

Softver otvorenog koda

Žarko Zečević
Elektrotehnički fakultet
Univerzitet Crne Gore

Predavanje 2

Apache Web server

Ishodi učenja:

Nakon savladavanja gradiva sa ovog predavanja studenti će moći da:

- Instaliraju i konfigurišu Apache web server (virtuelni hostovi, portovi, moduli, .htaccess fajl)
- Intaliraju i konfigurišu ftp server

Šta je web server?

Web server je računarski program koji je zadužen za prihvatanje zahtjeva od strane klijenata (web browsera), kao i slanje odgovora koji obično sadrže web stranice kao što su HTML dokumenti i linkovani objekti (slike, video, itd.)

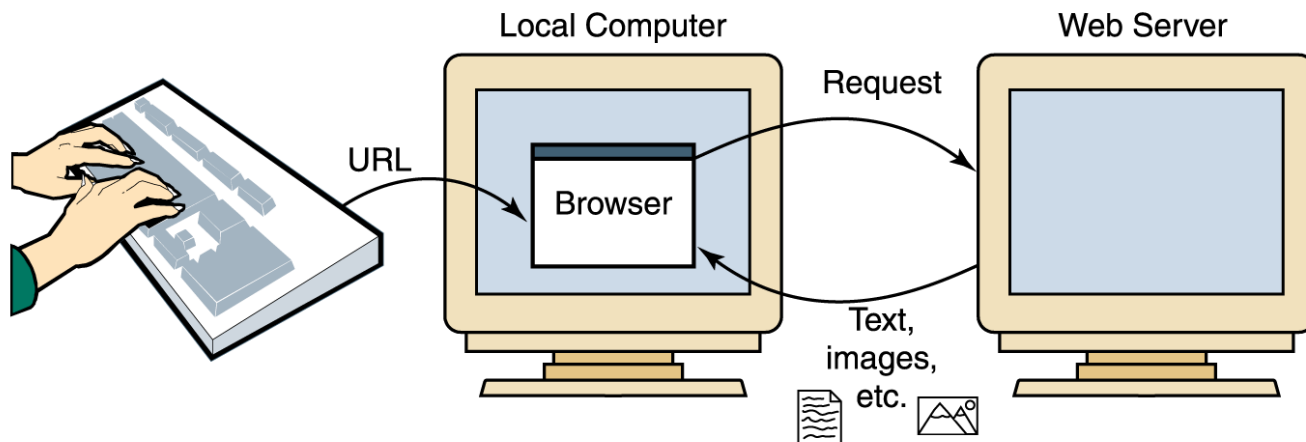
Web klijent može slati i neke parametre serveru (kao što su korisnički podaci). Server vraća tražene statičke datoteke ili generiše dinamičke datoteke na osnovu dobijenih podataka. Server je takođe zadužen za komunikaciju sa bazom podataka.

Komunikacija između web klijenta i web servera se odvija putem HTTP protokola.

Šta je web server?

- Kada u pretraživač kucate URL (na primjer, "http://www.ucg.ac.me/proba.html"), serveru se šalje zahtjev za stranicom „proba.html“ i on je vraća nazad.
- Web server osluškuje konekcije (zahtjeve) na određenom mrežnom portu. Podrazumjevani port za http konekcije je 80. Ukoliko se koristi drugi port, tada ga je neophodno specificirati u URL-u:

http://www.ucg.ac.me:port/proba.html



Popularni web serveri

- **Apache web server**
 - open source
 - najrašireniji web-server
- **NGINX**
 - noviji open-souce web-server, prvo izdanje 2004
 - popularnost mu jako raste zbog boljih performansi od Apache-a
 - dizajniran za tzv. C10K problem - 10000 simultanih konekcija
- **Microsoft IIS**
 - dostupan samo za MS Windows
 - dolazi kao integralni dio većine Windows-a

Popularni web serveri

Statistika korišćenja različitih web servera (top milion sajtova)

Tehnologija	Web sajtovi	%
<u>Apache</u>	<u>305,105</u>	30.51
<u>nginx</u>	<u>294,255</u>	29.43
<u>IIS</u>	<u>118,128</u>	11.81
<u>LiteSpeed</u>	<u>62,920</u>	6.29
<u>Varnish</u>	<u>32,299</u>	3.23
<u>BIG-IP</u>	<u>10,828</u>	1.08
<u>Apache Tomcat Coyote</u>	<u>10,211</u>	1.02
<u>Phusion Passenger</u>	<u>7,592</u>	0.76
<u>Rack Cache</u>	<u>7,036</u>	0.7

Apache web server

- Web server otvorenog koda koji sa najčešće koristi na Linux, Unix i Solaris platformama. Takođe je dostupan za WinOS i Mac.
- Prvu verziju je kreirao Robert McCool (1995). Najnovija stabilna verzija je 2.4.46.
- Apache je najpopularniji web server na internetu.
- Veoma je siguran, brz i pouzdan.
- Naziv „Apache“ potiče od riječi „patchy“ koju su Apache developeri koristili da označe rane verzije njihovog softvera. Pored toga cilj je bio da se oda počast domorodačkom plemenu Indijanaca iz Amerike.

Apache licenca

Apache web server je licenciran Apache licencom, čiji je autor Apache Software Foundation ili ASF. Verzija 2.0 licence odobrena je od strane ASF-a 2004. godine.

Apache je „popustljiva“ licenca jer nema načina kontrole nad softverom koji se dalje redistribuira, tako da ne zahtjeva da se dalje verzije softvera izdaju pod tom istom licencom, ali zahtjeva da se sačuvaju podaci o autoru pojedinog koda i to u svakoj datoteci, što se mora poštovati u svim daljim verzijama softvera.

Licenca dopušta da se softver slobodno koristi, izučava, mijenja i dalje redistribuira, pa je tako to jedna od licenci slobodnog softvera, a priznaje je i FSF. Apache licenca je kompatibilna samo sa GPL v3 licencom.

Instalacija na Ubuntu Linuxu

Na Ubuntu-u apache web server se instalira na sljedeći način:

```
sudo apt-get update  
sudo apt-get install apache2
```

Nakon uspješne instalacije, u browseru bi nakon kucanja URL-ova:

<http://localhost>

http://IP_adresa_racunara

trebalo da se otvori početna strana.

Po defaultu, korijenski web-direktorijum je:

`/var/www/html`

Instalacija na Ubuntu Linuxu

Ispod su date komande za pokretanje/stopiranje servera:

- Pokretanje Web Servisa

```
sudo systemctl start apache2.service
```

```
ili sudo service apache2 start
```

- Restartovanje Web Servisa

```
sudo systemctl restart apache2.service
```

- Stopiranje Web Servisa

```
sudo systemctl stop apache2.service
```

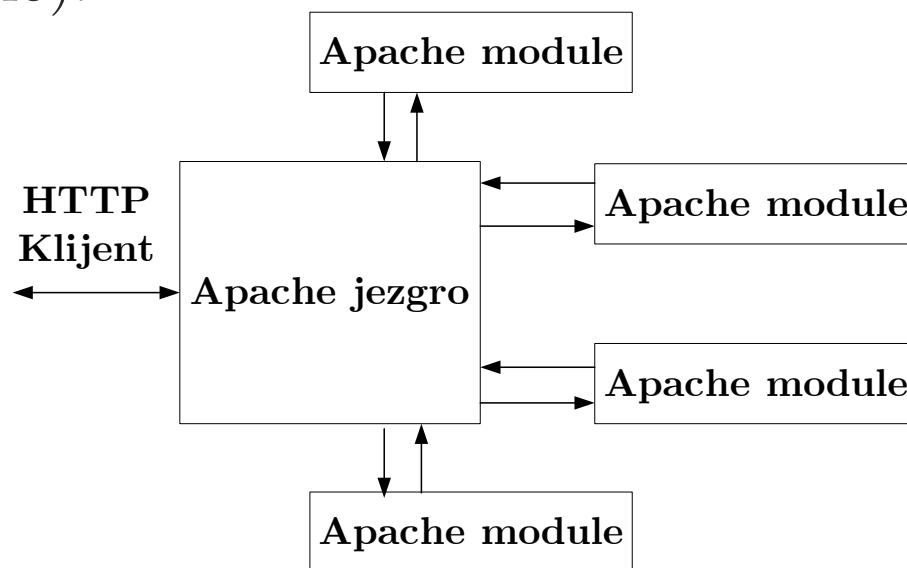
Spisak trenutno aktivnih konekcija se može dobiti na sljedeći način:

```
ss -tn src :80 or src :443
```

Arhitektura apache web servera

Apache server se sastoji iz relativno malog jezgra koje je zaduženo za osnovnu funkcionalnost servera. Pored toga, dostupan je veliki broj modula kojima se proširuje osnovna funkcionalnost i koji se mogu aktivirati po potrebi. Primjeri modula su `mod_php`, `mod_python` i `mod_ssl` (podrška za php, python i ssl respektivno).

Prilikom pokretanja sistema pokreće se apache daemon (pozadinski proces) koji se naziva `httpd`, a zatim se čita glavni konfiguracioni fajl i učitavaju aktivirani moduli.



Arhitektura apache web servera

Apache server obrađuje zahtjeve klijenata tako što za svaki zahtjev kreira po jedan proces. Kada je server opterećen, pristizanje novih zahtjeva i kreiranje novih procesa može dodatno zagušiti mašinu.

Ovaj problem se zaoblizi implementacijom koncepta – „**perzistentni serverski procesi**“. Ovo znači da u samom startu server kreira veliki broj podprocesa koji su zaduženi za prihvatanje konekcija. Ovi podprocesi su sve vrijeme aktivni, bez obzira na to da li ima aktivnih konekcija.

Ono što je interesantno je da Apache može dinamički da mijanja broj podprocesa u zavisnosti od opterećenosti servera.

Arhitektura apache web servera

Konfiguracioni fajlovi servera se nalaze u direktorijumu:

`/etc/apache2.`

```
zarkoz@sok:~$ ls /etc/apache2
apache2.conf      conf-enabled  magic          mods-enabled   sites-available
conf-available   envvars      mods-available ports.conf     sites-enabled
```

- `apache2.conf` – glavni konfiguracioni fajl
- `mods-available` – dostupni moduli
- `mods-enabled` – aktivirani moduli
- `sites-available` – dostupni virtuelni hostovi
- `sites-enabled` – aktivirani virtuelni hostovi
- `conf-available` – dostupna generalna podešavanja
- `conf-enabled` – aktivirana generalna podešavanja

Arhitektura apache web servera

Prilikom pokretanja servera, najprije se učitava glavni konfiguracioni fajl, nakon njega fajl **ports.conf**, i na kraju fajlovi iz direktorijuma **mods-enabled**, **conf-enabled** i **sites-enabled** (svi se nalaze unutar direktorijuma **/etc/apache2/**).

U okviru fajla **ports.conf** se podešavaju portovi koje server osluškuje i IP adrese sa kojih je server dostupan (ukoliko postoji više mrežnih kartica). U gorepomenutim direktorijumima se nalaze podešavanja vezana za module, globalna podešavanja i virtuelne hostove.

Log fajlovi servera se nalazi na lokaciji:

/var/log/apache2

Glavni konfiguracioni fajl

Većina podešavanja Apache servera smještena je u **glavnom konfiguracionom fajlu: apache2.conf** (ili **httpd.conf** na nekim distribucijama Linuxa). Ovaj fajl ima oko 1000 linija i njegova lokacija varira od verzije do verzije Linuxa.

Neka tipična podešavanja su:

- **Broj konkurentnih konekcija** (za svaku konekciju se startuje jedan proces, a svaki proces zauzima nezamarljivu količinu CPU-a i RAM-a),
- Različite vrste „**vremena čekanja**“ (eng. timeout),
- Ime servera (**ServerName**), itd.

Fajl ports.conf

Fajl **ports.conf** se može modifikovati pomoću komande:

nano /etc/apache2/ports.conf

Kao što je prikazano na slici ispod, podrazumjevani port je 80, dok server osluškuje i port 443 ukoliko su uključeni moduli `ssl_module` i `mod_gnutls.c`.

```
Listen 80
<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```


Konfiguracija modula

Apache sadrži veliki broj modula kojima se proširuje njegova funkcionalnost. Svi moduli su dostupni u direktorijumu **mods-available**, dok se aktivirani moduli nalaze u direktorijumu **mods-enabled**.

Moduli se koriste za omogućavanje korišćenja php-a, cgi skripti, za podešavanje autentifikacije, pružanje mogućnosti da home direktorijum svakog korisnika bude dostupan preko web-a, itd.

Moduli se omogućavaju tako što se u direktorijumu **mods-enabled** kreiraju simbolički linkovi na odgovarajuće module iz direktorijuma **mods-available**. To se postiže pomoću komande:

a2enmod putanja do modula

Konfiguracija modula

Na primjer, **userdir** predstavlja modul kojim se omogućava da home direktorijum svakog korisnika bude dostupan na web-u. Po default-u ovaj modul nije omogućen, a može se omogućiti na sljedeći način:

```
sudo a2enmod userdir
```

Treba napomenuti da se komanda `sudo` koristi za izvršavanje komandi kao administrator.

Nakon ovog koraka treba restartovati server i provjeriti sadržaj foldera **mods-enabled**:

```
ls /etc/apache2/mods-enabled
```

Novododati modul `userdir` se konfigurira na sljedeći način:

```
sudo nano /etc/apache2/mods-enabled/userdir.conf
```

Konfiguracija modula

```
<IfModule mod_userdir.c>
    UserDir public_html
    UserDir disabled root
    <Directory /home/*/public_html>
        AllowOverride All
        Options MultiViews Indexes
        SymLinksIfOwnerMatch
        <Limit GET POST OPTIONS>
            Order allow,deny
            Allow from all
        </Limit>
        <LimitExcept GET POST OPTIONS>
            Order deny,allow
            Deny from all
        </LimitExcept>
    </Directory>
</IfModule>
```

Konfiguracija modula

Na prethodnom slajdu je prikazan defaultni sadržaj fajla **user.conf**. Korisnik treba u svom home folderu da kreira folder **public_html**. Sve unutar tog foldera biće dostupno preko adrese:

http://89.188.32.136/~korisnicko_ime

Treba napomenuti da je izvršavanje php fajlova u home direktorijumima po default-u isključeno, iz sigurnosnih razloga.

PHP se uključuje tako što u fajlu:

sudo nano /etc/apache2/mods-available/php5.conf

linije koje se odnose na modul **userdir** treba staviti pod komentarom.

Konfiguracija virtuelnih hostova

Virtuelni host (virtual host) omogućava hostovanje više različitih domena na istoj mašini (serveru). Apache podržava dva tipa virtuelnih hostova:

- Name-based virtuelni hostovi
- Ip-based virtuelni hostovi

Ip-based virtuelni host se koristi kada mašina ima nekoliko različitih IP adresa. Tada se po jedan virtuelni host vezuje za svaku IP adresu.

Name-based virtuelni host omogućava pokretanje više virtuelnih hostova sa jedne iste IP adrese.

Konfiguracija virtuelnih hostova

Prvi korak u kreiranju virtuelnog hosta predstavlja kreiranje fajla u folderu **sites-enabled**. Potrebno je napraviti kopiju default-ne konfiguracije sajta i dati joj neki naziv (na primjer **test.com**)

```
sudo cp /etc/apache2/sites-available/000-default.conf  
/etc/apache2/sites-available/test.com.conf
```

Nakon ovog treba editovati fajl **test.com.conf** i podesiti domensko ime, root direktorijum sajta (dir. u kome se nalazi web stranica, itd.).

Na kraju, virtuelni host se omogućava pomoću komande:

```
sudo a2ensite test.com.conf
```

Konfiguracija virtualnih hostova

Iznad je prikazan primjer sadržaja virtual host fajla.

```
<VirtualHost *:80>
    ServerAdmin admin@test.com
    ServerName test.com
    Alias /test /var/www/test.com/public_html
    ServerAlias www.test.com
    DocumentRoot /var/www/test.com/public_html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog          ${APACHE_LOG_DIR}/access.log
    combined
</VirtualHost>
```

Konfiguracija virtuelnih hostova

Pored <Virtual host> direktive, virtual host fajl može da sadrži i dodatna podešavanja.

Na primjer, direktiva <Directory> se koristi za dodatna podešavanja direktorijuma u kome se nalaze fajlovi. U konkretnom primjeru radi se o direktorijumu:

```
/var/www/test.com/public_html
```

```
<Directory /home/*/public_html>  
    AllowOverride FileInfo AuthConfig Limit  
    Options MultiViews Indexes  
SymLinksIfOwnerMatch IncludesNoExec  
Order deny,allow  
    Deny from all  
</Directory>
```


Konfiguracija virtuelnih hostova

U prethodnom primjeru:

- **AllowOverride** znači da ova podešavanja nadvladavaju podešavanja u glavnom konfiguracionom fajlu
- **Authconfig** – omogućava korišćenje autentifikacije
- **Multiview** – ukoliko je zatražen direktorijum „proba“ pri čemu on ne postoji, tada će server tražiti fajlove koje sadrže riječ proba
- **ExecCGI** – omogućeno je izvršavanje CGI skripti
- **FollowSymLinks** – server će pratiti simboličke linkove u ovom direktorijumu
- **Indexes** – ako ne postoji fajl index.php, tada će server izlistati sadržaj root direktorijuma

Zaštita web servera

Jedan način da se zaštite podaci u nekom direktorijumu je da se koristi password. Ovo se može odraditi tako što se doda `.htaccess` fajl u direktorijum koji želite da zaštite šifrom. Jedan primjer sadržaja `.htaccess` fajl je dat ispod:

```
AuthUserFile /etc/apache2/.sifre (mora aps. put.)
```

```
AuthName "Please Enter Password"
```

```
AuthType Basic
```

```
Require valid-user
```

`AuthUserFile` predstavlja putanju do fajla u kom su sačuvani podaci o korisničkom imenu i šifri, dok ostala podešavanja se odnose na izgled prozora za logovanje i validna korisnička imena.

Zaštita web servera

Korisničko ime i šifra se kreiraju pomoću **htpasswd** komande:

htpasswd putanja_do_fajla user

Putanja_do_fajla predstavlja fajl u koji će se sačuvati podaci za logovanje. Ovaj fajl prethodno treba kreirati, ukoliko ne postoji. **User** predstavlja željeno korisničko ime. Nakon izvršavanja gornje komande sistem će zatražiti unošenje passworda. Na isti način se u isti fajl dodaju novi korisnici. Fajl sa šifrom treba sačuvati u nekom direktorijumu koji nije dostupan preko web-a. Treba napomeniti da na ovaj način ne bi trebalo štititi najosjetljivije podatke, jer se prilikom logovanja username i šifra šalju web serveru kao čisti tekst.

Zaštita web servera

Ukoliko želite da zabranite pristup web sajtu sa specifičnih IP adresa, tada u **.htaccess** fajl treba dodati sljedeće:

Order Deny, Allow

Deny from All

Allow from 192.168.1.100

Allow from 192.168.1.101

Podేశavanja **.htaccess** fajla se odnose i na sve poddirektorijume, a pored toga, u poddirektorijumima se mogu dodavati zasebni konfig. fajlovi. Generalno, u **.htaccess** fajl se mogu dodati i druge direktive, ali to treba izbjegavati, jer usporava rad servera.

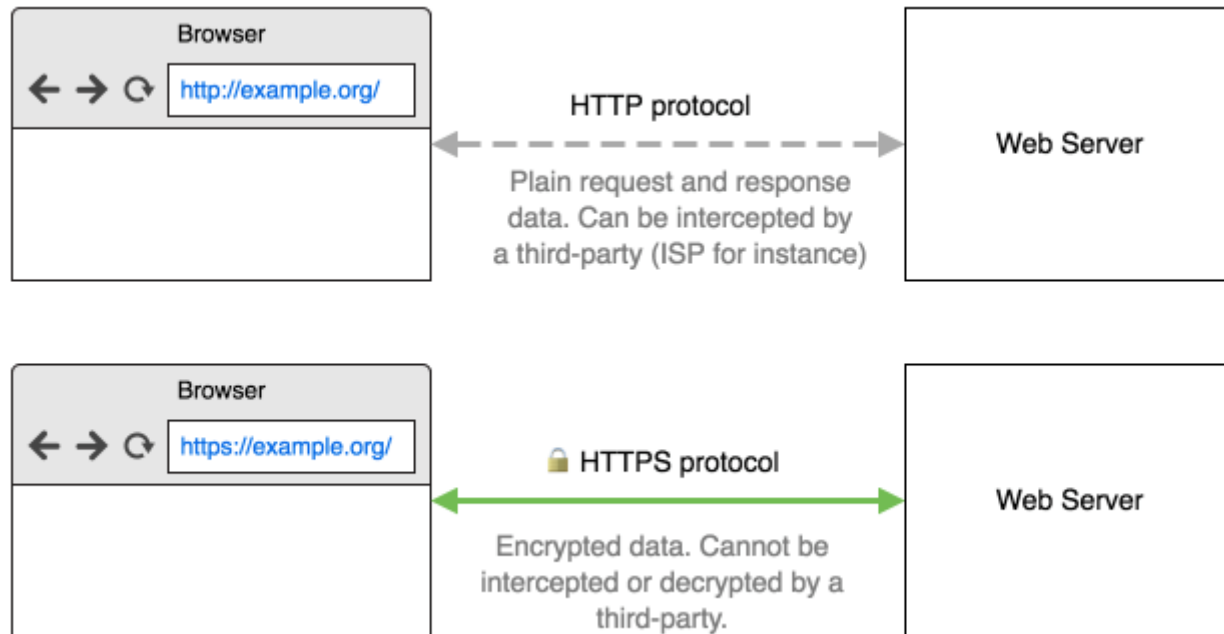
HTTPS protokol

HTTPS protokol predstavlja kombinaciju standardnog HTTP i SSL protokola. Korišćenje ovog protokola znači da će podaci koji se razmjenjuju između servera i klijenta biti kriptovani, čime se umanjuje mogućnost krađe podataka.

Da bi omogućili korišćenje HTTPS protokola najprije je potrebno kupiti ili generisati sigurnosni sertifikat. Sigurnosni sertifikat se može generisati pomoću besplatnog OpenSSL alata. Nakon toga treba konfigurirati apache virtuelni host da koristi ovaj sertifikat. Default-ni port je 443, a serveru su pristupa na sljedeći način:

https://IP_adresa_racunara

HTTPS protokol



Prilikom iniciranja konekcije server klijentu šalje javni ključ koji se koristi za uspostavljanje kriptovane konekcije.

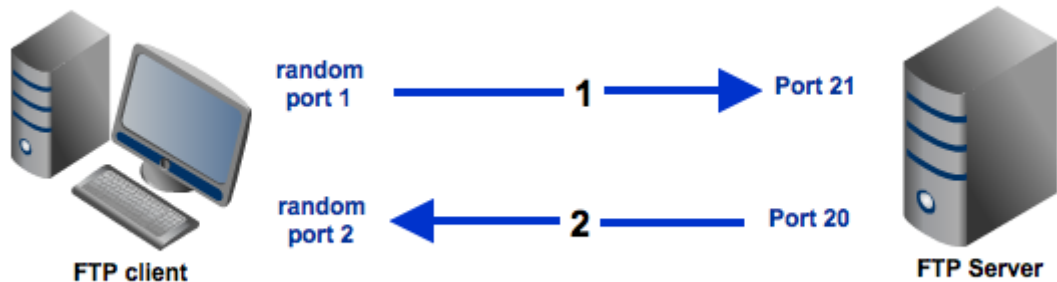
FTP server

FTP (File Transfer Protocol) protokol služi za razmjenu fajlova između računara. FTP može da radi u dva moda:

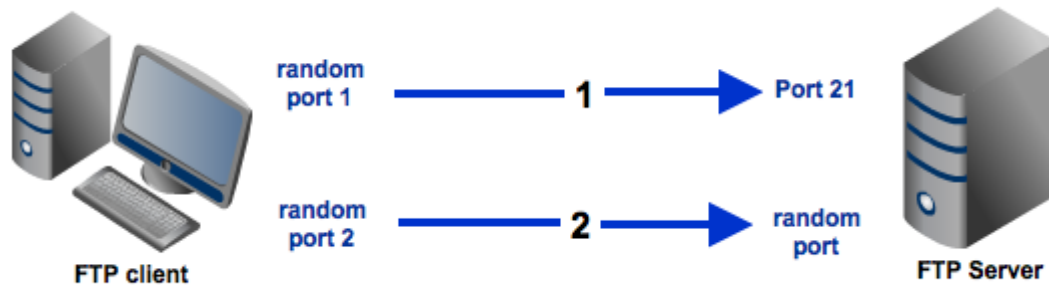
- U aktivnom modu, FTP klijent otvara dva slučajna neprivilegovana porta K1 i K2 (>1024). Klijent se konektuje sa porta K1 na FTP server, koji osluškuje na portu 21 i šalje mu informaciju o K2. Nakon toga, FTP server sa porta 20 otvara konekciju sa klijentom na portu K2.
- U pasivnom modu klijent otvara dvije konekcije, na neprivilegovanim portovima K1 i K2. Prva konekcija se obavlja između porta K1 i standardnog FTP porta 21. Kao odgovor, server otvara neprivilegovani port S1 i tu informaciju šalje klijentu. Dalja komunikacija se odvija između portova S2 i K2.

FTP server

- Aktivni mod
 - Server inicira drugu konekciju



- Pasivni mod
 - Klijent inicira drugu konekciju



FTP server

Neki nedostaci FTP-a su:

- Konekcija između klijenta i servera nije kriptovana
- FTP nije pouzdan (server ne dobija povratnu informaciju o tome da li je fajl uspješno preuzet). Ako dođe do greške server neće biti obavješten, odnosno potrebno je opet inicirati preuzimanje fajla.
- Za slanje fajlova je potrebna autorizacija, a samim tim i kreiranje i brisanje naloga, odnosno administriranje servera

FTPS je verzija FTP protokola nadograđena TLS (Transport Layer Security) i SSL (Secure Sockets Layer) kriptografskim protokolima.

FTP klijent

FTP klijent služi za povezivanje na ftp server. Linux-ov terminal i Windows-ov CMD imaju ugrađenu podršku za ftp. Postoji niz komandi za kreiranje korisnika, upload, brisanje fajlova, itd, koje se koriste u okviru FTP-a.

Pored terminala postoje i besplatni klijenti za grafičkim interfejsom. Neki od najpoznatijih su:

- FileZilla (postoji i server i klijent)

<https://filezilla-project.org/>

- WinSCP

<https://winscp.net/eng/download.php>

Instalacija na Ubuntu-u

Na Linuxu-u se besplatni ftp server instalira na sljedeći način:

```
sudo apt-get install vsftpd
```

Podešavanja ftp servera se nalaze u konfiguracionom fajlu:

```
sudo nano /etc/vsftpd.conf
```

U okviru ovog fajla se nalaze podešavanja vezana za upload fajlova, default-ne dozvole, anonimne korisnike, itd. Za korišćenje ftp servera je potrebno kreirati posebne naloge, a moguće je omogućiti da svaki korisnik Linux-a ima pristup svom home-u preko ftp-a.

Dio /etc/vsftpd.conf fajla

```
# Koristiti aktivni mod
pasv_enable=NO
#
# Dozvoliti pristup anonimnim korisnicima
anonymous_enable=NO
#
# Dozvoliti logovanje sa lokalnih naloga
local_enable=YES
#
# Dozvoliti promjene na ftp serveru
write_enable=YES
#
# Default-na maska za lokalne korisnike
local_umask=022
```