhetőség: támadó „szerverként pózolhat”, ha nincs meg a szerver nyilvános kulcsa

②

- a) Erős azonosítás nyilvános kulcsú rendszerrel
 - b) Jelszavas azonosítás
 - c) Berkeley r* használata (bizalmas, transzparens)
- sebezhetőség: uat. (jelszavas módszerrel)

③

- ha az előző 2 sikeres, akkor végleg titkosító algoritmusral

Gyakorlatban

- kulcsok tárolása
- `~/.ssh/known-hosts`

- erős azonosításhoz

- ssh-keygen program

- 2 file (`id-dsa`, `id-dsa.pub` / `id-rsa`, `id-rsa.pub` / `id-eddsa`, `id-eddsa.pub`)

dsa rsa eddsa

- kulcsok elhelyezése oda, ahova be szeretnénk lépni

- `ssh-copy-id -i ~/.ssh/id_dsa.pub felhasználó@gepnev`

- más felh. névvel:

- `ssh felhasználó@gepnev / ssh -C felhasználó gepnev`

- használható port-forwardingra is
- pl x grafikus felület elérése

- scp: másolás

FTP

- file transfer protocol
- kliens-szerver kapcsolat
- TCP-t használ - vezérlésre
- 2. TCP kapcsolat csak az adatátvitelre
 - **aktív:** szerver kérésére kliens küld IP+portszám
 - **passzív:** szerver küld IP+portszámot → kliens kezdeményez
- minden file új kapcsolat
- általában szerver, néha kliens is megtekinthető

Parancsok

- 4 Char + opcionális param.

[lásd jegyzet]
(felk. segédlet)

- válasz: nnn szöveges üzenet
 - 3 szám
 - 200: Command okay (pl.:)

FTP felhasználói szempontból

- távoli gépen interaktív file/könyvtárhozzáférés
 - list
 - remove/rename
 - download
 - upload
- cmd-ből
 - ftp [host name]
 - felhasználóként / anonymous
 - ↳ jelszó: dont care
 - általában /pub-ból letölthetünk incomingba fel
 - felhasználóként lehet több jogunk
 - unix szervereken működnek unix parancsok általában

HTTP

- HTML oldalakat HyperText Transfer Protocol segítségével tölthetjük le
- WWW → HTML oldalak összessége
- webszerverek
 - dokumentumok

!((WWW = világösszetes))

- szöveg

- kép

- hang

- stb.

weblap-okba szervezve

- **hyperlink**: web dokumentumokra mutató link
- web kliensen keresztül

HTML

- HyperText Markup Language
- Standard Generalized Markup Language implementációja
 - hyperlinket tartalmazó dokumentum szabvány
- **hyperdokumentum**: hyperlinket tartalmazó doc.
- **tag**-ekbe rendezett
 - <tag> Pl.: <HTML>
 - </tag> Pl.: </HTML>
 - HTML, HEAD, BODY, TITLE
 - tagok viselkedése "egyéb paraméterekkel" módosítható
- **URL**: Uniform Resource Locator
 - helymeghatározás az interneten
 - syntax: protokoll://név/elővási-út
 - másik gépen lévő dokumentum általában: HTML
 - általánosabb: URI

HTTP

- legelterjedtebb web-szerver: Apache httpd
- TCP kapcsolat alapértelmezetten 80-as porton
 - különben url-ben specifikálni kell

• példák:

- GET <betölteni doc> HTTP/1.0

ver. no.

• Válasz:

- **statusz**: egy sor, HTTP verzió, státusz kód, kérés eredménye

- **fejleszt**: szerver típusa, MIME verziószám, tartalom típusa, \n, fejléc és adat között is \n

- **adat**: HTML esetén egyszerű szöveg, a HTML doksi

• HTTP TCP bontása:

1.0: 4 új kérés/válasz új TCP kapcsolatot

1.1: beállítás kérdése

- többi példa jegyzetben, de nincs lényeges információ

HTTPS

• HTTP felett TLS/SSL

UNIX

Alapok

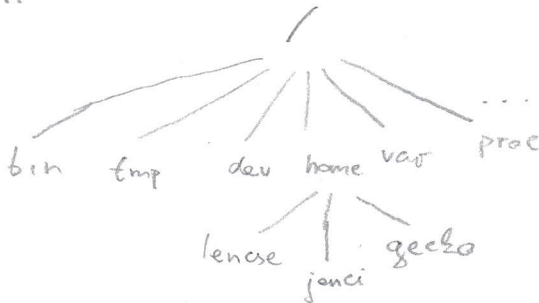
- multitasking OP-rendszer
 - egyszerre több programot futtathatunk
 - Védeni kell:
 - más programok
 - OP-RSZ.
 - hardware
- ↳ privilegációs szintek (min 2)
- többfelhasználós
 - fájlrendszer adminisztrátor
 - **superuser: root**
 - bgin: user, pw

Fájlrendszer

- # meghajtók
- egyetlen fájlrendszer a pontjaira fűzve

Könyvtárak

- root (/) alatt
- pl.:



- 7-féle bejegyzés:

directory - könyvtár

file

block device: speciális szövegfájl
(blokkos átviteli perifériák)

Character device: (karakter átviteli perifériák)

Symbolic link: más könyvtárbejegyzésre mutató link

socket

TCP/IP socket interface programozása

pipe

nevezített csővezeték

/bin: alap univerzális parancsok

/boot: boot infók

/dev: szövegfájl

/home: felhasználók

/lib: dinamikus programkönyvtárak

/mnt: ideiglenes kötetek

/proc: virtuális fájlrendszer (kernel belsője)

/root: rendszergazda home

/sbin: admin parancsok

/tmp: temporary

/usr: felhasználói programok

/var: változó dolgok

Fájlbrendezés parancsok

ls list (-a: rejtett is, -l attribútum is)

cd <dir>

cd $\emptyset$ home-ba

pwd working directory neve

mkdir <dir> létrehozás

rmdir <dir> törlés

rm <file (ok)> törlés

rm -r <dir> törlés (dir + subdiv + all files)

cat file hívása

cp <mit> <mibe> copy

cp <forrás fájl(ok)> <cél könyvtár>

mv ^(mit)
<honnnan> <hova> move

du dir és subdiv disc usage

df lemezhasználat (egyes kötetek)

quota felhasználható/felhasznált terület (felhasználónként)

Függelék

Jogosultságok:

- V fájlra 3 rész (9 bit**)

owner | group | world

rwx rwx rwx

- Read write execute bitek

- parancsok:

chmod <jogok> <filename> jogok beállítása (jogok átírása)

chown <username> <file/dir> tulaj megadása

chgrp <group> <file/dir> csoporttulaj megadása

Egyéb Unix parancsok

echo

ps aux

kill

move

less

: