Napredno korištenje operacijskog sustava Linux

3. Protokoli

Dominik Barbarić, Josip Domšić
Nositelj: doc.dr.sc. Stjepan Groš

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva

01.04.2016

OSI RM

Open Systems Interconnection Reference Model

- Fizički sloj - Ethernet, USB, ISDN, 802.11, Bluetooth
- Podatkovni sloj - Ethernet, PPP, CSMA/CA
- Mrežni sloj - ICMP, IPsec, IPv4, IPv6, AppleTalk
- Transportni sloj - UDP, TCP
- Sjednički sloj - HTTP, SMTP, SIP, Telnet
- Prezentacijski sloj - MIME
- Aplikacijski sloj - NFS

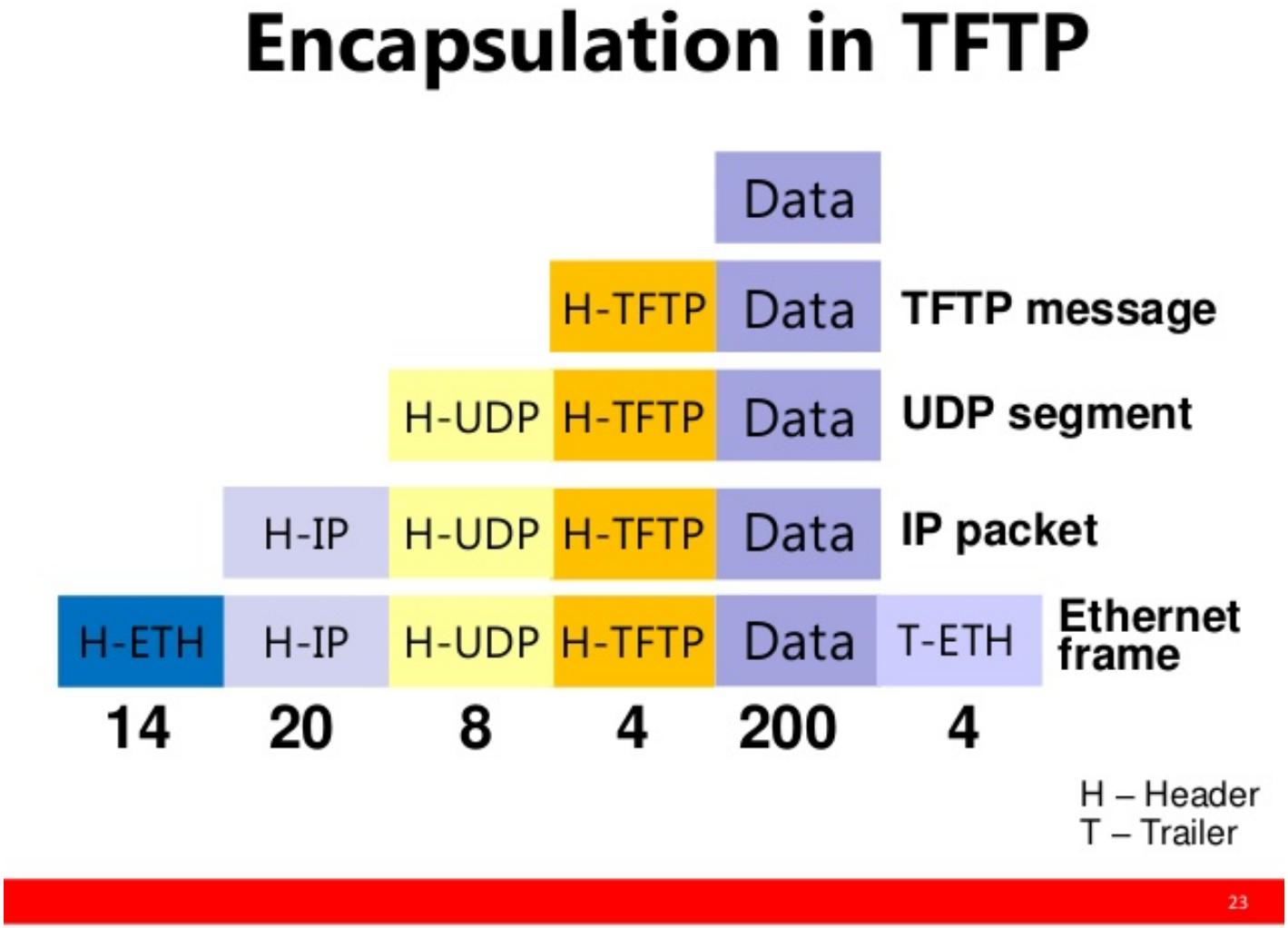
TCP/IP

Transmission Contral Protocol over Internet Protocol

Najrasprostranjenija implementacija

- Podatkovni sloj (Fizički i Podatkovni)
- Mrežni sloj
- Transportni sloj
- Aplikacijski sloj (Sjednički, Prezentacijski, Aplikacijski)

TCP/IP


Encapsulation in TFTP
Data
H-TFTP
Data
TFTP message
H-UDP
H-TFTP
Data
UDP segment
H-IP
H-UDP
H-TFTP
Data
IP packet
H-ETH
H-IP
H-UDP
H-TFTP
Data
T-ETH
Ethernet frame
14
20
8
4
200
4
H – Header
T – Trailer
23

Komunikacija

- IP protokol sadrži podatke o adresi, veličini paketa, . . .
- TCP održava vezu između 2 subjekta / računala / hosta
- Jedinstveno definirano s: parom IP adresa i port
- Alternativa je socket file
- Definira se i tip komunikacije: Stream, Datagram, RAW, ...

Klijent-Server arhitektura

- Server pruža usluge klijentima preko definiranih mrežnih protokola
- Alternativa je peer-to-peer
  - Serveru se pristupa preko *socketa*
    IP adresa i port
    Prijenosni protokol (TCP, UDP, ...)
- Serverski programi se pokreću kao *daemon*

Protokoli

- INETD / XINIETD
- SSH
- HTTP
- FTP
- NFS, SMB
- DNS

ssh

TCP port 22
OpenSSH, Dropbear, ...

- Pristup udaljenoj sesiji
- Enkriptirani protokol
- SFTP i SCP protokoli
- SSH tunnel

  X11 forwarding

ssh

/etc/ssh/sshd_config

```
Port 22
AddressFamily any
ListenAddress 0.0.0.0                    # IP adrese na kojima server slusa
ListenAddress ::                         #      IPv6

Protocol 2                               # SSH-2 protokol

HostKey for protocol version 1
HostKey /etc/ssh/ssh_host_key            # Sigurnosni kljucevi servera
HostKeys for protocol version 2          # Koriste se za enkripciju veze
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

SyslogFacility AUTH                      # Postavke logova
LogLevel INFO                            # Razina logiranja

PidFile /run/sshd.pid                    # Datoteka s PID-om servera
```

ssh

/etc/ssh/sshd_config

```
LoginGraceTime 600                          # Vrijeme cekanja prije ponovnog logina
PermitRootLogin no                         # Ogranicenja autentifikacije
StrictModes yes
axAuthTries 6
axSessions 10

# Odabir nacina autentifikacije korisnika
RSAAuthentication yes                      # RSA kljucevi
PubkeyAuthentication yes

# Datoteka s popisom kljuceva s dozvoljenim pristupom (za svakog korisnika)
AuthorizedKeysFile      .ssh/authorized_keys

RhostsRSAAuthentication no                 # Autentifikacija klijentskih racunala
HostbasedAuthentication no
```

ssh

/etc/ssh/sshd_config

```
# Onemogucavanje tekstualnih sifri
# Cesto "no" ako se koriste druge metode autentifikacije
PasswordAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no

# Autentifikacija kroz druge auth protokole
KerberosAuthentication no
GSSAPIAuthentication no
UsePAM yes

# Omogucen X11 forward za X klijente na serveru
X11Forwarding yes
```

telnet

TCP port 23
xinetd

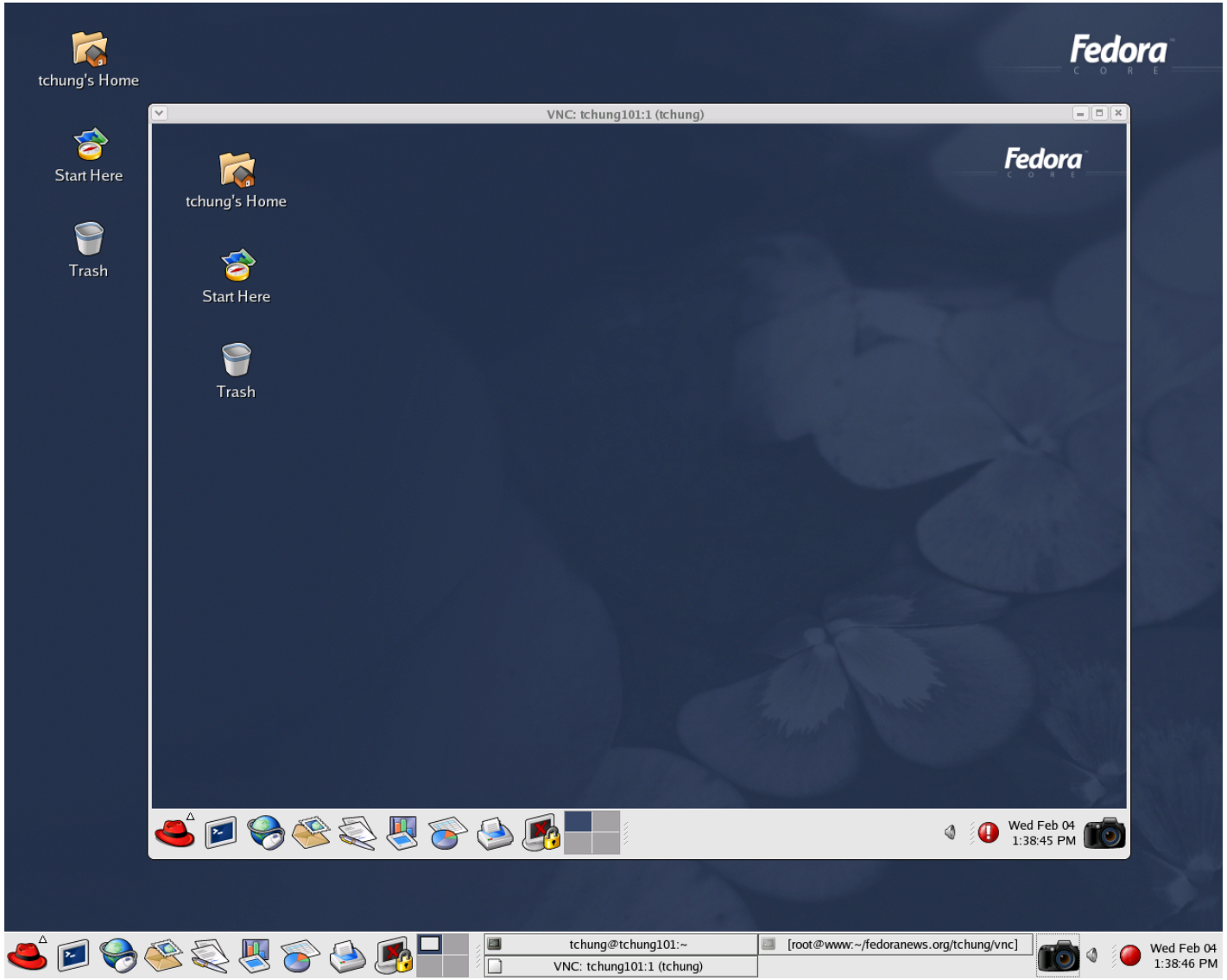
- Udaljeni pristup konzoli
- Nesiguran protokol
- Često korišten na ugradbenoj opremi

vnc

TCP port 5900
tightvnc, tigervnc, realvnc

- Virtual Network Computing
- Udaljeni pristup grafičkom sučelju
- Koristi Remote Framebuffer protokol
  - Rad s bilo kojim windowing sustavom

vnc


tchung's Home
Start Here
Trash
Fedora
VNC: tchung101:1 (tchung)
tchung's Home
Start Here
Trash
Fedora
Wed Feb 04
1:38:45 PM
tchung@tchung101:~
VNC: tchung101:1 (tchung)
[root@www:~/fedoranews.org/tchung/vnc]
Wed Feb 04
1:38:46 PM

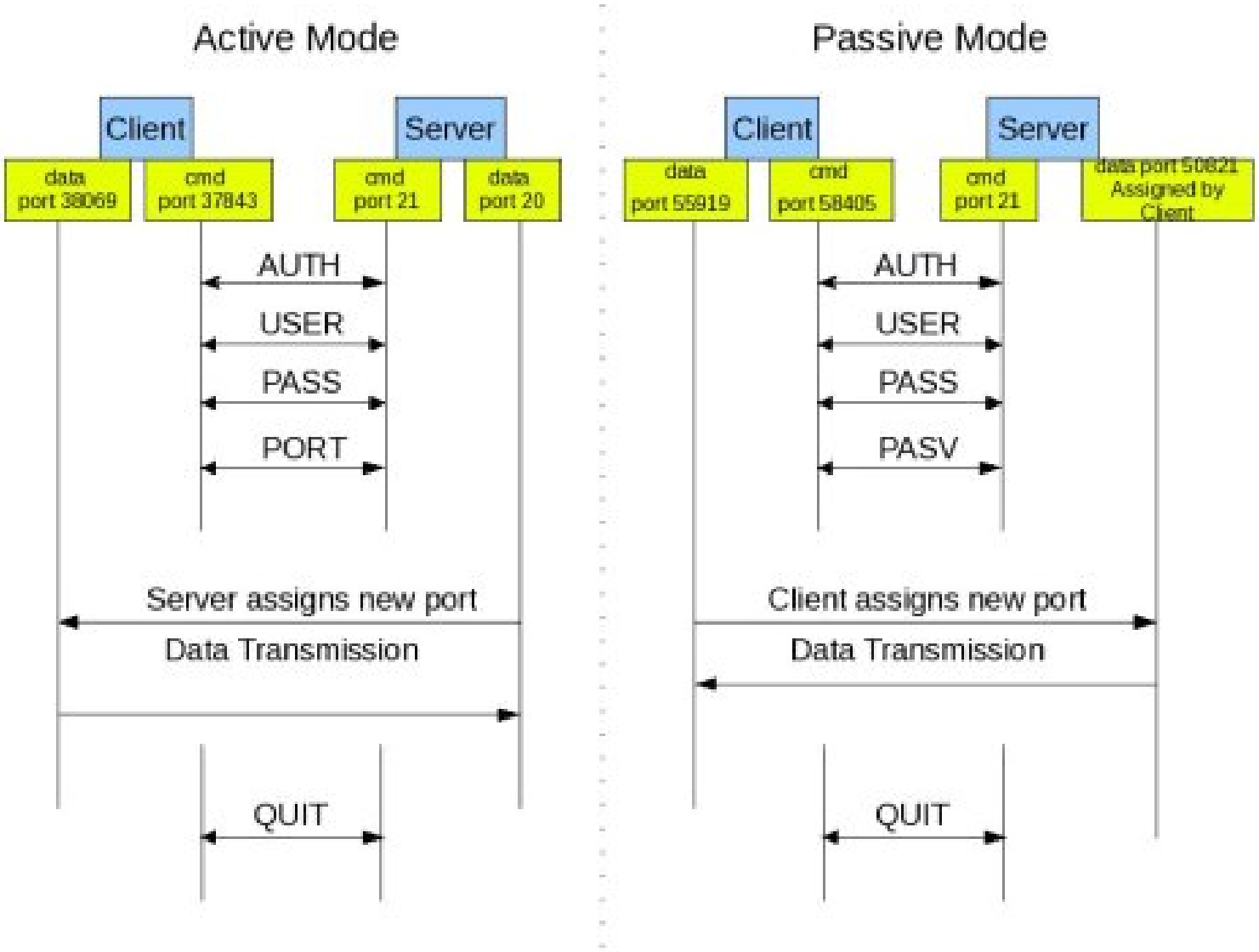
ftp

TCP port 21 (control)
vsftpd, proftpd, bftpd, ...

- File Transfer Protocol
- Varijante: TFTP, SFTP (SSH FTP), FTPS (SSL/TLS FTP)
- Dva načina rada:
  - Aktivni
  - Pasivni

ftp

Način rada



ftp

/etc/vsftpd.conf

```
anonymous_enable=NO                          # Anonimni pristup
local_enable=YES                             # Pristup lokalnim korisnicima

# Per-user configuration
user_config_dir=/etc/vsftpd_conf.d           # Folder u kojem se nalaze konfiguracije
                                             # za svakog korisnika

# Omogucena FTP write naredba (dozvola pisanja na server)
write_enable=YES
# Don't allow recursive listing { prevents excessive I/O usage.
ls_recurse_enable=NO

# Logiranje uploada i downloada u xfer formatu
xferlog_enable=YES
xferlog_std_format=NO
log_ftp_protocol=YES

# ftp data kroz port 20 (active mode)
connect_from_port_20=YES
```

ftp

/etc/vsftpd.conf

```
# Uploaded files are owned by the uploader.
chown_uploads=NO

# You may change the default value for timing out an idle session.
idle_session_timeout=600

# You may change the default value for timing out a data connection.
data_connection_timeout=120

# Location of the RSA certificate to use for SSL encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem

# Allow PASV (passive ftp)
pasv_enable=YES
pasv_min_port=12000                     # Dozovljeni portovi u pasivnom modu
pasv_max_port=12500
pasv_address=123.45.678.901             # Javna adresa servera
pasv_addr_resolve=NO
# Allow active ftp
port_enable=YES
```

http

TCP port 80, 443
Apache, Nginx

HyperText Transfer Protocol

Port 80 - neenkriptirana veza

Port 443 - SSL veza

Apache konfiguracija `/etc/httpd/conf`

Nginx konfiguracija `/etc/nginx`

Apache

/etc/httpd/conf/httpd.conf

```
Listen 80                                   # Port servera

ServerRoot "/srv/apache"
DocumentRoot "/srv/apache/www"

ServerName localhost:80
ServerAdmin admin@example.com

ErrorLog logs/error.log                     # Postavke logiranja
LogLevel error

LoadModule cgi_module modules/mod_cgi.so
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule dir_module modules/mod_dir.so
LoadModule mime_module modules/mod_mime.so

DefaultType text/plain                      # Defaultni MIME type
```

Apache

/etc/httpd/conf/httpd.conf

```
<IfModule dir_module>
   DirectoryIndex index.html index.php index.aspx
</IfModule>

IndexIgnore .htaccess                                    # .htaccess datoteka nije index

<FilesMatch "^.ht">                                      # Zabrani pristup .htaccess datotekama
   Order allow,deny
   Deny from all
</FilesMatch>

<Directory />
   Options FollowSymLinks
   AllowOverride all
   Order deny,allow
   Allow from all
   Satisfy all
</Directory>

<Directory "/srv/apache/www/phpMyAdmin">                 # Razlicite postavke za direktorij
   Options None
   AllowOverride None
   order deny,allow
   deny from all
   allow from 127.0.0.1
</Directory>
```

DHCP, DNS

DHCP serveri

- dhcpd, dnsmasq

DNS serveri

- BIND, pdnsd, dnsmasq

Primjer konfiguracije `/etc/dhcpd.conf`

```
# Postavke za sve rangeove koje router dodjeljuje
option domain-name-servers 8.8.8.8, 8.8.4.4;            # Adresa DNS-a koja se predaje klijentima
option subnet-mask 255.255.255.0;
option routers 139.96.30.100;                           # Gateway

# Postavke IP rangea
subnet 139.96.30.0 netmask 255.255.255.0 {
    range 139.96.30.150 139.96.30.250;

    host racunalo1 {                                    # Fiksna IP adresa za određenu MAC adresu
        hardware ethernet 70:56:81:22:33:44;
        fixed-address 139.96.30.199;
    }
}
```

Literatura

https://wiki.archlinux.org/index.php/Server

https://wiki.archlinux.org/index.php/vsftpd
https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-ftp-vsftpd-conf.html

http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-RH-Edition-v1.3/chap15sec122.html

https://wiki.archlinux.org/index.php/tightvnc

https://wiki.archlinux.org/index.php/Dhcpd
http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch08_:_Configuring_the_DHCP_Server