

Silvano Čulinović¹

Marin Kaluža²

Dijana Liverić³

Pregledni rad

UDK 004.772.057.4

USPOREDBA PROTOKOLA ZA PRIJENOS DATOTEKA⁴

SAŽETAK

Za pristup podatkovnim (datotečnim) resursima sustava, na korisničkoj razini upotrebljavaju se za to izgrađene namjenske aplikacije. Takav aplikativni softver može se izvršavati lokalno na računalu korisnika i na udaljenom aplikacijskom poslužitelju. U oba slučaja komunikacija korisnika s podatkovnim (datotečnim) poslužiteljem odvija se korištenjem mrežnih resursa. Mrežni resursi predstavljaju najsporije komponente u radu sustava. Aplikativni softver za komunikaciju s datotečnim poslužiteljem može koristiti različite mrežne protokole. U ovom radu analizirani su protokoli za prijenos datoteka na aplikacijskom sloju. Objasnjeni su korišteni sigurnosni mehanizmi u analiziranim protokolima. Izvršeno je mjerenje vremena i brzine prijenosa datoteka u LAN mreži na brzinama 10 Mbps, 100 Mbps i 1 Gbps, te u nezaštićenoj i zaštićenoj (VPN) WAN mreži. Pokazano je da su protokoli koji koriste sigurnosne mehanizme sporiji od protokola koji ne koriste sigurnosne mehanizme. Također je pokazano da korištenje FTP HTTPS sigurnog protokola predstavlja optimalno rješenje – visoka razina sigurnosti i ne značajno manja brzina.

Ključne riječi: protokol za razmjenu datoteka, sigurnost, mreža, brzina prijenosa

1. UVOD

Korisnička aplikacija predstavlja osnovu komunikacije između korisnika i računala. Korisnik putem aplikacije upućuje zahtjeve te vrši obrade više ili manje složenih (multimedijskih) podataka.

Aplikacije koje koriste podatkovne (datotečne) resurse s udaljenih mjesta mogu biti instalirane na računalu korisnika, a može im se pristupati udaljeno. Aplikacije koje su instalirane na računalu korisnika izvode lokalno sve osnovne operacije čitanja i ažuriranja udaljenih podatkovnih resursa. Programske operacije koje se izvode na lokalnom računalu koristeći radnu memoriju i sekundarne nosioce podataka, brže se izvode od programskih operacija koje koriste udaljene podatkovne resurse. Propusnost internih računalnih sabirnica veća je od propusnosti mrežnih komponenti. Za komunikaciju prema sekundarnim nosiocima podataka računalo često koristi SATA, SCSI ili

¹ Bacc. inf., policijski tehničar za održavanje EOP opreme, MUP RH PU primorsko-goranska, Ulica žrtava fašizma 3, Rijeka, Hrvatska. E-mail: silvano.culinovic@gmail.com

² Mr. sc., viši predavač, Veleučilište u Rijeci, Vukovarska 58, Rijeka, Hrvatska. E-mail: mkaluza@veleri.hr

³ Asistent, Veleučilište u Rijeci, Vukovarska 58, Rijeka, Hrvatska. E-mail: dliveric@veleri.hr

⁴ Datum primitka rada: 16. 2. 2014.; datum prihvaćanja rada: 5. 5. 2014.

USB sabirnice kojima je propusnost uglavnom višestruko veća od 480 Mbps, što je brzina USB 2.0 sabirnice. S druge strane propusnosti dostupnih i korištenih mreža su uglavnom niže od propusnosti 100 Mbps LAN mreže. Komunikacijski kanal aplikacije s udaljenim podatkovnim resursima koristi mrežne resurse korisničkog računala i time predstavlja najsporiju aplikacijsku komponentu sustava. S druge strane, aplikacije kojima korisnik pristupa udaljeno ne izvode se na računalu korisnika, a korisniku je dostupno sučelje korištenja aplikacijskih operacija. Upravo komunikacija korisničkog sučelja s udaljenim aplikacijskim poslužiteljem također koristi mrežne resurse i time predstavlja najsporiju aplikacijsku komponentu sustava.

Bez obzira na lokaciju izvođenja aplikacije, komunikacija korisnika sa sustavom koristi mrežne resurse korisničkog računala i provodi se standardiziranim mrežnim protokolima.

Komunikacija između dvaju računala, prema OSI modelu, provodi se kroz sedam slojeva. Ti slojevi su (počevši od najnižega): fizički (engl. *physical*), podatkovni (engl. *data link*), mrežni (engl. *network*), transportni (engl. *transport*), sesijski (engl. *session*), prezentacijski (engl. *presentation*) i aplikacijski (engl. *application*) (Dulaney, Harwood, 2012:45). Kada aplikacijski (vršni) korisnički sloj na jednom računalu provodi komunikaciju s aplikacijskim slojem na drugom računalu koriste se unaprijed definirani komunikacijski mehanizmi (protokoli) nižih razina. Neki od TCP/IP protokola koji se koriste na aplikacijskom sloju su: FTP, SFTP, HTTP/S (Dulaney, Harwood, 2012:69-70).

Protokoli koji se u radu analiziraju koriste različite mehanizme za osiguranje povjerljivosti i integriteta paketa (certifikati, privatni ključevi, enkriptirana veza itd.). Protokoli koji koriste potpunije (opširnije) sigurnosne mehanizme su opisom veći (širi), a time je i paket fizički teži (ima više bajtova), pa se može pretpostaviti da će i vrijeme potrebno za prijenos podataka (datoteka) biti dulje, odnosno proces prijena sporiji.

Kako mrežna komunikacija predstavlja najsporiju aplikacijsku komponentu sustava, u komunikaciji je potrebno koristiti što brže komunikacijske protokole.

Udaljeni podatkovni ili aplikacijski poslužitelj ne mora biti u LAN mreži korisnika, može biti dostupan kroz WAN mrežu. Komunikacija korisnika sa sustavom provodi se putem nezaštićenog kanala, pa je potrebno koristiti što sigurnije komunikacijske protokole. Radom će se analizirati sigurnosni mehanizmi dostupnih i često korištenih protokola za prijenos datoteka. Pokazat će se koji protokoli zadovoljavaju sigurnosne zahtjeve u komunikaciji.

Izmjerit će se vrijeme prijena i prosječna brzina prijena datoteka pomoću analiziranih protokola. Zbog kombiniranja različitih „nižih“ protokola u osnovnim aplikacijskim protokolima s ciljem osiguranja komunikacije, izmjerit će se vrijeme i prosječna brzina prijena na različitim mrežama.

Radom će se pokazati da su protokoli koji koriste sigurnosne mehanizme apsolutno sporiji od protokola koji ne koriste sigurnosne mehanizme. Istražit će se koji protokol i u kojim mrežnim uvjetima postiže najbolje rezultate - najviša razina sigurnosti i najveća brzina.

2. PROTOKOLI ZA PRIJENOS DATOTEKA

2.1 FTP

Standardizirani protokol koji se koristi za prijenos datoteka. Baziran je na arhitekturi klijent-poslužitelj, pri čemu, u ovisnosti o konfiguraciji, poslužitelj može zahtijevati autentifikaciju ili pristup može biti anoniman pa ona nije potrebna. Najčešće se koristi dedicerani port 21.

Prilikom dizajna ovog protokola u obzir nisu uzeti sigurnosni standardi pa tako protokol ne provodi enkripciju podataka. Drugim riječima, putem dostupnih softvera za presretanje mrežnih paketa moguće je, u tekstualnom obliku, pročitati naredbe, korisničko ime, zaporku, sadržaj datoteka itd. Neki od sigurnosnih propusta su (Allman, Ostermann, 1999):

- *bounce* napad
- *brute force* napad
- presretanje paketa
- krađa dediceranog porta
- *spoof* napadi.

2.2 FTPS

S obzirom na brojne sigurnosne propuste FTP protokola, pojavila se potreba za njegovom „nadogradnjom“. Jedan od načina ublažavanja potencijalnih napada tijekom otvorene sesije je korištenje sigurnosnog protokola za enkripciju podataka koji se prenose između klijenta i poslužitelja. FTPS koristi TLS ili SSL sigurnosni protokol.

SSL protokol kreirao je Netscape. Posljednja verzija je SSL 3.0 koja datira iz 1999. godine. Kao odgovor na SSL protokol, a potaknuto zahtjevom za standardiziranim protokolom, IETF (engl. *Internet Engineering Task Force*)⁵ kreirao je TLS protokol. Prva verzija TLS protokola izdana je 1999. godine, a posljednja verzija TLS 1.2 datira iz 2008. godine. TLS pruža sljedeća svojstva (Ford-Hutchinson, 2005):

- fleksibilna razina sigurnosti, podržava povjerljivost, integritet, autentifikaciju ili njihovu kombinaciju, što tijekom sesije omogućuje da klijent i poslužitelji dinamički odlučuju o potrebnoj razini sigurnosti za specifičan prijenos datoteka
- pruža snažniju autentifikaciju na FTP poslužitelju
- formalizirano upravljanje javnim ključem (engl. *public key*), korištenjem utvrđenih mehanizama identifikacije klijenata u fazi autentifikacije, u središnju funkciju može biti ugrađeno upravljanje certifikatom
- kompatibilnost s autentifikacijskim mehanizmima koji se već koriste unutar HTTP protokola, što *web*-preglednicima omogućuje ugradnju sigurnog prijenosa datoteka korištenjem iste postavljene infrastrukture koja omogućuje sigurno pregledavanje *web*-sadržaja.

Osnovna zadaća TLS protokola je pružanje privatnosti i integriteta podataka između klijenta i poslužitelja. Sastoji se od dvaju slojeva - TLS Record protokol i TLS Handshake protokol.

⁵ <http://www.ietf.org/>

TLS Record protokol omogućuje sigurnost veze koji ima dva osnovna svojstva:

- veza je privatna, koristi se simetrična kriptografija za enkripciju podataka, ključevi su jedinstveni za svaku vezu i bazirani su na TLS Handshake protokolu
- veza je pouzdana, prijenos poruka uključuje provjeru integriteta poruke korištenjem *hash* funkcija (SHA, MD5 itd.).

TLS Record protokol može se koristiti bez enkripcije i bez *hash* funkcije. Nadalje, koristi se prilikom enkapsulacije različitih protokola na višim razinama, kao npr. TLS Handshake protokol.

TLS Handshake protokol omogućuje autentifikaciju između klijenta i poslužitelja te njihov „dogovor“ oko korištenog enkripcijskog algoritma i kriptografskih ključeva prije nego aplikacijski protokol pošalje ili primi prve podatke. Protokol pruža sigurnost veze uz tri osnovna svojstva:

- provjera autentičnosti može se utvrditi korištenjem asimetrične kriptografije (javnog ključa)
- nije moguće presresti „dogovorenu“ lozinku (engl. *shared secret*)
- „dogovaranje“ je pouzdano, napadač ne može mijenjati dogovorenu komunikaciju bez da bude otkriven.

Sigurnosnim mehanizmima koje koristi ovaj protokol umanjuje se zlonamjerno iskorištavanje ranije navedenih sigurnosnih propusta FTP protokola. Najčešće se koristi dedicerani port 990.

2.3 SFTP

SFTP protokol i FTP protokol nisu kompatibilni. SFTP softver ne može se koristiti za siguran pristup FTP poslužitelju. SFTP protokol, nadalje, ne posjeduje niti jednu sigurnosnu značajku. Za sigurnost je zadužen SSH protokol (Barrett, 2005:81-82). Najčešće se koristi dedicerani port 22.

SSH protokol pojavio se 1995. godine u verziji SSH-1. Kako se povećavao broj aktivnih korisnika, otkriveni su brojni propusti i nedostaci, što je rezultiralo razvojem i standardizacijom SSH-2 protokola od strane Secure Shell (SECSH) radne skupine osnovane pri IETF-u.

SSH protokol omogućuje korištenje sigurnih mrežnih servisa korištenjem nesigurnih (javnih) mreža. Sastoji se od triju glavnih komponenti (Ylonen, Lonvick, 2006):

- SSH-TRANS protokol pruža autentifikaciju poslužitelja, povjerljivost i integritet, te opcionalno i kompresiju
- SSH-USERAUTH protokol služi za autentifikaciju klijentskih računala na poslužitelju
- SSH-CONNECT protokol provodi multipleksiranje enkriptiranog tunela u nekoliko logičkih kanala.

SFTP protokol omogućuje siguran prijenos datoteka, pod pretpostavkom da se koristi siguran komunikacijski kanal koji je omogućen korištenjem SSH-2 protokola. SFTP protokol radi na principu *request-response* modela, pri čemu postoji velik broj *request* poruka, ali mali broj mogućih *response* poruka (Galbraith, Saarenmaa, 2006).

2.4 FTP preko HTTP-a

Kombinacijom FTP i HTTP protokola, moguć je prijenos datoteka korištenjem *web*-preglednika. *Web*-preglednik omogućuje pristup FTP poslužitelju neovisno o uređaju kojim se pristupa (pametni telefon, desktop/tablet/prijenosno računalo), neovisno o operacijskom sustavu (Windows, MacOS, Linux, Android, iOS itd.). *Web*-preglednik prikazuje korisničko sučelje sustava kojem korisnik pristupa.

Ovakav pristup FTP poslužitelju nije zaštićen. Uz ranije navedene sigurnosne propuste samog FTP protokola, kako se radi o *web*-aplikaciji, mogući su i DoS napadi. Najčešće se koristi HTTP dedicerani port 80.

2.5 FTP preko HTTPS-a

Razvojem interneta kao medija sve veći broj osjetljivih *web*-aplikacija (bankarske usluge i sl.) ukazuje na brojne sigurnosne propuste i nedostatke HTTP protokola. Kao odgovor stvoren je HTTPS protokol koji omogućuje enkripciju podataka korištenjem TLS/SSL protokola. HTTPS protokol je ustvari HTTP protokol zaštićen SSL/TLS protokolom.

Na nižoj razini aplikacijskog sloja OSI modela kreira se sigurna enkriptirana veza korištenjem SSL/TLS protokola. Pri prijenosu podataka cjelokupan HTTP promet (zaglavlje paketa, *get/post* zahtjevi, URL, podaci itd.) šalju se kroz zaštićeni SSL/TLS tunel.

S obzirom na to da HTTPS koristi iste sigurnosne mehanizme kao i FTPS protokol, može se reći da je ovo *web*-inačica FTPS protokola. I u tom slučaju *web*-aplikacija zamjenjuje klijentski softver. Najčešće se koristi dedicerani port 443.

2.6 Druge značajke mreže u prijenosu podataka

Svaki od protokola na podatkovnom sloju OSI modela ima definiranu veličinu okvira za podatke koji se prenose. Unutar Ethernet LAN mreže, definirana veličina okvira je 1.500 bajtova. Kako bi se omogućilo korištenje IP protokola neovisno o fizičkoj mreži, definirano je visoko ograničenje na veličinu IP okvira 65.535 bajtova. S obzirom na to da su veličine okvira na podatkovnom sloju manje od veličine okvira IP protokola, IP okvir se u prijenosu fragmentira na pakete veličine okvira podatkovnog sloja.

Proces fragmentacije IP okvira odvija se na transportnom sloju OSI modela, pri čemu svaki od fragmenata postaje zaseban paket. Zbog preusmjeravanja, na putu od izvora do odredišta paketi promijene nekoliko različitih mreža (WAN), pri čemu na svakom usmjerivaču (engl. *routeru*) dolazi do dekapulacije (raspakiravanja) paketa, obrade i ponovne enkapsulacije (pakiranja) paketa. Zbog razlike u veličini okvira podatkovnog sloja mreže u kojoj se paket nalazi može doći do daljnje fragmentacije.

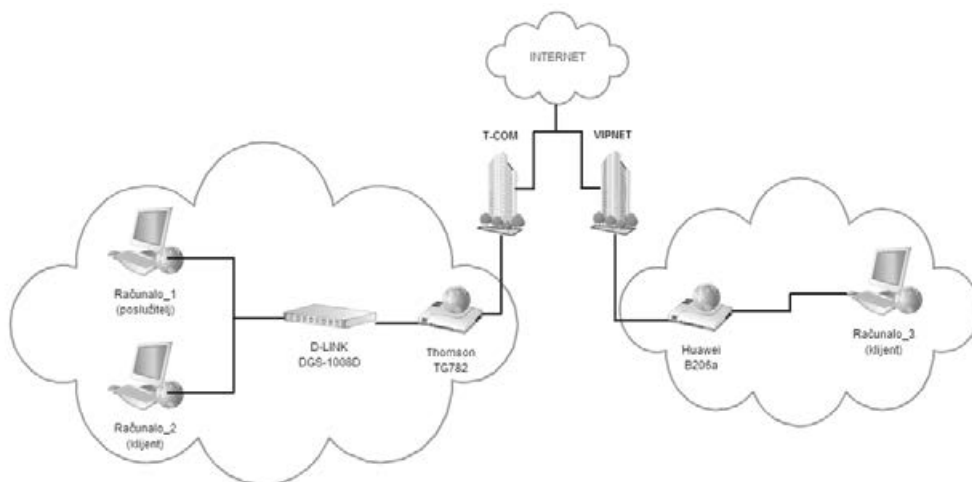
Fragmenti mogu putovati različitim putovima (rutama) od izvora do odredišta, postoji mogućnost gubitka paketa pa ih je potrebno ponovno poslati. Ponovno povezivanje fragmenata obavlja se isključivo na odredištu (Forouzan, 2010:193).

Kako bi se omogućio prijenos većih okvira, na gigabitnoj mrežnoj opremi (mrežne kartice, preklopnici, usmjerivači) moguće je povećati veličinu okvira do najviše 9.000 bajtova. Kako ne bi dolazilo do daljnje fragmentacije, sva korištena oprema unutar LAN mreže morala bi podržavati okvire ove veličine.

3. OPIS TESTNOG OKRUŽENJA

Testno okruženje sastoji se od tri osobna računala različitih tehničkih karakteristika. Temeljeno je na arhitekturi klijent-poslužitelj. Jedno od računala predstavlja poslužiteljsko računalo, dok ostala dva predstavljaju klijentska računala koja će se pomoću klijentskog softvera povezivati s poslužiteljem te prenositi testne datoteke.

Slika 1. Mrežna infrastruktura



Izvor: obrada autora

Računalna mreža (slika 1) sastoji se od dviju geografski odvojenih LAN mreža. Lokacije imaju različitog pružatelja internetskih usluga. Na jednoj lokaciji poslužitelj internetskih usluga je T-COM, a na drugoj VIPNET. Obje lokacije imaju različite brzine pristupa. Jedna lokacija ima brzinu od 10 Mbps *download* i 640 kbps *upload*, dok na drugoj lokaciji, zbog ograničenja mobilnog operatera (kapacitet bazne stanice, broj aktivnih korisnika itd.) brzina varira od 1 Mbps - 2 Mbps za *download* i *upload*. Kako bi se ispitale brzine prijenosa datoteka pri različitim propusnostima LAN mreže (10/100/1000 Mbps), koristi se D-LINK DGS-1008D, gigabitni mrežni preklopnik (engl. *switch*). Za kreiranje VPN veze korišten je VPN softver koji je integralni dio Microsoft Windows operacijskog sustava, koji na podatkovnom sloju OSI modela koristi PPTP protokol (engl. *point-to-point tunneling protocol*), čime se ostvaruje sigurna veza između dviju udaljenih lokacija.

Na poslužiteljsko računalo instaliran je softver Serv-U⁶. To je komercijalni FTP poslužitelj koji podržava FTP, FTPS (TLS/SSL) i SFTP (SSH2) protokole za prijenos datoteka korištenjem klijentskih softvera, te HTTP/S za prijenos datoteka putem *web*-preglednika. Budući da se namjeravaju koristiti FTPS, HTTPS i SFTP protokoli, kreiran je certifikat i privatni ključ za FTPS i HTTPS protokole te privatni ključ za SFTP protokol.

Za pristup poslužitelju i prijenos datoteka korišten je WinSCP⁷, besplatan klijentski softver otvorenog koda koji putem grafičkog korisničkog sučelja omogućuje FTP, FTPS i SFTP pristup poslužitelju ili udaljenom računalu, te osnovne funkcionalnosti za rad s datotekama (engl. *file manager*).

4. OPIS TESTNIH SLUČAJA

Prilikom izvođenja inicijalnih testova i provjera uočeno je da, neovisno o propusnosti mreže, brzina prijenosa nije konstantna. Tako je prilikom prijenosa datoteka uočena razlika u brzini prijenosa. Shodno tome, odabran je uzorak od deset kopiranja.

S obzirom na to da se provjeravala brzina prijenosa korištenjem različitih protokola te različitih propusnosti WAN i LAN mreže, pri manjim propusnostima mreže nisu se prenosile sve datoteke nego samo one čiji se prijenos obavio u prihvatljivom vremenskom razdoblju.

Tijekom izvođenja testova s udaljene lokacije (WAN mreža), zbog propusnosti koja varira od 1 Mbps (cca 125 KB/s) do 2 Mbps (cca 250 KB/s) nisu se vršili prijenosi datoteka većih od 10 MB.

Tijekom izvođenja testova unutar LAN mreže, pri propusnosti od 10 Mbps (cca 1,25 MB/s) nisu se vršili prijenosi datoteka većih od 100 MB.

Pri propusnosti od 100 Mbps (cca 12,5 MB/s) nisu se vršili prijenosi datoteka većih od 1 GB, dok su se pri propusnosti od 1 Gbps (cca 125 MB/s) vršili prijenosi svih datoteka.

Log datoteka Serv-U poslužitelja koristila se kao mjerni instrument. Zapisano je vrijeme početka i vrijeme završetka kopiranja svake datoteke. Vrijeme je zapisano u obliku „YYYYmmdd HH:mm:ss“. Dakle, mjerni instrument može izmjeriti prijenos datoteke koji će trajati više od jedne sekunde. To predstavlja točnost instrumenta mjerenja.

U postupku mjerenja provodila se sljedeća procedura:

⁶ <http://www.serv-u.com/>

⁷ <http://winscp.net/eng/index.php>

1. podešavanje propusnosti LAN mreže (10/100/1000 Mbps)
2. uspostava veze FTP/FTPS/SFTP/HTTP/HTTPS protokolom
3. kreiranje mape na poslužitelju ovisno o trenutno korištenom protokolu
4. kreiranje mape na poslužitelju ovisno o trenutnom rednom broju kopiranja
5. prijenos datoteka
6. prekid veze po završetku kopiranja svih datoteka
7. spremanje log datoteke poslužitelja.

5. REZULTATI MJERENJA

Prema prije definiranom postupku izvršeno je mjerenje brzine i trajanja prijenosa datoteka između dvaju računala. U tablici 1 prikazane su prosječne vrijednosti brzine prijenosa i prosječno vrijeme trajanja prijenosa datoteka po svim promatranim protokolima, u LAN mreži propusnosti od 10 Mbps.

Tablica 1. LAN mreža 10 Mbps, rezultati mjerenja

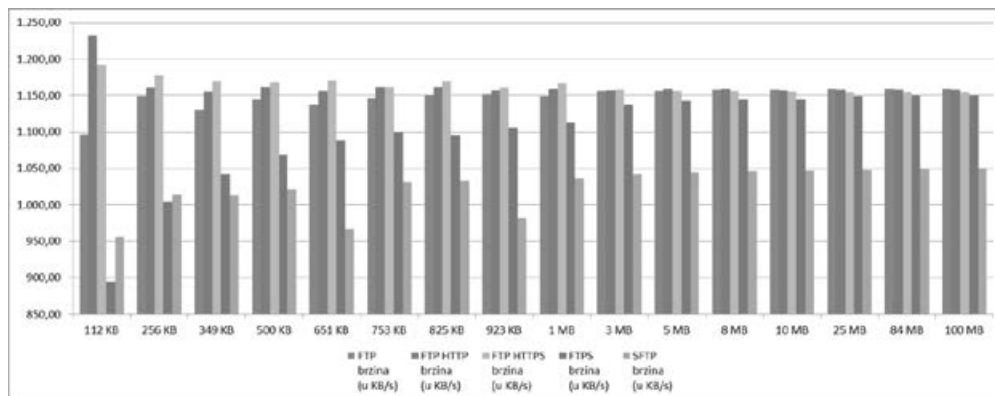
veličina datoteke	FTP vrijeme	FTP brzina (u KB/s)	FTP HTTP vrijeme	FTP HTTP brzina (u KB/s)	FTP HTTPS vrijeme	FTP HTTPS brzina (u KB/s)	FTPS vrijeme	FTPS brzina (u KB/s)	SFTP vrijeme	SFTP brzina (u KB/s)
112 KB	00:00	1.095,67	00:00	1.232,14	00:00	1.191,70	00:00	894,23	00:00	956,17
256 KB	00:00	1.148,62	00:00	1.161,07	00:00	1.177,88	00:00	1.004,56	00:00	1.014,35
349 KB	00:00	1.130,29	00:00	1.155,10	00:00	1.170,01	00:00	1.042,48	00:00	1.013,17
500 KB	00:01	1.144,95	00:01	1.161,52	00:00	1.168,34	00:01	1.069,11	00:00	1.021,29
651 KB	00:00	1.137,50	00:00	1.156,52	00:00	1.170,37	00:01	1.087,60	00:01	966,50
753 KB	00:01	1.146,88	00:01	1.162,08	00:01	1.161,47	00:01	1.099,76	00:01	1.031,40
825 KB	00:01	1.149,83	00:01	1.161,91	00:01	1.169,46	00:01	1.095,04	00:01	1.032,73
923 KB	00:01	1.151,12	00:01	1.156,74	00:01	1.161,20	00:01	1.105,92	00:01	982,15
1 MB	00:01	1.149,30	00:01	1.158,81	00:01	1.166,92	00:01	1.112,57	00:01	1.036,86
3 MB	00:03	1.156,33	00:03	1.156,78	00:03	1.158,06	00:03	1.137,64	00:03	1.042,46
5 MB	00:04	1.156,55	00:05	1.158,41	00:04	1.155,82	00:05	1.142,38	00:05	1.044,93
8 MB	00:07	1.157,70	00:07	1.158,26	00:07	1.156,46	00:07	1.145,32	00:08	1.046,28
10 MB	00:09	1.157,86	00:09	1.157,25	00:09	1.155,33	00:09	1.145,35	00:10	1.046,73
25 MB	00:22	1.158,50	00:22	1.157,91	00:22	1.154,86	00:22	1.148,94	00:24	1.048,11
84 MB	01:14	1.158,64	01:15	1.157,71	01:15	1.154,83	01:15	1.149,96	01:22	1.048,88
100 MB	01:28	1.158,66	01:28	1.157,70	01:29	1.154,86	01:29	1.150,13	01:37	1.049,68

Izvor: obrada autora

Propusnost takve mreže je cca 1,25 Mb/s, a kako je mjerni instrument ograničen na minimalno 1 s promjene, podaci datoteka koje su manje od 1 Mb ne mogu biti točni, pa se isključuju iz daljnje analize.

Prosječne brzine prijenosa datoteka većih od 1 Mb variraju od 1036,86 kB/s do 1.166,92 kB/s po svim promatranim protokolima. To pokazuje visoku podudarnost brzina prijenosa svih protokola.

Slika 2. LAN 10 Mbps, brzina prijenosa



Izvor: obrada autora

Na slici 2 vidljivo je da kod prijenosa datoteka manjih od 1 MB, zbog kratkog vremena koje je potrebno za prijenos (oko jedne sekunde), dolazi do većih odstupanja u brzini prijenosa. Kod prijenosa datoteka većih od 1 MB zbog dužeg trajanja samog prijenosa, odstupanja u brzini prijenosa su unutar prihvatljivih $\pm 1\%$ (cca 10 kB/s).

Prema slici 2, SFTP protokol je značajnije sporiji od ostalih. Najbrži protokoli su uglavnom nesigurni FTP i FTP-HTTP. Sigurni FTP HTTPS i FTSP su sporiji do 1 % (cca 10 kB/s). S obzirom na to da ne postoji značajna razlika u brzini prijenosa pomoću sigurnih protokola u odnosu na brzinu prijenosa pomoću nesigurnih protokola, optimalno rješenje je korištenje sigurnih FTP HTTPS i FTSP protokola, a pritom je veće brzine prijenosa ostvario FTP HTTPS protokol.

Drugo mjerenje brzine protokola izvršeno je u lokalnoj mreži na brzini od 100 Mbps. Tablica 2 pokazuje rezultate tog mjerenja.

Tablica 2. LAN mreža 100 Mbps, rezultati mjerenja

veličina datoteke	FTP vrijeme	FTP brzina (u KB/s)	FTP HTTP vrijeme	FTP HTTP brzina (u KB/s)	FTP HTTPS vrijeme	FTP HTTPS brzina (u KB/s)	FTSP vrijeme	FTSP brzina (u KB/s)	SFTP vrijeme	SFTP brzina (u KB/s)
112 KB	00:00	1.238,08	00:00	1.133,62	00:00	6.442,48	00:00	803,04	00:00	6.077,20
256 KB	00:00	11.435,70	00:00	9.690,41	00:00	13.839,06	00:00	5.061,22	00:00	5.739,78
349 KB	00:00	10.874,81	00:00	11.823,38	00:00	12.235,30	00:00	5.684,28	00:00	5.477,82
500 KB	00:00	10.684,55	00:00	14.944,11	00:00	11.608,35	00:00	6.562,89	00:00	5.663,64
651 KB	00:00	10.938,16	00:00	11.673,89	00:00	11.437,93	00:00	8.150,24	00:00	4.842,37
753 KB	00:00	11.052,25	00:00	11.616,68	00:00	11.516,24	00:00	7.742,62	00:00	5.561,80
825 KB	00:00	10.849,87	00:00	10.754,18	00:00	11.413,77	00:00	8.485,51	00:00	5.465,60
923 KB	00:00	11.048,77	00:00	10.976,62	00:00	10.777,79	00:00	8.479,23	00:00	5.047,76
1 MB	00:00	10.940,47	00:00	11.878,02	00:00	10.203,41	00:00	8.961,48	00:00	5.464,29
3 MB	00:00	11.517,73	00:01	9.977,79	00:00	9.705,55	00:00	10.478,82	00:00	5.455,74
5 MB	00:00	11.522,21	00:00	10.037,55	00:01	9.691,66	00:01	10.802,45	00:01	5.517,65
8 MB	00:01	11.416,38	00:01	11.407,74	00:01	11.077,80	00:00	11.011,40	00:01	5.432,62
10 MB	00:01	11.494,31	00:01	11.485,61	00:01	11.145,34	00:01	11.146,59	00:03	3.415,49
25 MB	00:02	11.540,46	00:02	11.501,22	00:02	11.217,47	00:03	11.348,76	00:06	4.458,31
84 MB	00:08	11.557,26	00:08	11.487,56	00:08	11.236,93	00:07	11.429,96	00:22	3.892,61
100 MB	00:09	11.554,46	00:09	11.519,33	00:09	11.290,01	00:09	11.437,65	00:29	3.547,12
550 MB	00:49	11.506,36	00:49	11.534,67	00:50	11.322,33	00:49	11.456,78	-	-
650 MB	00:58	11.552,66	00:58	11.522,78	00:59	11.330,32	00:58	11.449,59	-	-
900 MB	01:20	11.548,32	01:20	11.543,10	01:21	11.336,92	01:21	11.447,86	-	-
1 GB	01:30	11.550,55	01:31	11.553,78	01:33	11.322,90	01:33	11.277,73	-	-

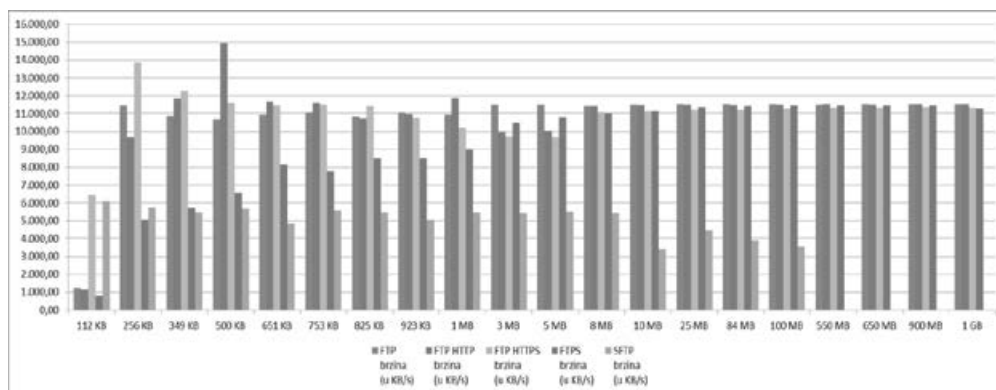
Izvor: obrada autora

Tablica 2 pokazuje prosječno vrijeme i prosječnu brzinu prijenosa datoteka po promatranim protokolima u LAN mreži na brzini od 100 Mbps. Propusnost mreže je cca 12,5 Mb/s, a kako je mjerni instrument ograničen na minimalno 1 s promjene, podaci datoteka koje su manje od 12 Mb ne mogu biti točni, pa se isključuju iz daljnje analize.

Može se uočiti da je prosječna brzina prijenosa korištenjem SFTP protokola nekoliko puta manja u odnosu na prosječne brzine prijenosa prilikom korištenja ostalih protokola. Razlika pogotovo dolazi do izražaja tijekom prijenosa većih datoteka (10 MB i više) kada se prosječno vrijeme prijenosa povećalo za tri puta u odnosu na prosječna vremena prilikom korištenja ostalih protokola. Brzina prijenosa datoteka SFTP protokolom je cca 3 puta manja od ostalih protokola, pa se SFTP protokol isključuje iz daljnje analize. Tijekom daljnjih testiranja korištenjem SFTP protokola nisu se prenosile datoteke veće od 100 MB.

Prosječne brzine prijenosa datoteka većih od 10 MB variraju od 11.217,47 kB/s do 11.557,26 kB/s na preostala 4 protokola, što pokazuje visoku podudarnost brzina prijenosa datoteka pomoću njih.

Slika 3. LAN 100 Mbps, brzina prijenosa



Izvor: obrada autora

Na slici 3 vidljivo je da kod prijenosa datoteka manjih od 10 MB, zbog kratkog vremena koje je potrebno za prijenos (oko jedne sekunde), dolazi do većih odstupanja u brzini prijenosa. Kod prijenosa datoteka većih od 10 MB zbog dužeg trajanja samog prijenosa, odstupanja u brzini prijenosa su unutar prihvatljivih $\pm 1,5\%$ (cca 150 kB/s).

Prema slici 3, SFTP protokol značajnije je sporiji od ostalih. Najbrži protokoli su uglavnom nesigurni FTP i FTP-HTTP. Sigurni FTP HTTPS i FTPS sporiji su do 2 % (cca 200 kB/s).

S obzirom na to da i u ovom slučaju ne postoji značajna razlika u brzini prijenosa pomoću sigurnih protokola u odnosu na brzinu prijenosa pomoću nesigurnih protokola, kao u sporijoj LAN 10 Mbps mreži, optimalno rješenje je korištenje sigurnih FTP HTTPS i FTPS protokola, a pritom ipak nešto veće brzine prijenosa ostvario je FTPS protokol.

Treće mjerenje brzine protokola izvršeno je u lokalnoj mreži na brzini od 1 Gbps. Tablica 3 pokazuje rezultate tog mjerenja.

Tablica 3. LAN mreža 1000 Mbps, rezultati mjerenja

veličina datoteke	FTP vrijeme	FTP brzina (u KB/s)	FTP HTTP vrijeme	FTP HTTP brzina (u KB/s)	FTP HTTPS vrijeme	FTP HTTPS brzina (u KB/s)	FTPS vrijeme	FTPS brzina (u KB/s)	SFTP vrijeme	SFTP brzina (u KB/s)
112 KB	00:00	999,86	00:00	2.866,80	00:00	1.938,43	00:00	772,13	00:00	4.783,02
256 KB	00:00	13.758,28	00:00	5.012,92	00:00	13.518,36	00:00	7.723,32	00:00	5.470,49
349 KB	00:00	19.047,24	00:00	11.188,18	00:00	21.955,21	00:00	9.771,18	00:00	5.172,46
500 KB	00:00	22.284,95	00:00	22.843,67	00:00	29.945,12	00:00	12.130,23	00:00	5.026,66
651 KB	00:00	22.489,59	00:00	19.151,09	00:00	24.292,89	00:00	11.868,44	00:00	5.001,19
753 KB	00:00	26.653,57	00:00	4.252,71	00:00	44.569,48	00:00	14.497,08	00:00	4.664,09
825 KB	00:00	29.368,45	00:00	19.312,84	00:00	40.253,53	00:00	15.015,44	00:00	4.579,84
923 KB	00:00	35.741,44	00:00	26.037,42	00:00	28.969,18	00:00	15.742,82	00:01	4.185,52
1 MB	00:00	26.847,92	00:00	44.800,40	00:00	29.950,88	00:00	14.860,01	00:00	5.338,22
3 MB	00:00	30.151,83	00:00	73.439,40	00:00	32.236,55	00:00	19.734,59	00:01	5.627,10
5 MB	00:00	34.916,15	00:00	77.340,55	00:00	35.618,43	00:00	21.524,14	00:01	5.659,96
8 MB	00:00	31.924,42	00:00	83.924,66	00:00	38.403,19	00:00	22.357,64	00:02	5.344,72
10 MB	00:00	37.586,44	00:00	68.534,16	00:00	40.616,92	00:00	23.385,10	00:03	3.447,65
25 MB	00:01	36.671,92	00:01	77.878,24	00:01	46.491,99	00:01	23.992,29	00:06	4.434,52
84 MB	00:01	80.508,84	00:01	66.488,91	00:02	42.387,52	00:04	24.446,33	00:22	3.840,04
100 MB	00:01	76.663,58	00:01	68.652,86	00:02	42.226,60	00:04	24.377,09	00:29	3.566,48
550 MB	00:05	105.866,55	00:09	61.251,70	00:14	40.236,55	00:23	24.631,74	-	-
650 MB	00:07	98.933,60	00:11	61.200,33	00:17	40.508,19	00:27	24.680,79	-	-
900 MB	00:09	105.014,02	00:15	60.578,79	00:23	40.079,50	00:37	24.902,19	-	-
1 GB	00:10	104.724,06	00:17	61.364,86	00:26	40.231,50	00:43	24.753,84	-	-
4.8 GB	00:42	110.738,77	-	-	-	-	-	-	-	-
8.5 GB	01:15	110.705,22	-	-	-	-	-	-	-	-
10 GB	01:35	111.270,94	-	-	-	-	-	-	-	-

Izvor: obrada autora

Tablica 3 pokazuje prosječno vrijeme i prosječnu brzinu prijenosa datoteka po promatranim protokolima u LAN mreži na brzini od 1 Gbps. Propusnost mreže veća je od 100 Mb/s, a kako je mjerni instrument ograničen na minimalno 1 s promjene, podaci datoteka koje su manje od 100 Mb ne mogu biti točni, pa se isključuju iz daljnje analize.

Prilikom korištenja FTP protokola postiže se skoro maksimalna brzina prijenosa (preko 100 MB/s).

SFTP protokol je na sporijoj LAN mreži isključen iz analize, pa se i u ovoj analizi isključuje.

Prosječna brzina prijenosa korištenjem FTP preko HTTP je skoro 40 % manja u odnosu na prosječnu brzinu prijenosa prilikom korištenja FTP protokola.

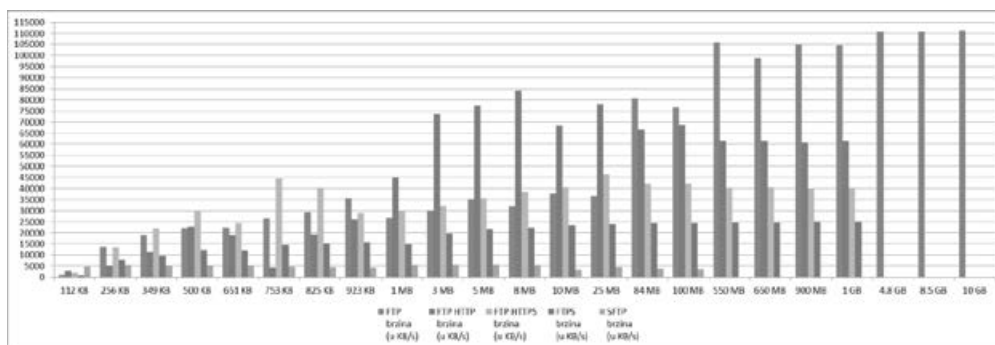
Prosječna brzina prijenosa korištenjem FTP-a preko HTTPS protokola je skoro 60 % manja u odnosu na prosječnu brzinu prijenosa prilikom korištenja FTP protokola.

Prosječna brzina prijenosa korištenjem FTPS protokola je skoro 80 % manja u odnosu na prosječnu brzinu prijenosa prilikom korištenja FTP protokola.

S obzirom na neočekivano velike razlike prosječnih brzina prijenosa, u nastavku testiranja korištenjem FTP-a preko HTTP-a, FTP preko HTTPS-a te FTPS protokola nisu se prenosile datoteke veće od 1 GB, dok se prilikom testiranja korištenjem SFTP protokola nisu prenosile datoteke veće od 100 MB.

Kod prijenosa datoteka većih od 100 MB zbog dužeg trajanja samog prijenosa, odstupanja u brzini prijenosa su unutar prihvatljivih $\pm 1\%$ (< 1 MB/s) za protokole FTP HTTP, FTP HTTPS i FTPS te 5,54% za FTP protokol.

Slika 4. LAN 1000 Mbps, brzina prijenosa



Izvor: obrada autora

Na slici 4 vidljivo je da kod prijenosa datoteka manjih od 100 MB, zbog kratkog vremena koje je potrebno za prijenos (oko jedne sekunde), dolazi do većih odstupanja u brzini prijenosa. Prema slici 3 FTP protokol je najbrži. FTP HTTP i FTP HTTPS značajnije su sporiji od FTP protokola. FTPS protokol je do 4 puta sporiji od FTP protokola.

Postoji značajna razlika u brzini prijenosa pomoću sigurnih protokola u odnosu na brzinu prijenosa pomoću nesigurnih protokola. Brzine prijenosa su visoke (sve iznad 20 Mbps), a datoteke koje su se prenosile su veće od 100 MB.

Ovakva brzina mreže može se ostvariti isključivo u LAN uvjetima. Najčešće se takve brzine postavljaju kao tzv. „LAN backbone“ između poslužitelja, a rjeđe u komunikaciji između klijenta i poslužitelja, pa u tom slučaju postoji manja potreba za korištenjem sigurnih protokola. Kako su brzine koje su ostvarene korištenjem sigurnih protokola (bez SFTP protokola) iznad 20 Mbps, a rijetki su slučajevi prijenosa toliko velikih datoteka (> 100 MB) i pritom se takvi prijenosi odvijaju u razumnom vremenu od nekoliko sekundi, korištenje sigurnih protokola ne bi trebalo značajnije utjecati na performanse sustava.

Sljedeća mjerenja izvršena su na WAN mreži i to u dva oblika:

- nezaštićeni (otvoreni),
- zaštićeni (osiguran VPN na mrežnoj razini).

Tablica 4 pokazuje rezultate mjerenja prijenosa datoteka u nezaštićenoj WAN mreži.

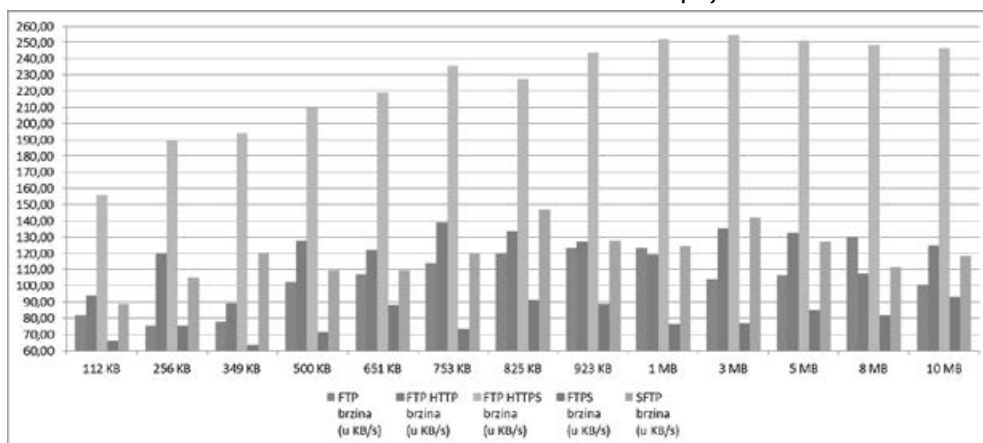
Tablica 4. Nezaštićena WAN mreža, rezultati mjerenja

veličina datoteke	FTP vrijeme	FTP brzina (u KB/s)	FTP HTTP vrijeme	FTP HTTP brzina (u KB/s)	FTP HTTPS vrijeme	FTP HTTPS brzina (u KB/s)	FTPS vrijeme	FTPS brzina (u KB/s)	SFTP vrijeme	SFTP brzina (u KB/s)
112 KB	00:02	81,78	00:01	93,68	00:01	155,83	00:02	66,12	00:01	88,68
256 KB	00:04	75,36	00:03	119,58	00:02	190,20	00:04	75,37	00:02	105,20
349 KB	00:05	77,71	00:05	89,02	00:02	193,96	00:07	63,64	00:03	120,54
500 KB	00:06	102,42	00:04	127,80	00:02	209,79	00:08	71,26	00:05	109,36
651 KB	00:07	107,28	00:06	121,84	00:03	219,06	00:09	88,25	00:06	109,48
753 KB	00:07	113,79	00:08	138,79	00:04	235,53	00:13	73,12	00:07	119,48
825 KB	00:08	119,74	00:08	133,68	00:05	227,27	00:12	90,86	00:06	146,77
923 KB	00:08	123,02	00:10	127,04	00:04	243,48	00:12	88,57	00:08	127,82
1 MB	00:10	123,38	00:11	119,07	00:04	252,08	00:15	76,52	00:09	124,34
3 MB	00:30	104,00	00:27	135,43	00:12	254,48	00:45	76,76	00:23	142,23
5 MB	00:52	106,43	00:45	132,27	00:21	251,30	01:09	84,76	00:41	127,19
8 MB	01:07	129,84	01:26	107,59	00:35	248,28	01:50	81,68	01:19	111,70
10 MB	01:46	100,48	01:33	124,81	00:43	246,56	01:57	92,94	01:37	118,34

Izvor: obrada autora

Tablica 4 pokazuje prosječno vrijeme i prosječnu brzinu prijenosa datoteka po promatranim protokolima u nezaštićenoj WAN mreži. Vidljivo je da je prosječno vrijeme prijenosa datoteka manjih od 1 MB po svim protokolima u prihvatljivim granicama od nekoliko sekundi. Kod prijenosa datoteka većih od 1 MB dolazi do većih odstupanja koja u pojedinim slučajevima iznose i do pola minute. Iz tablice je također vidljivo da po svim protokolima dolazi do većih odstupanja u brzini prijenosa, pogotovo kod FTP HTTPS protokola, gdje je brzina prijenosa čak i dvostruko veća od ostalih protokola. Razlog tome može biti stoga što je korišten posljednji, pri čemu postoji mogućnost da je došlo do rasterećenja mobilne mreže internetskog pružatelja usluge.

Slika 5. Nezaštićena WAN mreža, brzina prijenosa



Izvor: obrada autora

Na slici 5 vidi se da je brzina prijenosa FTP HTTPS protokolom u svim prijenosima više nego dvostruko veća od izmjerenih brzina prijenosa ostalim protokolima. Nadalje, brzina prijenosa FTP protokolom uglavnom je manja od brzine prijenosa FTP HTTP protokolom. Brzina prijenosa FTPS protokolom više je nego dvostruko manja od brzine prijenosa FTP HTTP protokolom. Brzine prijenosa SFTP protokolom uglavnom se podudaraju s brzinama prijenosa FTP HTTP protokolom.

Posljednje mjerenje brzine protokola izvršeno je u WAN zaštićenoj mreži. Tablica 5 pokazuje rezultate tog mjerenja.

Tablica 5. Zaštićena WAN mreža, rezultati mjerenja

veličina datoteke	FTP vrijeme	FTP brzina (u KB/s)	FTP HTTP vrijeme	FTP HTTP brzina (u KB/s)	FTP HTTPS vrijeme	FTP HTTPS brzina (u KB/s)	FTPS vrijeme	FTPS brzina (u KB/s)	SFTP vrijeme	SFTP brzina (u KB/s)
112 KB	00:01	98,81	00:01	95,93	00:02	78,15	00:02	75,08	00:01	84,45
256 KB	00:03	104,52	00:03	120,83	00:04	96,73	00:03	81,17	00:02	112,75
349 KB	00:04	115,45	00:05	104,20	00:04	106,89	00:04	91,33	00:03	114,33
500 KB	00:05	111,34	00:05	121,87	00:05	118,13	00:05	97,87	00:04	121,9
651 KB	00:05	135,89	00:06	125,87	00:08	115,50	00:06	113,17	00:05	118,65
753 KB	00:06	133,43	00:07	140,80	00:07	132,07	00:07	115,21	00:06	112,57
825 KB	00:06	142,74	00:07	139,44	00:07	130,14	00:08	105,27	00:06	116,64
923 KB	00:07	139,39	00:08	142,78	00:08	142,24	00:09	106,02	00:07	114,35
1 MB	00:08	134,22	00:09	156,15	00:10	131,61	00:10	111,45	00:08	116,75
3 MB	00:23	144,53	00:27	133,38	00:30	124,04	00:27	117,53	00:24	123,08
5 MB	00:37	150,37	00:45	128,40	01:02	98,34	00:43	122,18	00:40	125,56
8 MB	01:01	136,65	01:19	113,71	01:19	110,43	01:05	128,34	01:05	125,19
10 MB	01:14	139,56	01:37	118,65	01:51	100,50	01:26	121,22	01:23	123,58

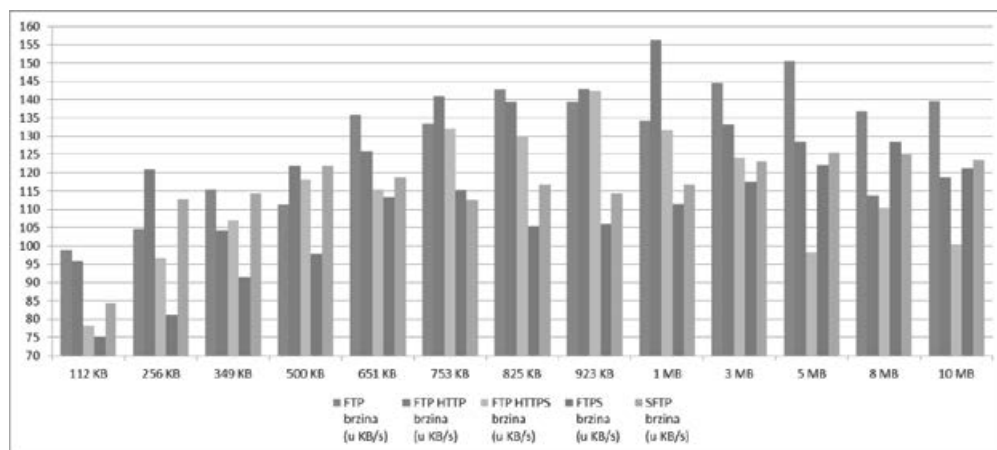
Izvor: obrada autora

Tablica 5 pokazuje prosječno vrijeme i prosječnu brzinu prijenosa datoteka po promatranim protokolima u zaštićenoj WAN mreži.

Propusnost testne mreže za prijenos datoteka od klijenta Računalo 3 do poslužitelja Računalo 1 (slika 1) je minimalno 1 Mbps (128 kbps), a točnost mjernog instrumenta je vremenski period od 1 s. Zbog toga se prijenosi datoteke od 112 kB isključuju iz daljnje analize.

Vidljivo je da, neovisno o korištenom protokolu, ne postoji velika razlika u prosječnom vremenu prijenosa datoteka. Sva odstupanja su unutar prihvatljivih granica od nekoliko sekundi. Prilikom prijenosa većih datoteka (5 MB, 8 MB, 10 MB) primijeti se da je prosječno vrijeme prijenosa datoteka korištenjem FTP HTTPS protokola osjetno duže, pa razlika iznosi i do pola minute u odnosu na prosječno vrijeme prijenosa prilikom korištenja ostalih protokola.

Slika 6. Zaštićena WAN mreža, brzina prijenosa



Izvor: obrada autora

Na slici 6 vidi se da su FTP, FTP HTTP i FTP HTTPS protokoli uglavnom najbrži, a posebno u prijenosu datoteka između 300 kB i 3 MB. Prijenosi datoteka sa SFTP protokolom su uglavnom ujednačenih brzina s prosječnim odstupanjem 8,07 %. Brzine prijenosa datoteka s FTPS protokolom uglavnom se podudaraju brzinama prijenosa sa SFTP protokolom.

Tablica 6 prikazuje najveće i prosječne brzine prijenosa za sve promatrane protokole po svim obavljenim prijenosima.

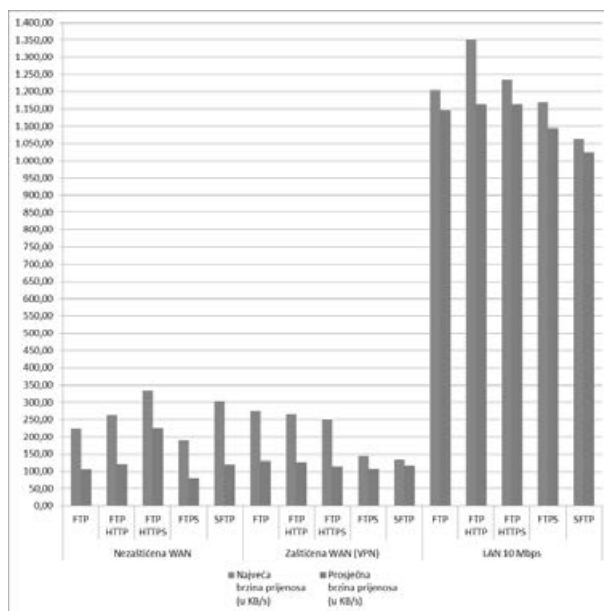
Tablica 6. Usporedni prikaz brzina prijenosa

Tip i propusnost mreže	Protokol	Najveća brzina prijenosa (u KB/s)	Prosječna brzina prijenosa (u KB/s)
Nezaštićena WAN	FTP	223,15	105,02
	FTP HTTP	263,76	120,81
	FTP HTTPS	334,04	225,26
	FTPS	190,06	79,22
	SFTP	302,20	119,32
Zaštićena WAN (VPN)	FTP	274,29	129,76
	FTP HTTP	267,08	126,31
	FTP HTTPS	249,58	114,21
	FTPS	144,98	106,60
	SFTP	132,23	116,14
LAN 10 Mbps	FTP	1.204,30	1.147,40
	FTP HTTP	1.351,39	1.163,12
	FTP HTTPS	1.233,20	1.164,22
	FTPS	1.168,95	1.095,69
	SFTP	1.064,02	1.023,85
LAN 100 Mbps	FTP	17.066,67	10.791,17
	FTP HTTP	21.187,74	10.903,10
	FTP HTTPS	23.269,21	11.007,58
	FTPS	11.592,45	9.160,91
	SFTP	8.258,06	5.066,24
LAN 1000 Mbps	FTP	113.655,69	55.342,07
	FTP HTTP	111.305,18	45.806,02
	FTP HTTPS	52.319,60	33.721,50
	FTPS	31.250,00	18.058,32
	SFTP	7.466,67	4.758,87

Izvor: obrada autora

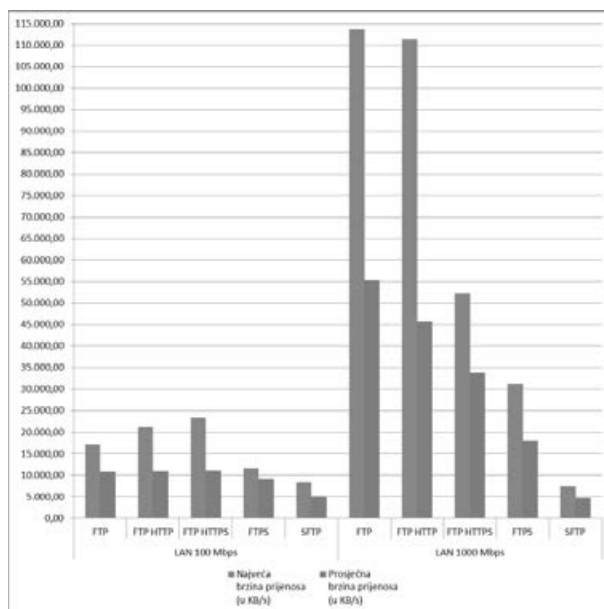
S obzirom na različite čimbenike koji su uključeni u sam proces prijenos datoteka (propusnost mreže, propusnost sabirnice računala, veličina datoteke, sučelje i brzina zapisivanja čvrstog diska, sigurnosni mehanizmi pojedinih protokola) očekivalo se da će biti odstupanja u brzini prijenosa. U tablici 6 odstupanje najveće brzine prijenosa od prosječne po svim testiranim protokolima je od 3,77 % (LAN 10 Mbps, SFTP) do 60,51 % (nezaštićeni WAN, SFTP), a prosječno odstupanje je 36,5%.

Slika 7. Usporedni prikaz brzina prijenosa, propusnost manja od 100 Mbps



Izvor: obrada autora

Slika 8. Usporedni prikaz brzina prijenosa, propusnost veća od 100 Mbps



Izvor: obrada autora

Slike 7 i 8 pokazuju odnos maksimalne i prosječne brzine prijenosa po svim protokolima i mrežama. Pri manjim propusnostima mreže, svi su protokoli ostvarili uglavnom ujednačene brzine prijenosa. Veća razlika u prosječnim brzinama po protokolima vidi se u slučajevima: nezaštićena WAN mreža i LAN 1 Gbps mreža.

Prethodno je pokazano (slike 2 i 3) da na LAN mrežama s propusnostima 10 Mbps i 100 Mbps ne postoji značajna razlika u prosječnoj brzini prijenosa datoteka pomoću sigurnih protokola FTP HTTPS i FTPS u odnosu na nesigurne protokole. Brzina prijenosa datoteka u LAN mreži na brzini od 1 Gbps s protokolima FTP HTTPS i FTPS je značajnije manja od brzine prijenosa s nesigurnim protokolima (slika 4), ali kako se pri takvoj brzini mreže rijetko prenose velike datoteke iznad 100 MB, korištenje sigurnih sporijih protokola FTP HTTP i FTP HTTPS ne bi trebalo previše utjecati na performanse sustava. Ako se LAN 1 Gbps koristi u komunikaciji između poslužitelja, tada sigurnost može biti riješena drugim mehanizmima LAN mreže, pomoću nesigurnog FTP protokola ostvarit će se najveće brzine prijenosa datoteka.

Kod nezaštićene WAN mreže najveće brzine prijenosa (slika 5) ostvarene su pomoću FTP HTTPS protokola. U daljnjim istraživanjima potrebno je ispitati različite WAN mreže (pružatelje usluga), čime će se provjeriti točnost rezultata.

Najbrži prijenosi podataka u zaštićenoj WAN mreži (slika 6) ostvareni su uglavnom pomoću FTP, FTP HTTP i FTP HTTPS protokola. Isti protokoli ostvarili su uglavnom najbolje rezultate na svim nepromjenjivim mrežama (LAN 10 Mbps, 100 Mbps i 1 Gbps).

Kako se prema mjerenjima u nepromjenjivim mrežama (LAN 10 Mbps, 100 Mbps i 1 Gbps) protokol FTP HTTPS pokazao optimalnim u svim slučajevima, a istim je protokolom ostvarena apsolutno najveća brzina prijenosa na nezaštićenoj WAN mreži, i zaštićena WAN mreža ima uglavnom sličan odnos brzina (po protokolima) s nepromjenjivim LAN mrežama, FTP HTTPS protokol predstavlja optimalno rješenje u svim slučajevima prijenosa datoteka.

Kod korištenja LAN ili WAN računalnih mreža čija je propusnost 10 Mbps ili manja, temeljem dobivenih rezultata preporučuje se korištenje nekog od sigurnijih protokola za prijenos datoteka (SFTP, FTPS ili FTP preko HTTPS). Razlika u prosječnom vremenu prijenosa datoteka od nekoliko sekundi je zanemariva, a korištenjem navedenih protokola ostvaruje se sigurnija veza između klijenta i poslužitelja.

Postoji li potreba za razmjenom povjerljivih podataka na geografski udaljenim lokacijama (izdvojeni uredi, poslovnice i sl.), zbog nedovoljne sigurnosti javnih mreža preporučuje se povezivanje u VPN mrežu. VPN omogućuje „siguran“ prijenos podataka.

Kod korištenja LAN računalne mreže čija je propusnost veća od 100 Mbps, razlike u prosječnoj brzini prijenosa datoteka su izraženije. Kada se radi o računalnoj mreži koja je zaštićena od neovlaštenog upada (hardverski i/ili softverski vatrozid i sl.) s pretpostavkom da nitko od korisnika ili zaposlenika neće pratiti mrežni promet i presretati pakete, mogu se koristiti nesigurni protokoli za prijenos datoteka, a posebice FTP s kojim se ostvaruju najveće brzine prijenosa.

S obzirom na drastične razlike u brzini prijenosa pri većim propusnostima računalne mreže, u budućim istraživanjima mogu se ispitati uzroci koji mogu biti:

- zaštitni mehanizmi u vidu dodatnih protokola
- postavke računalne mreže
- interne računalne komponente.

Zbog upitne točnosti rezultata mjerenja na nezaštićenoj WAN mreži potrebno je izvršiti mjerenje na različitim WAN mrežama u nezaštićenom i zaštićenom (VPN) obliku.

6. ZAKLJUČAK

Ovim su radom uspoređeni različiti protokoli koji se na aplikacijskom sloju OSI modela koriste za prijenos podataka. Neki od korištenih protokola (FTP, FTP HTTP) ne posjeduju nikakve zaštitne mehanizme, tj. podatke koji se prenose moguće je presresti i pročitati njihov sadržaj.

Na osnovi jasnih sigurnosnih propusta kreirani su zaštitni mehanizmi u obliku dodatnih protokola (SSL/TLS, SSH itd.). Takvi protokoli dijele zajednički cilj (osiguranje povjerljivosti i integriteta podataka), ali ih ostvaruju na različite načine.

Odabir najprikladnijeg protokola trebao bi ovisiti o namjeni i tipu sustava unutar kojega će se koristiti (prijenos datoteka unutar poslovne ili privatne mreže, *stream* multimedijskog sadržaja, pristup sadržaju internetom i sl.), što bi moglo biti predmet nekih budućih istraživanja.

Kada se govori o računalnim mrežama poznato je da ne postoji apsolutna sigurnost i zaštita od zlonamjernih napada. Korištenjem sigurnosnih mehanizama i protokola potencijalne napadače može se odvratiti od napada ili im se barem može uvelike otežati pristup.

Radom je pokazano da na lokalnoj mrežnoj infrastrukturi prosječnih brzina (10 Mbps i 100 Mbps) ne postoji značajna razlika u brzini prijenosa datoteka korištenjem FTP, FTP HTTP, FTP HTTPS i FTPS protokola.

U lokalnoj mreži na brzini od 1 Gbps zbog rjeđih potreba za prijenosom velikih datoteka, kada korištenje sigurnih protokola neće značajnije utjecati na performanse sustava, treba koristiti siguran protokol FTP HTTPS. Ako se mrežna komunikacija ostvaruje između poslužitelja i sigurnost je riješena drugim sustavnim mehanizmima, treba koristiti FTP protokol.

Prijenos datoteka u WAN mreži treba biti siguran. Mjerenja su pokazala da je FTP HTTPS protokolom ostvarena najveća brzina prijenosa u nezaštićenoj WAN mreži, a zaštićena WAN mreža ima sličan omjer brzina kao i nepromjenjiva LAN mreža, pa prema tome FTP HTTPS protokol predstavlja najbolje rješenje.

LITERATURA

- Allman, M., Ostermann, S. (1999) *FTP Security Considerations*, IETF RFC 2577, <http://tools.ietf.org/html/rfc2577> (pristupano 22. 12. 2013.)
- Barrett, D. (2005) *SSH, The Secure Shell: The Definitive Guide*, drugo izdanje, SAD: O'Rilley Media
- Dulaney, E., Harwood, M. (2012) *CompTIA Network+ N10-005 Authorized Exam Cram*, četvrto izdanje, SAD: Pearson
- Ford-Hutchinson, P. (2005) *Securing FTP with TLS*, IETF RFC 4217, <http://tools.ietf.org/html/rfc4217> (pristupano 22. 12. 2013.)
- Forouzan, B. (2010) *TCP/IP Protocol Suite*, četvrto izdanje, SAD: McGraw-Hill
- Galbraith, J., Saarenmaa, O. (2006) *SSH File Transfer Protocol*, IETF SECSH Draft, <http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13> (pristupano 22. 12. 2013.)
- McKinley, H., *SSL and TLS: A Beginners Guide*, SANS Institute, 2003. <http://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029> (pristupano 22. 12. 2013.)
- Ylonen, T., Lonvick, C. (2006) *The Secure Shell (SSH) Protocol Architecture*, IETF RFC 4251, <http://tools.ietf.org/html/rfc4251> (pristupano 22. 12. 2013.)

Silvano Čulinović¹
Marin Kaluža²
Dijana Liverić³

Review article
UDC 004.772.057.4

COMPARISON OF FILE TRANSFER PROTOCOLS⁴

ABSTRACT

To access the system data (file) resources, specially built software is used at the user level. This software can be run locally on the user computer and remotely on the remote application server. In both cases, communication with the database server (file server) takes place using network resources. Network resources are the slowest component in the system. Software that communicates with the file server can use different network protocols.

This paper analyzes different file transfer protocols at the application layer of the OSI model. Security mechanisms used in the analyzed protocols are explained. Timing and speed of transferring files in the LAN at the speeds of 10Mbps, 100Mbps and 1Gbps, and the unprotected and protected (VPN), WAN network were measured and noted.

It is shown that the protocols that use security mechanisms are slower than those that do not use security mechanisms. It is also shown that the use of FTP HTTPS secure protocol is an optimal solution - high level of security and non-significantly lower speed.

Key words: file transfer protocol, safety, network, transfer speed

¹ Bacc. inf., Police technician for EOP equipment maintenance, Ministry of the Interior of the Republic of Croatia, Police Directorate Primorsko-Goranska, Ulica žrtava fašizma 3, Rijeka, Croatia. E-mail: silvano.culinovic@gmail.com

² MSc, Senior Lecturer, Polytechnic of Rijeka, Vukovarska 58, Rijeka, Croatia. E-mail: mkaluza@veleri.hr

³ Assistant, Polytechnic of Rijeka, Vukovarska 58, Rijeka, Croatia. E-mail: dliveric@veleri.hr

⁴ Received: 16. 2. 2014.; accepted: 5. 5. 2014.