FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAGREB

SUSTAVI ZA PRAĆENJE I VOĐENJE PROCESA

PROTOKOLI ZA PRIJENOS DATOTEKA:

FTP

TFTP

RCP

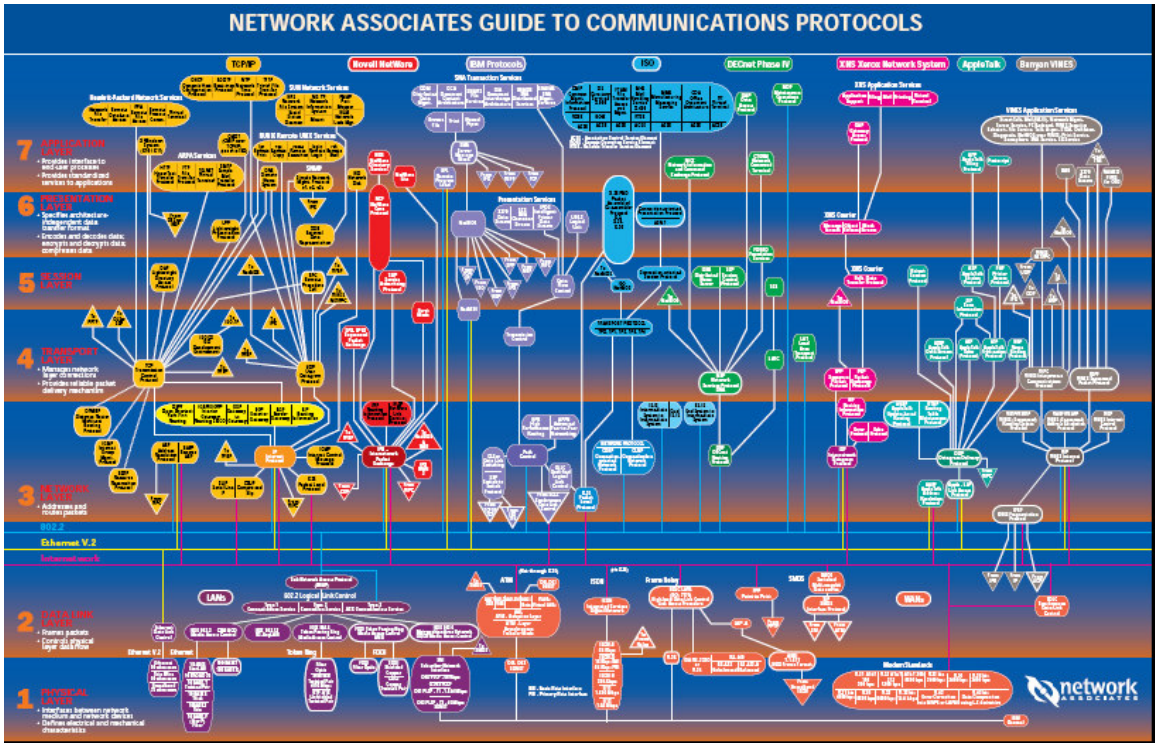
SCP

KRISTINA LEVAK

0036394408

SADRŽAJ:

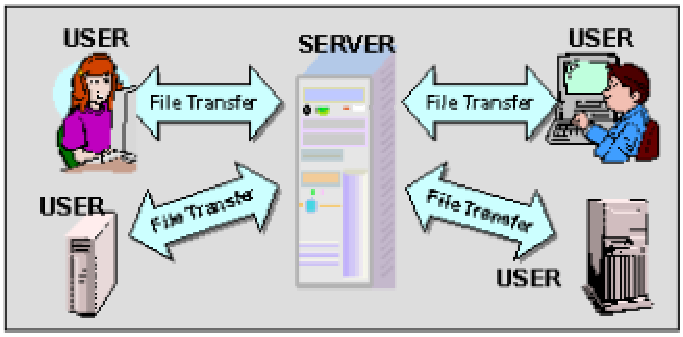
PROTOKOLNI SLOJ



FTP – File Transfer Protocol – aplikacijski sloj
TFTP – Trivial File Transfer Protocol – aplikacijski sloj
RCP – Remote Copy Protocol
SCP – Secure Copy Protocol

FTP – PROTOKOL ZA PRIJENOS DATOTEKA

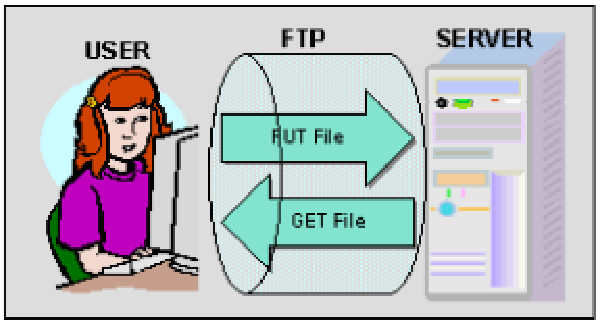
- DEFINICIJA



Slika1. Strukturna skica FTP servisa

FTP je osnovni servis za razmjenu datoteka između domaćina preko TCP/IP mreže (npr. privatne mreže ili Internet). FTP podržava prijenos datoteka i konverziju kodova oznaka kad se razmjenjuje tekst ili binarne datoteke. Korištenje FTP-a je djelotvorno u razmjeni ili distribuciji brojnih podataka preko privatne mreže i/ili Interneta.

FTP je definiran kao komunikacijski protokol između poslužitelja i korisnika za razmjenu datoteka. FTP poslužitelj sprema datoteke koje treba razmjeniti. Korisnik, koji želi razmjeniti datoteke, će se logirati na poslužitelja i ostaviti/uzeti datoteke u/od poslužitelja (Slika 2).

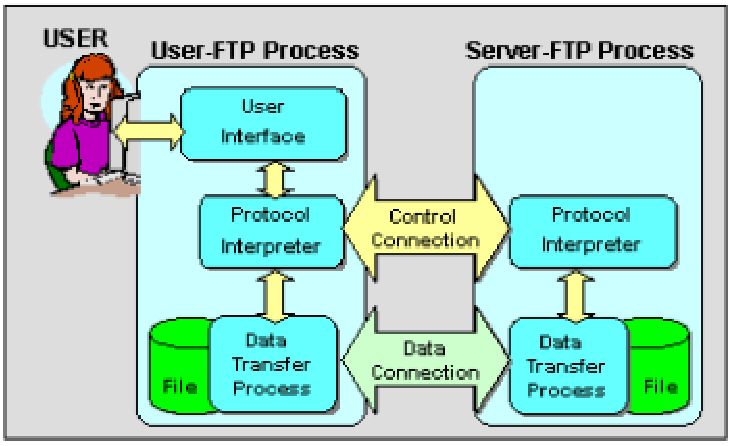


Slika 2. FTP

Korisnik može biti osoba ili proces u ime osobe koji želi dobiti servis za prijenos datoteka. Za razmjenu datoteka preko FTP je neophodno postaviti FTP poslužitelja.

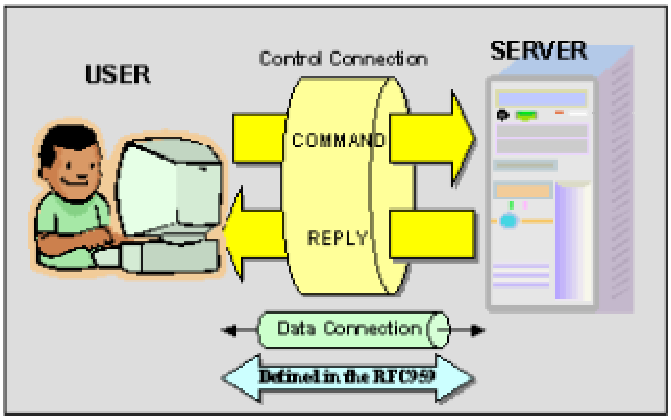
- KAKO FTP RADI

FTP koristi dvije TCP/IP veze između korisnika i poslužitelja npr. kontrolna veza i podatkovna veza. Kontrolna veza upravlja i kontrolira poslužitelja koji prenosi datoteke između poslužitelja i korisnika preko podatkovnih veza.



Slika 3. FTP model

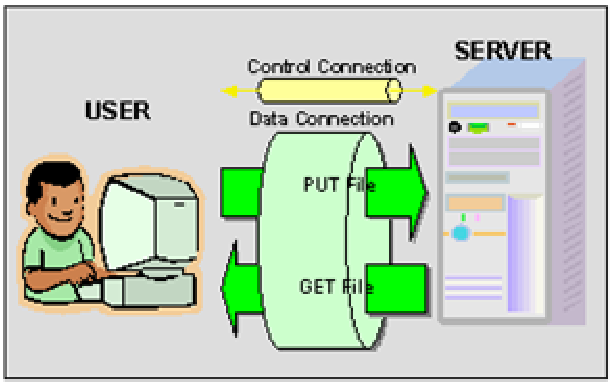
Kontrolna veza je dvosmjeran komunikacijski put između poslužitelja i korisnika u razmjeni naredbi i odgovora.



Slika 4. Kontrolna veza

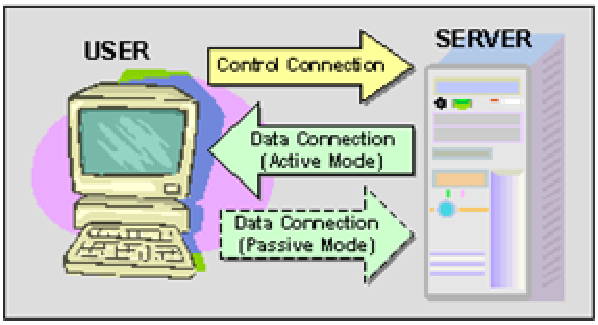
FTP koristi Telnet protokol za kontrolnu vezu. FTP poslužitelj pasivno čeka za uspostavu kontrolne veze, iniciranu od strane korisnika, prema TCP portu 21 od poslužitelja. Kad je jednom uspostavljena kontrolna veza, poslužitelj odgovara sa porukom "Spreman sam" i čeka logiranje korisnika prihvačajući *korisničko ime* i *zaporku,* te čekajući suglasnost od strane poslužitelja (autorizacija). Nakon što je prepoznato legalno logiranje korisnika, poslužitelj odgovara s porukom logina i čeka naredbe za daljnje operacije.

Podatkovna veza je dvosmjerna veza preko koje se podaci prenose između poslužitelja i korisnika sa specificiranim tipom i načinom. Podatkovna veza je uspostavljena privremeno (na zapovjed) za prijenos podataka i datoteka.



Slika 5. Podatkovna veza

Preko podatkovne veze prenosi se, osim sadržaja datoteka, i ostali podaci ili poruke kao rezultat izvršenja FTP naredbi. (Npr.: *help* poruke). Podatkovna veza je upućena od strane polužitelja prema korisniku bez obzira na smjer prijenosa i korisnik pasivno čeka da uspostavu veze (*aktivni* ili *normalni* način).



Slika 6. Smjer FTP veza

Međutim, u nekim slučajevima, uglavnom na strani korisnika, pokretanje veze sa vanjske mreže je nedopušteno zbog sigurnosnih razloga i blokirano je filtriranjem software-a ili vatrozida. U tom slučaju, FTP prijenos neće uspjeti. U takvoj okolini govorimo o *pasivnom* načinu, načinu koji pokreće podatkovnu vezu sa strane korisnika slično kao kontrolnu vezu i ne blokira zbog osiguranja.

FTP dopušta vrlo malo tipova reprezentacija i konverzija podataka. Dva glavna tipa podataka koji FTP dopušta jesu ***ASCII*** i ***IMAGE.*** ASCII tip je osnovni tip. Pošiljaoc pretvara podatke iz unutarnjih oznaka u standardnu 8-bitnu ASCII reprezentaciju. Primaoc će pretvoriti podatke iz standardne forme u unutarnju. Većina FTP primjena ne provodi druge tipova oznaka, osobito višebajtne oznake. Preporučeno je da svi FTP software-i primjenjuju IMAGE tip. Ovdje je datoteka tretirana kao slijed 8-bitnih podatkovnih bajtova i moraju biti

pohranjeni kao susjedni bajtovi bez modifikacije. Ukratko, sa IMAGE tipom datoteka je prenešena onakva kakva je.

- FTP NAREDBE

FTP naredba je naredbena riječ iza koje može slijediti niz parametara završena sa ograničivačem <CRLF>. Svaka naredba je riječ od tri ili četiri osnovna dijela. Slijedi par primjera:

USER <SP> <username> <CRLF>
PASS <SP> <password> <CRLF>
QUIT <CRLF>
PORT <SP> <host-port> <CRLF>
PASV <CRLF>
TYPE <SP> <type-code> <CRLF>
RETR <SP> <pathname> <CRLF>
STOR <SP> <pathname> <CRLF>
ABOR <CRLF>
LIST [<SP> <pathname>] <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CRLF>

- FTP ODGOVORI

Svaka poruka odgovora poslana od FTP poslužitelja se temelji na tri digitalna broja koji se prenose kao tri numerička znaka iza kojih slijedi tekst. Postoji pet vrijednosti za prvu znamenku:

1yz pozitivan preliminarni odgovor
2yz pozitivan završni odgovor
3yz pozitivan središnji odgovor
4yz prijelazni negativni završni odgovor
5yz trajni negativni završni odgovor

Druga znamenka prevodi funkcije grupirajući ih kao:

x0z Sintaksa
x1z Informacije
x2z Veze
x3z Legaliziranje i izvješće
x5z Sustav datoteka

Treća znamenka daje finije stupnjevanje značenja u svakoj od kategorija funkcija, koja je specificirana sa drugom znamenkom.

Primjer FTP operacije na Linux platformi koristeći tradicionalnog FTP posjetioca gdje crveni tekst označava ulaze koje je otipkao korisnik zeleni tekst za odgovore ili brze poruke od software posjetioca i plavi tekst za odgovore od poslužitelja.

USER = username
PASS = password

```
$ ftp servername                    ; korisnik:   početak FTP posjetioca i spajanje imena poslužitelja
Connected to servername.            ; posjetioc: uspostavljena veza
220 servername FTP server ready.    ; poslužitelj: veza potvrđena i čekanje logina
Name (servername:defaultusername):username  ; korisnik: šalji "USER username" naredbu
331 Password required for username. ; poslužitelj: čekaj zaporku za korisničko ime
Password:xxxxxx(not displayed)      ; korisnik: šalji "PASS xxxxxx" naredbu
230 User username logged in.        ; poslužitelj: prihvaća login
Remote system type is UNIX.         ; posjetioc: izvještava trenutni status
Using binary mode to transfer files.
ftp> bye                            ; korisnik:  šalje "QUIT" naredbu
221 Goodbye.                        ; poslužitelj:  QUIT potvrđen
$
```

- OPASKE NA FTP

- Izlaganje zaporke

  Korisničko ime i zaporka su slani kao čisti tekst preko kontrolne veze. Lako je, sa nekim alatom, uhvatiti i baciti IP paket da bi se dobilo korisničko ime i zaporka. Korišenje anonimnih "računa" i/ili ograničenje pristupačnosti datoteka će smanjiti taj rizik.

- Ograničenje naziva datoteka

  Svaki korisnik mora slijediti pravila nazivlja datoteka sustava datoteka obuhvaćenog u prijenosu. Ako nazovete datoteku koristeći skup kodova nespojiv sa ASCII-em, osobito višebajtne kodove, može se dogoditi da FTP ne uspije u prijenosu ili će prenešene datoteke imati nedopuštene nazive datoteka.

- Duljina naziva datoteka

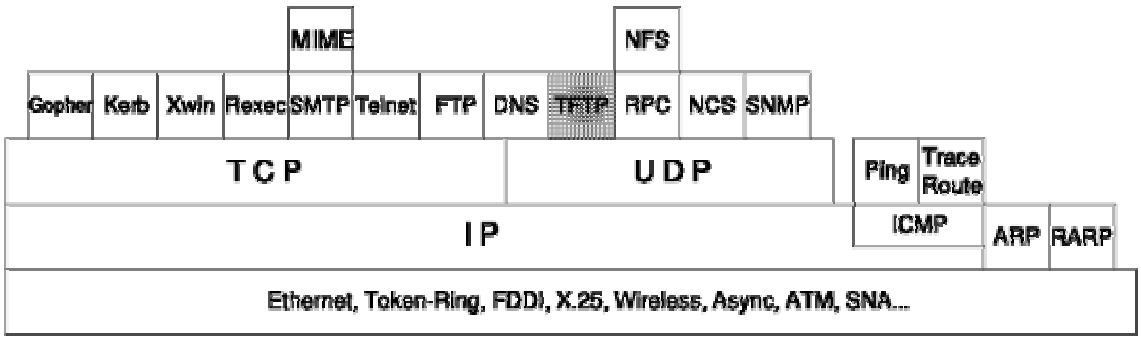
  Ne definira se maksimalna duljina puta imena i imena datoteke. Zapravo, te duljine ovise o platformi i primjeni i variraju od slučaja do slučaja. u najgorem slučaju, ftp posjetilac sa starim Windowsima može obrađivati samo 8-znamenkasta imena i tri ozanke produljenja, npr.: MS-DOS.

- Odsutnost funkcija izmjena

  FTP model ovisi o modelu posjetilac/poslužitelj. Posjetilac aktivno kontrolira poslužitelja da bi se prenijela datoteka između njih, dok se poslužitelj ponaša pasivno. FTP poslužitelj ne izmjenjuje podatke sa trećim domaćinom. Da se postigne ta funkcija, neki procesi izmjena koji

bi periodično provjeravali postojanje datoteka i izveli daljni prijenos datoteka, su potebni izvan FTP-a.

TFTP – TRIVIJALNI PROTOKOL ZA PRIJENOS DATOTEKA

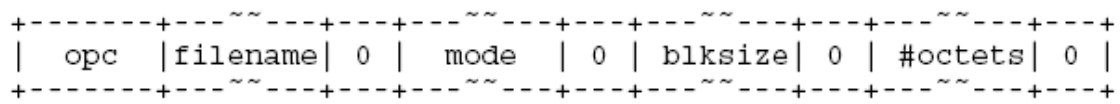


Slika 12. Struktura

Mehanizam TFTP je potpuno drugačiji od FTP-a. TFTP servis koristi samo TCP port 69 umjesto porta 20 i 21 koje koristi FTP. TFTP nema mehanizma za autentikaciju, ograničene su mogućnosti autorizacije, nema izlistavanja sadržaja direktorija, neprikladan je za korištenje kod Internet poslužitelja jer bi bilo tko mogao čitati/pisati podatke sa/u poslužitelj. Primjer primjene TFTP protokola je prijenos datoteka operacijskog sustava prilikom podizanja računala, ili za pohranu parametara konfiguracije na udaljena računala itd. TFTP se koristi jer ga je vrlo jednostavno ugraditi u vrlo mali ograničeni ROM prostor, ali ta prednost je ujedno i glavni nedostatak protokola, jer je prilikom upotrebe tog protokola na Internetu potrebna opreznost kako ne bi došlo do njegove zloupotrebe.

TFTP ima pet tipa poruka:

- zahtjev za čitanjem – RRQ
- zahtjev za pisanjem – WRQ
- podaci – DATA
- potvrda – ACK
- pogreška – ERROR



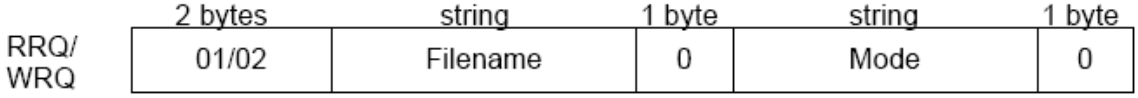
Slika 13. TFTP zahtjev za čitanje ili pisanje

opc: polje «opc» sadrži ili 1 (zahtjev za čitanjem) ili 2 (zahtjev za pisanjem)
filename: ime datoteke koja se čita ili koja će biti upisana, promjenjive duljine
mode: promjenjive duljine

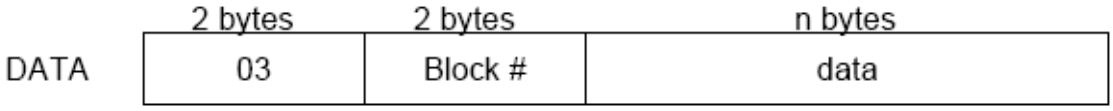
- netascii
  - za prijenos tekstualnih datoteka
  - dopušta standardni format za prijenos tekstualnih datoteka
- octet
  - za prijenos binarnih datoteka

- mail

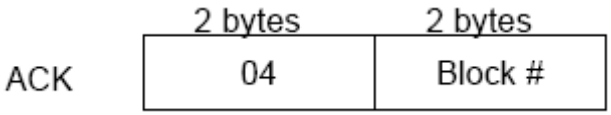
blksize: dvobajtna veličina
#octets: broj okteta u bloku, specificirano u ASCII. Dozvoljene vrijednosti su između 8 i 65464. Veličina bloka se odnosi na broj podatkovnih okteta, ne uključujući četiri okteta TFTP zaglavlja.



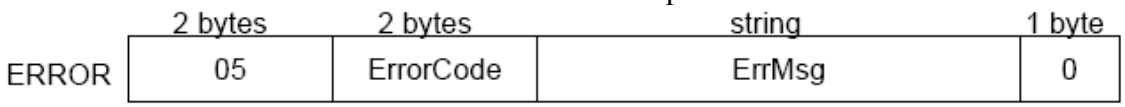
Slika 14. Zahtjev za čitanjem/pisanjem



Slika 15. TFTP podatkovni paket



Slika 16. TFTP potvrda



Slika 17. TFTP paket pogreške

ErrorCode:

0 – nedefinirano
1 – datoteka nije pronađena
2 – povreda pristupa
3 – puni disk
4 – ilegalna TFTP operacija
5 – nepoznati port
6 – datoteka već postoji
7 – nepostojeći korisnik

Ukoliko računalo A želi pročitati datoteku sa računala B, računalo A šalje RRQ računalu B sa izvorom jednakim A's TID i destinacijom 69. Računalo B šalje podatak sa blokovnim brojem 1 prema računalu A sa izvorim jednakim B's TID i destinacijom A's TID.

Ako poslužitelj želi prihvatiti blok podataka, šalje posjetitelju OACK (Option Acknowledgment = potvrda). Specificirana vrijednost mora biti manja ili jednaka specificiranoj vrijednosti od posjetitelja. Posjetitelj mora tada koristiti specificiranu veličinu u OACK-u ili poslati paket pogreške sa kodom pogreške 8, da bi se prijenos završio.

Zadnji paket je kad se primi paket podataka sa duljinom podataka manjom od dogovorene veličine bloka. Ako je veličina bloka veća od količine podataka koja se prenosi, prvi paket je ujedno i zadnji paket. Ako je količina podataka koju treba prenijeti višestruki integral od veličine bloka, šalje se jedan dodatni paket na kraju prijenosa koji ne sadrži nikakve podatke.

Argumenti klijentu trebaju biti GET (za prihvat datoteke sa udaljenog računala na lokalno računalo) ili PUT (za prijenos lokalne datoteke na udaljeno računalo), IP adresa ili ime računala na kojemu se nalazi poslužitelj, pristup na kojemu čeka poslužitelj i na kraju ime datoteke.

Primjer pokretanja TFTP poslužitelja:

tftp_server 32777

Primjer poziva TFTP klijenta kako bi se sa poslužitelja dohvatila datoteka test.c:

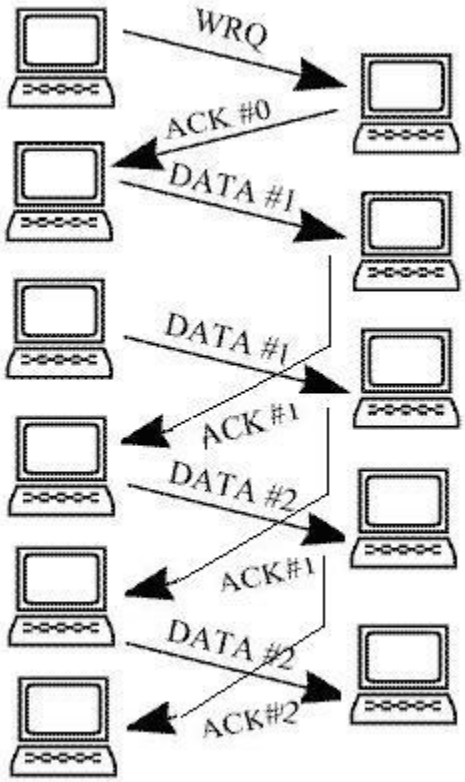
tftp_client get 127.0.0.1 32777 test.c

Kako bi se ta ista datoteka prebacila na poslužitelj koristi se sljedeći oblik:

tftp_client put 127.0.0.1 32777 test.c

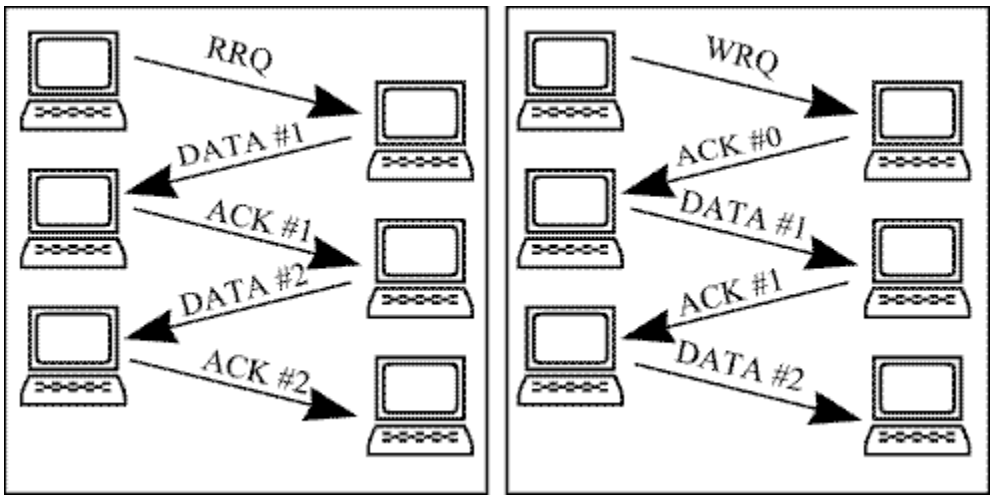
- IZGUBLJENI PAKETI

Pošiljaoc (posjetitelj ili poslužitelj) čeka neko vrijeme, pa ponavlja prijenos. U slučaju primitka dupliciranih paketa, oni se moraju prepoznati, zanemariti i vratiti ACK prijenosom. Ovaj originalni protokol pati od sindroma «čaranje naučnika» (sorcerer's apprentice):



Slika 18. Prikaz TFTP prijenosa

Ako pošiljaoc primi ACK [n], ne smije slati PODATAK [n+1] ako je ACK dupliciran.



Slika 19. Prikat TFTP prijenosa

RCP – REMOTE COPY PROTOKOL

RCP kopira datoteke između lokalnog domaćina i udaljenog domaćina ili između dva udaljena domaćina. Uobičajena sintaksa je u osnovi ista kao i kod regularne *cp* naredbe, ali izvor i/ili destinacija su specificirani ako radimo s udaljenim domaćinom. RCP naredba može biti korištena na način kao i FTP naredba, ali je mnogo jednostavnija. Ovo je udaljen verzija UNIX copy naredbe *cp*. Svaki argument *file* ili *directory* je ili udaljeno ime datoteke oblika "rhost:path" ili lokalno ime datoteke (ne sadržavajući ":", oznake ili "/" prije ":"). RCP ne pita za zaporku. On koristi Kerberos autentikaciju kad se spaja na *rhost*. Svaki korisnik može imati privatnu autorizacijsku listu u datoteci **.k5login** u svom login direktoriju. Svaka linija te datoteke treba sadržavati Kerberos načelno ime u formi *principal/instance@realm.* Ako postoji ~/.k5login datoteka, tada je pristup dopušten ako i samo ako je originalni korisnik prepoznat u datoteci ~/.k5login. Inače, originalnom korisniku će biti dopušten pristup ako i samo ako je načelno ime korisnika unešeno u lokalni račun koristeći *aname -> lname* pravila.

- OBLIKOVANJE RCP-a

rcp [**-p**] [**-x**] [**-k** *realm*] [**-D** *port*] [**-N**] *file1 file2*

rcp [**-p**] [**-x**] [**-k** *realm*] [**-r**] [**-D** *port*] [**-N**] *file ... directory*

-p očuvanje (dupliciranje) modificiranog vremena i načina izvorne datoteke u kopiji
-x šifriranje svih informacija koje se prenose između domaćina
-k *realm* – dobivanje ulaznice za udaljenog domaćina u *realm* umjesto *krb_realmofhost*
-r ako je bilo koja izvorna datoteka direktorij, kopiraj svako podstablo usmjereno na to ime ; u ovom slučaju destinacija mora biti direktorij
-D *port* – poveži se sa portom na udaljeni stroj
-N koristi mrežnu vezu, čak i kad se kopira na lokalnom stroju (u svrhu testiranja)

RCP obrađuje treće odjeljenje kopiranja, gdje niti datoteka izvora niti datoteka odredišta nisu na tekućem stroju. Imena domaćina su oblika *"rname@rhost"* **.**

- OPASKE

RCP ne detektira sve slučajeve gdje bi odredište kopiranja mogla biti datoteka u slučaju gdje bi samo direktorij smio biti legalno odredište. RCP je zbunjen sa bilo kojim izlazom generiran naredbama u datotekama **.login, .profile** ili **.cshrc** kod udaljenog domaćina.

Kerberos je korišten samo za prvu vezu trećeg odjeljenja kopiranja, dok druga veza koristi standardni Berkeley RCP protokol.

SCP – SECURE COPY PROTOCOL

SCP omogućava pouzdanu i legaliziranu metodu za kopiranje konfiguracije usmjeritelja ili datotetaka sa slikama usmjeritelja. SCP je izveden iz RCP-a, ali za razliku od njega, on traži zaporku ili propusne fraze ako su potrebne za autentikaciju. Dakle, SCP kopira datoteke između domaćina na mreži. Pri tome se oslanja na SSH (kostur zaštite), te koristi istu autentikaciju i pruža istu sigurnost kao i SSH. Bilo koji podatak može sadržavati specifikaciju domaćina ili korisnika da bi ukazivalo kako ja ta datoteka kopirana od/prema domaćinu. Dopuštena su kopiranja i između dva udaljena domaćina. SCP je prikladana za automatizirane operacije jer je jednoretčana naredba i nezahtjeva dodatne ulaze. Sa FTP-om datoteka može biti prenešena kao ASCII, BINARY, RECORD ili u Open VMS formatu. SCPv2 ima jedan specificirani format: BINARY. Definirana sintaksa za specifikaciju datoteke je UNIX

- KAKO SCP RADI

Ponašanje SCP je slično ponašanju protokola RCP, osim što se SCP oslanja na SSH radi sigurnosti. Osim toga, SCP zahtjeva autentikaciju, autorizaciju i obračunavanje autorizacije (AAA= Authentication, Authorization, Accounting) kako bi usmjeritelj mogao odrediti da li korisnik ima ispravno pravo pristupa. SCP dopušta korisniku koji ima odgovarajuću autorizaciju da kopira bilo koju datoteku koja postoji u Cisco IOS sustavu datoteka (IFS = IOS File System) prema ili od usmjeritelja koristeći naredbu *copy*. Ovlašteni administrator može također provesti ovu akciju iz radne stanice.

- OBLIKOVANJE SCP-a

scp [**-1246BCpqrv**] [**-c** *cipher*] [**-F** *ssh_config*] [**-i** *identity_file*][**-l** *limit*] [**-o** *ssh_option*][**-P** *port*] [**-S** *program*][[*user@*]*host1*:]*file1* [...] [[*user@*]*host2*:]*file2*

-1 Tjera **scp** da koristi protokol 1.
-2 Tjera **scp** to da koristi protokol 2.
-4 Tjera **scp** da koristi IPv4 adrese.
-6 Tjera **scp** da korsti IPv6 adrese.
-B Selects batch mode (spriječava pitanja za zaporkama).
-C Omogućena kompresija.
-c *cipher* – odabire šifru koju koristi za enkripciju prijenosa podataka
-F *ssh_config*
-i *identity_file*
-l *limit* – ograničava korištenu širinu pojasa u Kbit/s
-o *ssh_option* – korisno za specifikaciju opcija za koje nema odvojene scp naredbene zastavice.
-P *port* – port za povezivanje na udaljenog domaćina

-p Čuvanje modificiranog vremena, pristupnog vremena i načina u odnosu na originalnu datoteku
-q Onemogućava napredovanje brojila
-r Rekurzivno kopiranje cijelih direktorija
-S *program* – ime programa korištenog za enkripcijsku vezu
-v Opširan način. Uzrokuje da **scp** i **ssh** printaju debagirajuće poruke o svom napredovanju. To je od pomoći kod debagirajućih veza, autentikacije i problema oblikovanja.

	Naredba	**Svrha**
Korak 1	OMOGUĆAVANJE Primjer: Router>enable	Omogućava privilegirani EXEC način. • Unesite svoju lozinku.
Korak 2	OBLIKOVANJE TERMINALA Primjer:Router# configure terminal	Unosi globalni konfiguracijski način.
Korak 3	AAA NOVI MODEL Primjer: Router (config)# aaa new-model	Postavlja AAA autentikaciju kod logiranja.
Korak 4	AAA AUTENTIKACIJSKI LOGIN {default | *list-name*} *method1* [*method2...*] Primjer: Router (config)# aaa authentication login default group tacacs+	Omogućava AAA pristupni kontrolni sustav.
Korak 5	AAA AUTORIZACIJA {network | exec | commands *level* | reverse-access | configuration} {default | *list-name*} [*method1* [*method2...*]] Primjer: Router (config)# aaa authorization exec default group tacacs+	Postavlja parametre koji ograničavaju pristup korisnika mreži. Opaska: **exec** - pokreće autorizaciju da bi utvrdio da li je korisniku dozvoljeno da pokrene EXEC. Zbog toga je moramo koristiti kod oblikovanja SCP-a
Korak 6	KORISNIČKO IME [**privilege** *level*] {**password** *encryption-type encrypted-password*} Primjer: Router (config)# username superuser privilege 2 password 0 superpassword	Uvodi korisničko ime – sustav osnovne autentikacije. Opaska**:** Ovaj korak se može preskočiti ako je oblikovan mehanizam *mreža-osnovna autenitikacija.*
Korak 7	OSPOSOBI IP SCP POSLUŽITELJA Primjer: Router (config)# ip scp server enable	Funkcijski osposobljava SCP poslužitelja

Slika 20. Koraci u oblikovanju SCP-a

- PROVJERA SCP-a

	Naredba ili akcija	Svrha
Korak 1	OMOGUĆAVANJE Primjer: Router> enable	Omogućava privilegirani EXEC način. • Unesite svoju lozinku.
Korak 2	PRIKAŽI POKRENUTU KONFIGURACIJU Primjer: Router# show running-config	Provjerava SCP poslužitelja.

Slika 21. Koraci u provjeri SCP-a

- OTKRIVANJE KVAROVA

	Naredba ili akcija	Svrha
Korak 1	OMOGUĆAVANJE Primjer: Router> enable	Omogućava privilegirani EXEC način. • Unesite svoju lozinku..
Korak 2	DEBUG IP SCP Primjer: Router# debug ip scp	Riješava probleme SCP autentikacije.

Slika 22. Koraci u debagiranju SCP-a

Primjer debagiranja:

```
Router# debug ip scp

4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv C0644 20 scptest.cfg
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv 20 bytes
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <OK>
4d06h:SCP:[22 -> 10.11.29.252:1018] send <OK>
4d06h:SCP:[22 <- 10.11.29.252:1018] recv <EOF>
```

- OPĆENITE OPCIJE
  - **p** :dozvole, pokušaji da se održe dozvole na orginalnoj datoteci kad se iskopira na novu lokaciju.
  - **r** : rekurzivno kopiranje cijelih direktorija.
  - **q** : tihi način, onemogućava napredovanje brojila.
  - **v** : opširan način, korisno za pokazivanje što se događa kad kopiranje ne radi.
  - **man scp** – kompletna lista opcija i njihova upotreba

Ali kad je potrebno više naprednih upotreba, bolje je koristiti SFTP**.**

- PREDZAHTJEVI NA SCP

    - prije uspostavljanja SCP-a mora se točno oblikovati SSH, autentikacija i autorizacija na usmjeritelju
    - budući da SCP počiva na SSH za siguran prijenos usmjeritelj mora imati Rivest, Shamir, and Adelman (RSA) par

Primjer:

Vi ste kod kuće za vašim osobnim računalom, Linux je pokrenut i spojeni ste na Linux poslužitelj koristeći SSH. Imate nekoliko datoteka koje želite kopirati u web mapu na poslužitelju. Imate razvrstane sve dozvole da ih ne morate ponavljati kad šaljete podatke. Morate napisati:

scp [options] source-files destination-files

$ *scp -pr ~/public_html/* username@server-address:~/public_html*

ili

$ *mkdir ~/test*

$ *scp -pr ~/public_html/* username@localhost:~/test*

Ako trebate, možete kopirati datoteke i sa udaljenog servera koristeći slijedeći format:

$ *scp -pr username@server-address:~/public_html/* ~/public_html*

ili

$ *scp -pr username@localhost:~/public_html/* ~/test*