

Fakulteta za elektrotehniko,  
računalništvo in informatiko  
Inštitut za avtomatiko  
Laboratorij za obdelavo signalov in daljinska vodenja

**Navodila za vaje pri predmetu Internetne tehnologije**  
**VAJA 3**

Dušan Gleich

Maribor, februar 2008

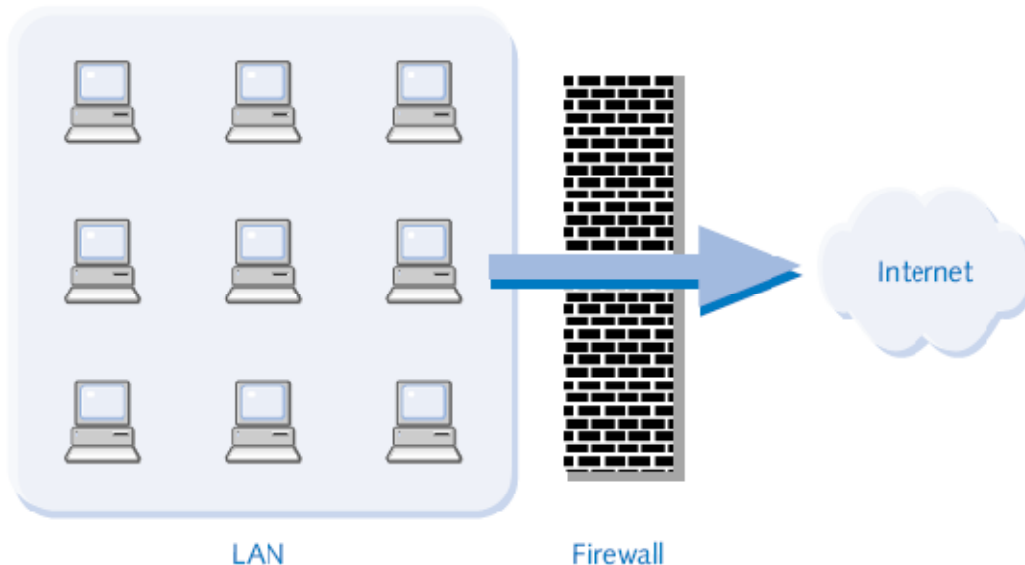
## Vsebina

Požarni zid .....	3
Aktiviranje ICF .....	4
Internet informacijski servisi .....	6
Namestitev IIS .....	6
Nastavitev IIS.....	6
Servisi spletnega strežnika .....	7
ISAPI filter.....	7
Domača mapa (Home Directory).....	7
Documents .....	7
Directory Security .....	7
Http Headers .....	7
Nastavitev privzete spletne strani .....	8
FTP (file transfer protocol) strežnik .....	9
Skupna raba datotek in map.....	11
Varnost map .....	11
Skupna raba tiskalnika .....	12
Net session, net share in net File ,net stat .....	13
Navidezno omrežje (Virtual Private Networking) (VPN) .....	14
Povezava na VPN strežnik.....	14
Povezava .....	15
Ustvarjanje VPN strežnika.....	16

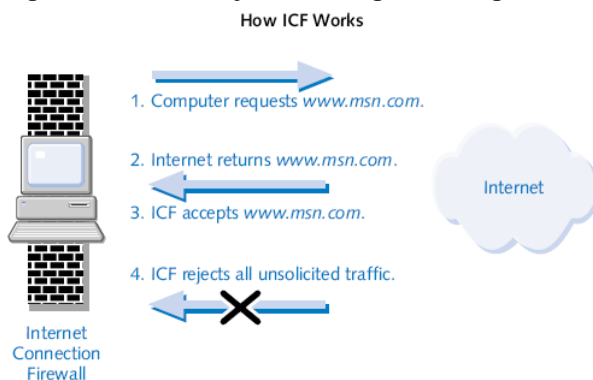
## Požarni zid

Požarni zid (firewall) je naprava ali programska oprema, ki se namesti med omrežjem ali računalnikom z namenom, da se zagotovi varnost.

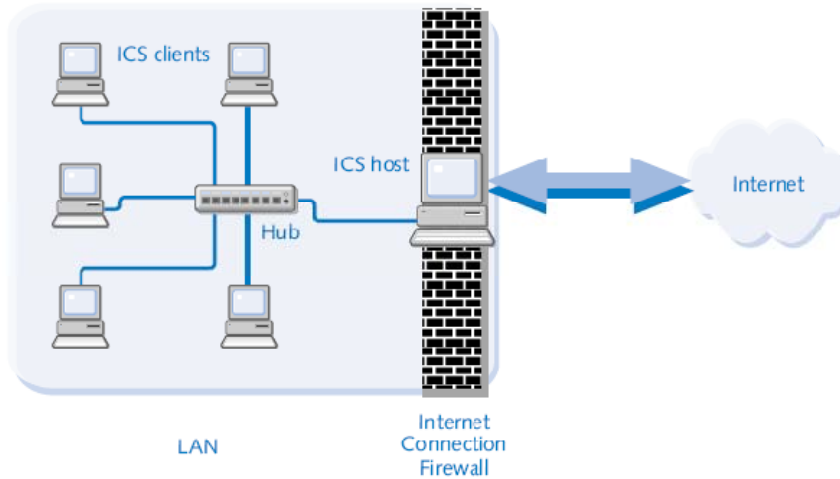
Ponavadi se požarni zid uporabi v točki, kjer se lokalno računalniško omrežje priključi na internetno omrežje, da ščiti računalnike pred splošnim TCP/IP prometom, kot je pokazano na spodnji sliki.



Pogledali bomo kako deluje Internet Connection Firewall (ICF), ki je sestavni del operacijskega sistema Windows XP in je namenjen varovanju enega PC računalnika ob dostupu na Internet. ICF deluje tako, da varuje PC računalnik pred zunanji vdori. Poglejmo si primer, ko zahtevamo podatke iz web strani se podatki prenesejo iz PCV računalnika na web strežnik in iz web strežnika nazaj na PC, pri tem pa ICF pregleda pakete in primerja IP naslov. Če najde pravi IP naslov tabeli destinacijskih naslovov potem spusti promet na PC. Če med tem prispe kakršen koli drug promet na PC; ki ni zapisan v destinacijski tabeli, potem se paketi zavrnejo



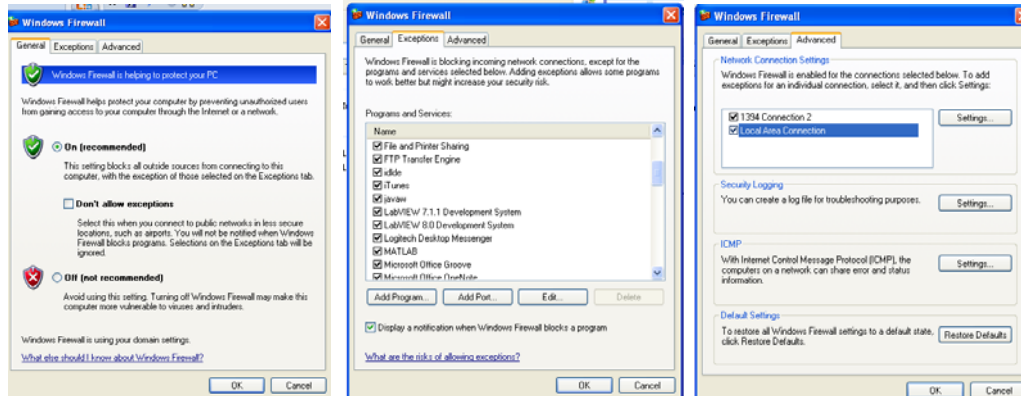
Z ICF lahko tudi varujemo celotno omrežje, če uporabimo računalnik, ki se direktno povezuje na Internet z uporabo Internet Connection Sharing. Ves promet se potem nadzoruje preko enega računalnika, kot je pokazano na spodnji sliki

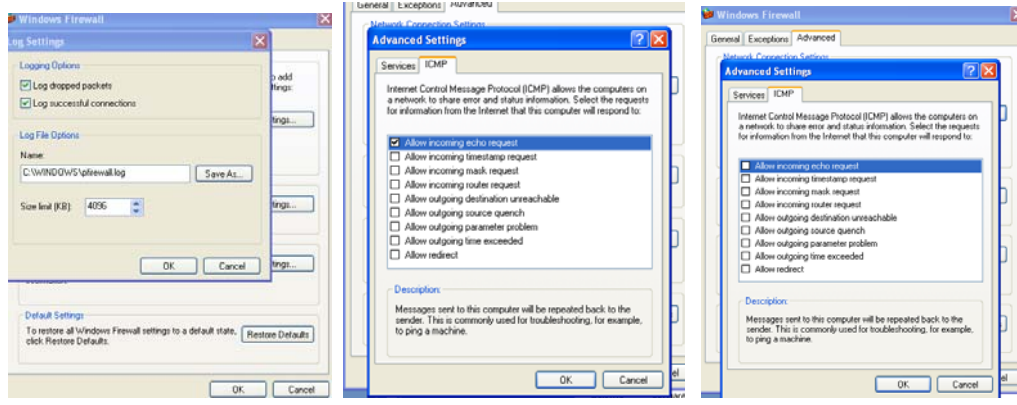


ICF ne šiti računalnika pred črvi in virusi in Trojanskimi konji

## Aktiviranje ICF

Start->Control Panel->Windows Firewall





## Internet informacijski servisi

Internet informacijski servisi (Internet information services) IIS, ki je vgrajen v Windows XP je namenjen za enostavne web aplikacije in ima omejitev na 10 TCP povezav. IIS omogočajo

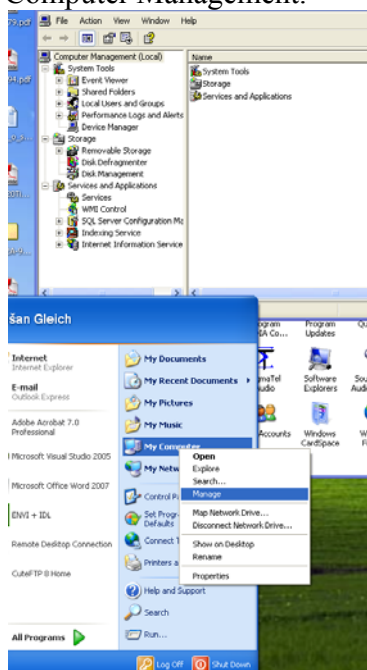
- Gostovanje ene spletne strani
- Gostovanje enega ftp (file transfer protocol) strežnika
- SMTP virtualni strežnik
- Uporabo IIS za testiranje spletnih aplikacij
- Skupna raba tiskalnikov preko Interneta

## Namestitev IIS

V nadzorni plošči izberemo oddaj/odstrani programe (add/remove programs) in izberemo IIS servise pod Windows Components (potrebujete CD windows SP2)

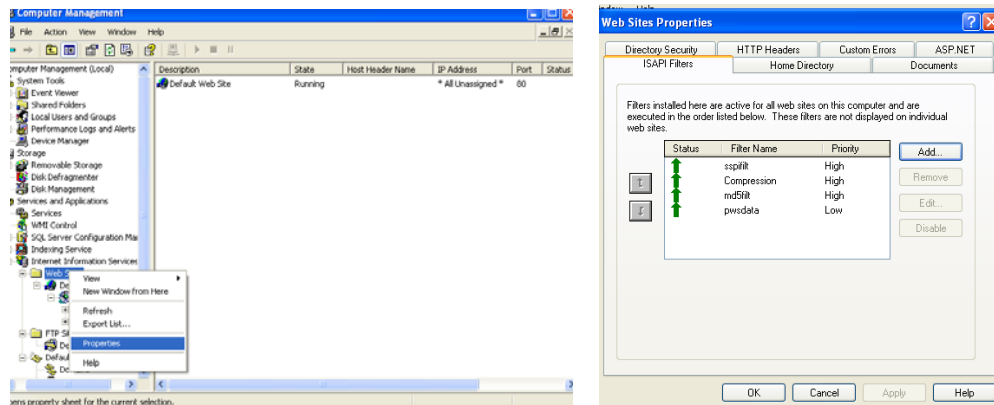
## Nastavitev IIS

Najprej odpremo okno za upravljanje z IIS servisi. Start->All Programs, My Computer, kliknemo na desni miškin gumb in izberemo Manage, odpre se nam pogovorno okno Computer Management.



## Servisi spletnega strežnika

Pod IIS izberite Web Sites, kliknite miškin desni gumb in izberite Properties (Lastnosti) in pokaže se vam pogovorno okno.



### ISAPI filter

ISAPI filter je program, ki ustreza določenim dogodkom za procesiranje http zahteve. Lahko spremeni vhodno zahtevo, vrača podatke in dodaja nove lastnosti IIS. Z gumbom add lahko dodamo nove servise.

### Domača mapa (Home Directory)

Home directory jezikček vsebuje lastnosti o spletni strani, kje se spletna stran nahaja, način dostopa, dovoljenja do mape in konfiguracija spletne strani, kateri servisi so na voljo in kako naj se dostopa do mape, kjer se nahaja spletna stran. Drugi razdelek pa predstavlja nastavitve aplikacije pod Configuration, kjer lahko določimo kašen tip spletne strani se bo izvajal v spletni mapi in nastavitve za asp spletne strani.

### Documents

Tukaj nastavimo ime dokumenta, ki se bo odprl ob dostopanju do naše spletne strani.

### Directory Security

Tukaj nastavimo dostop uporabnikom do spletne strani.

### Http Headers

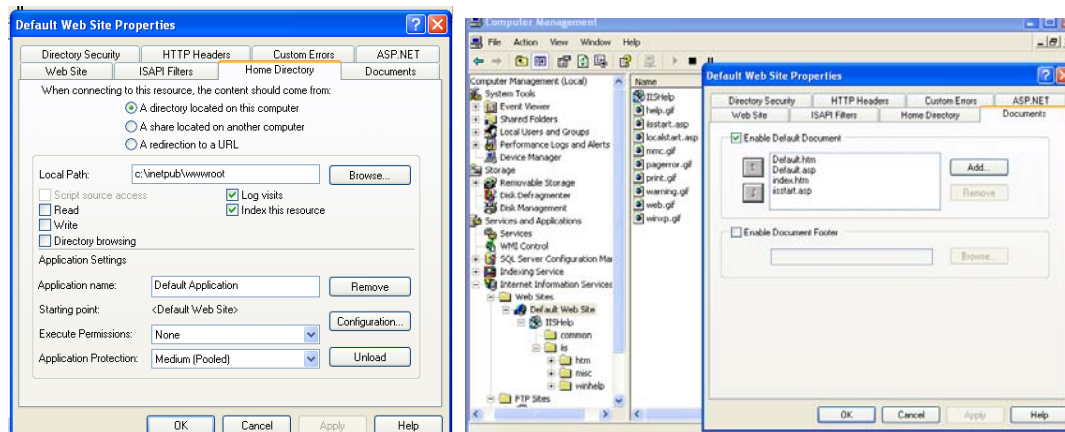
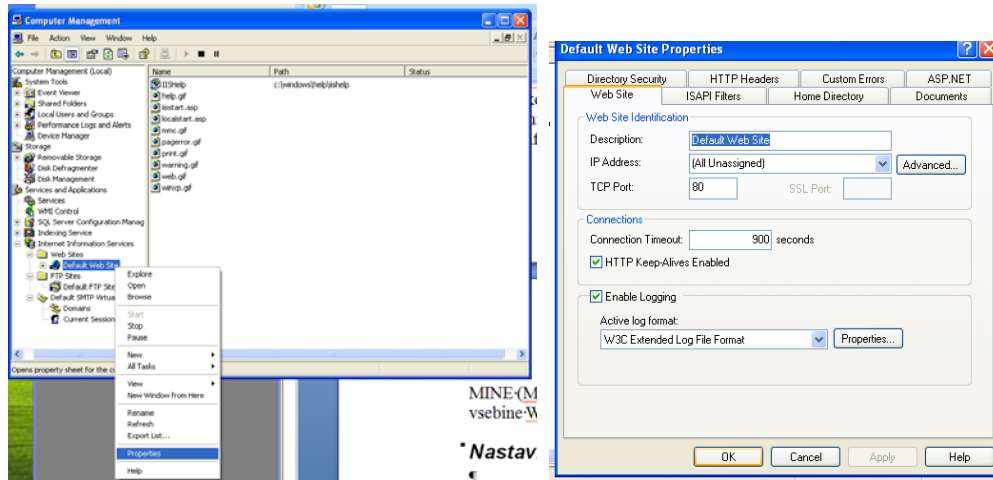
V tem razdelku določamo veljavnost vsebine (Enable Content Expiration), kjer določimo časovno veljavnost informacij.

možnosti zaglavja (Custom Header Option), tukaj nastavljamo možnosti zaglavja http iz ISS spletnega strežnika proti uporabniku (klientu).

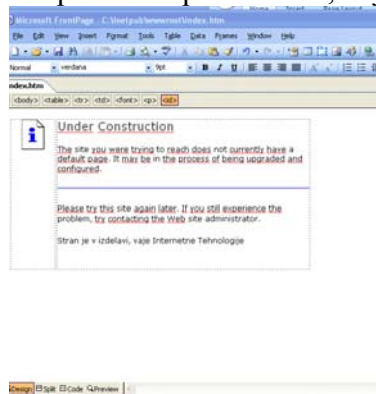
Vsebinsko ocenitev, kjer določamo vsebino http zaglavja, ki definirajo vsebino gostujoče web strani. Uporabnik lahko nastavi vsebinske nastavitve za spletni brskalnik z uporabo MIME informacije, kot na primer kratice datotek.

MINE (Multipurpose Internet MAil Extensions) map. Te nastavitve identificirajo tip vsebine Web stani

## Nastavitev privzete spletne strani



Nastavite ip vašega računalnika in vtipkajte vaš IP naslov v obliki <http://192.198.1.106>. Če ste vse dobro naredili se mora pokazati spletna stran, ki je v obliki index.htm.

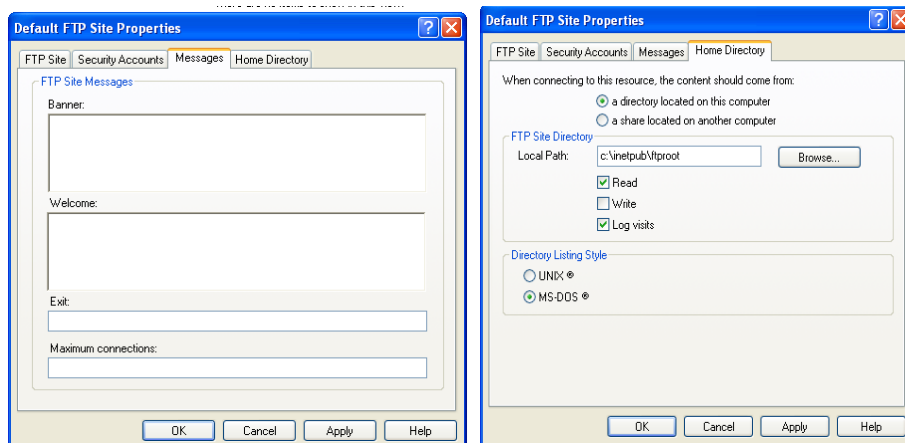
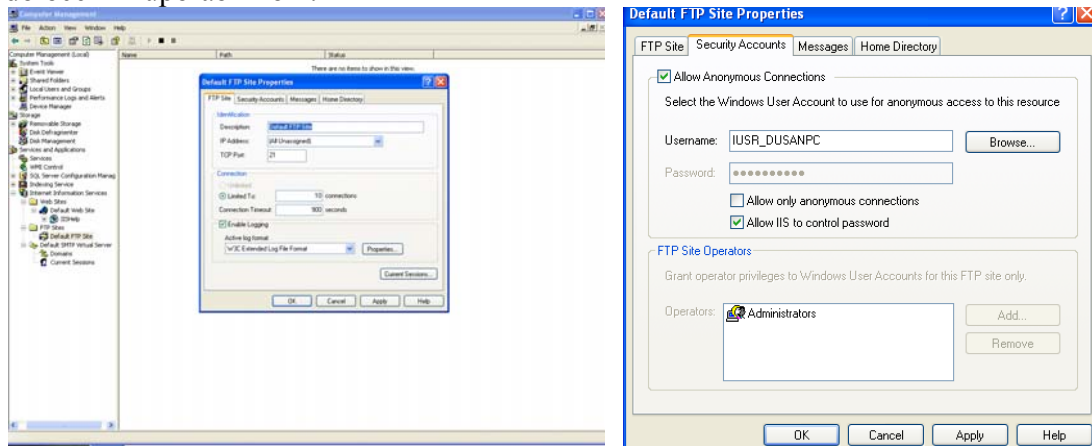




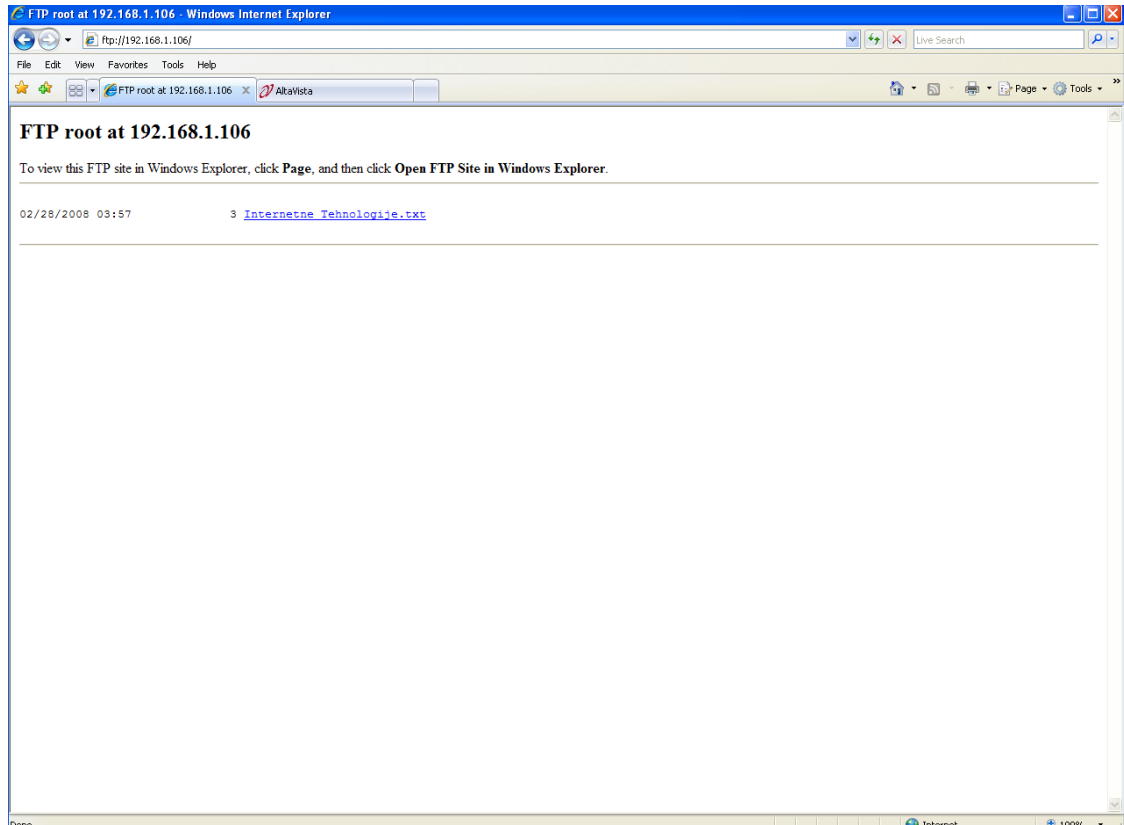
## FTP (file transfer protocol) strežnik

Ftp ostaja zelo atraktiven za prenos datotek v medmrežju. FTP strežnik se nastavi zelo podobno kakor http strežnik, preko Computer Management konzole.

Zanimiva je konfiguracija uporabnikov, kjer lahko omejimo dostop do ftp strežnika samo določenim uporabnikom.

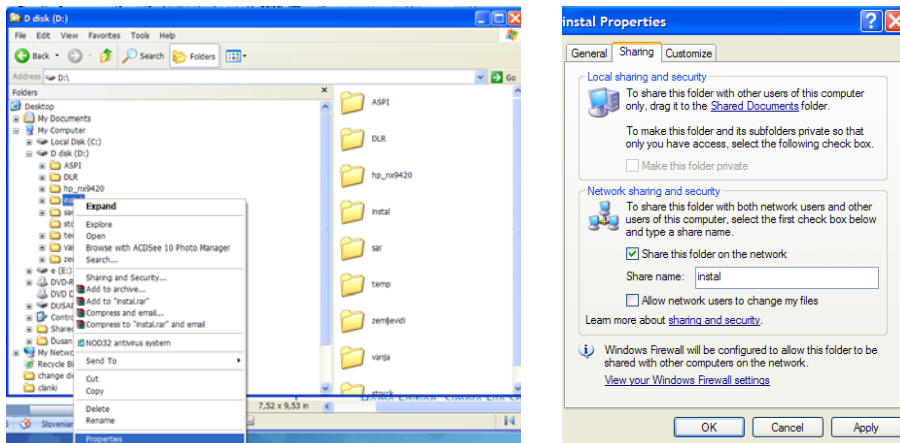


Ob pravilni konfiguraciji strežnika ftp in pravilnem vnosu ip naslova lahko vidimo datoteke, ki jih imamo na ftp strežniku.



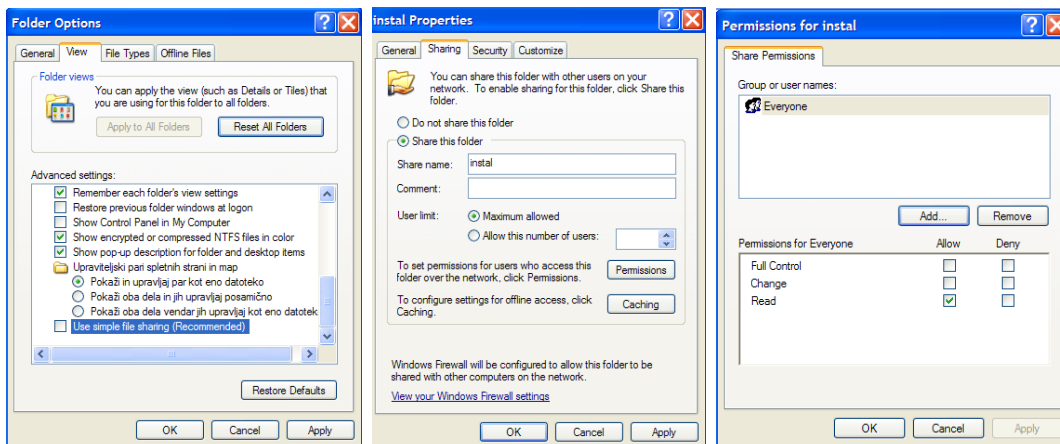
## Skupna raba datotek in map

Namen skupne rabe datotek je, da omogočimo datoteke, ki so na enem računalniku vsem ostalim računalnikom, ki so bodisi v enaki delovni skupini ali v enakem podomrežju. Če želimo postaviti mapo v skupno rabo kliknemo v brskalniku na zeleno mapo, ki se nahaja na našem disku in kliknemo lastnosti (Properties). Nato pritisnemo jeziček Sharing in izberemo »Share this folder on the network« in na ta način omogočimo skupno rabo datotek.



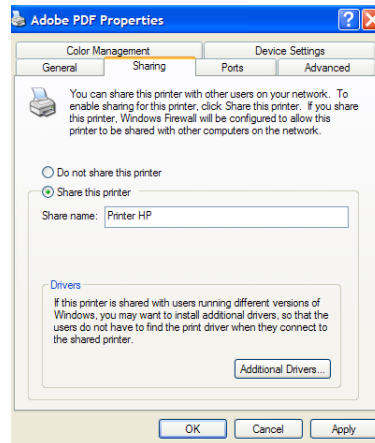
## Varnost map

Če želimo določiti varnost mape in dodeliti dostop le do posameznih uporabnikov, moramo izklopiti enostavno skupno rabo datotek. To naredimo tako, da v nadzorni plošči izberemo (Control Panel) Folder Options in izklopimo Simple File Sharing in če sedaj kliknemo na mapo in z pogledamo njene lastnosti lahko določimo še uporabnika, ki ima dostop do te mape in ali lahko datoteke samo spreminja, bere ali pa ima popoln nadzor nad njimi.

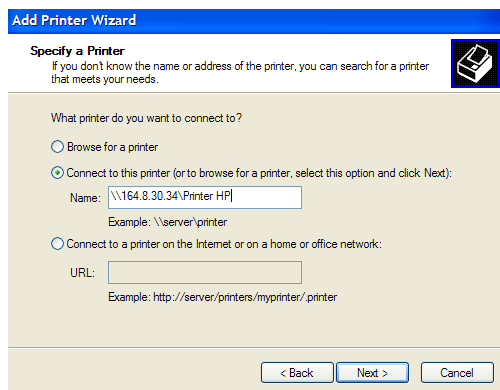
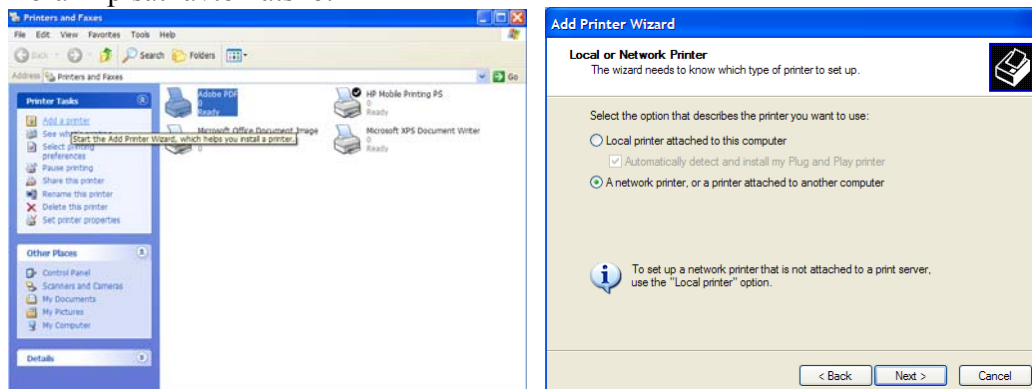


## Skupna raba tiskalnika

Nameščen tiskalnik lahko damo v skupno rabo, podobno kakor smo to storili za mape. Do printerjev pridemo preko Start->Printers and Faxes, izberemo printer in kliknemo na lastnosti (Properties). Pod Sharing damo tiskalnik v skupno rabo in ga poimenujemo.



Na drugih računalnikih lahko dodamo tiskalnik (Add printer), kakor omrežni tiskalnik. V čarovniku izberemo naprej (Next), dodamo mrežni tiskalnik in nato dodamo IP naslov računalnika na katerem je tiskalnik nameščen za skupno rabo in ime računalnika, bi se moral izpisati avtomatsko.



**Net session, net share in net File ,net stat**

Ugotovite pomen Net Session, Net Share in Net file.

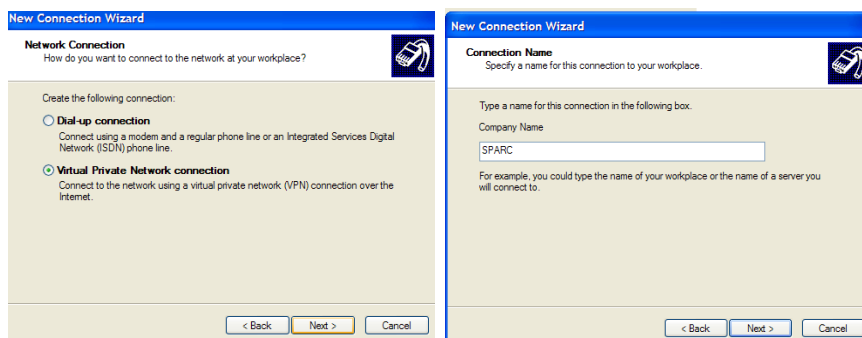
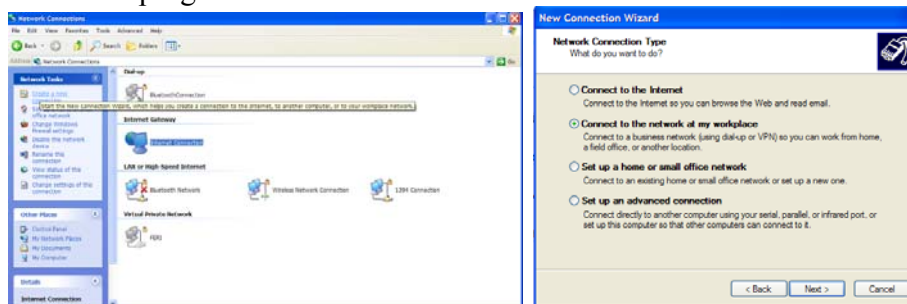
## Navidezno omrežje (Virtual Private Networking) (VPN)

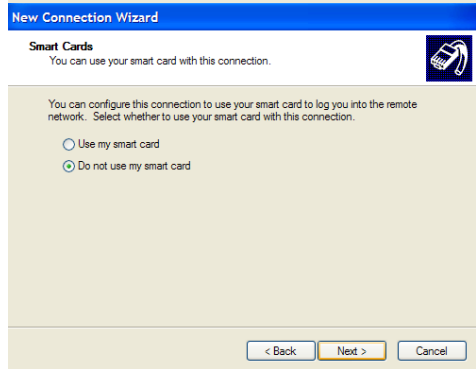
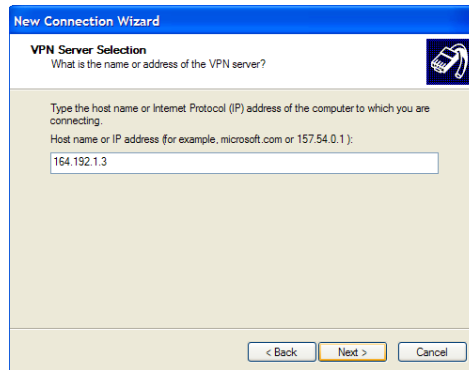
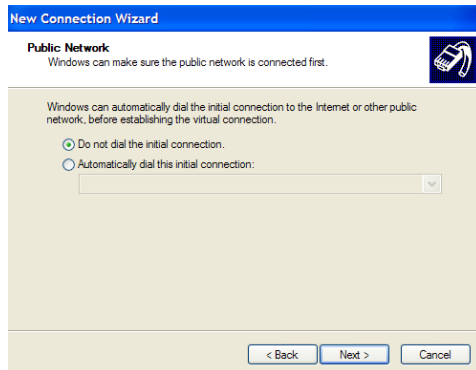
Navidezna privatna omrežja ali (Virtual Private Networking VPN) si lahko predstavljamo kakor razširitev privatnega omrežja, uporabniki pa se »priklopijo na omrežje« in navidezno omrežje omogoča, da uporabniki uporabljajo omrežje kakor da bi bili priključeni na omrežje. Posamezne VPN povezave se obnašajo tako, kakor povezave točka-točka. Računalnik se lahko poveže na virtualno omrežje z katerokoli povezavo (modemom, široko-pasovnim internetom,...) VPN nadzoruje avtentičnost, torej se uporabnik mora prijaviti v omrežje, pri tem lahko preveri IP naslov in uporabniško ime in geslo, VPN lahko upravlja z naslovi tako, da dodeli uporabniku IP naslov omrežja, omogoča enkripcijo podatkov.

VPN uporablja t.i. tunelski transport (ang. tunneling) za izmenjavo podatkov med klientom in omrežjem. Promet iz omrežja 1 se prenaša na klienta v omrežju 1 s pomočjo komponent omrežja 2. Uporabljata se dva protokola point to point tunneling protocol (PPTP) in Layer two tunneling protocol (L2TP) z uporabo Internet protocol security (IPSec).

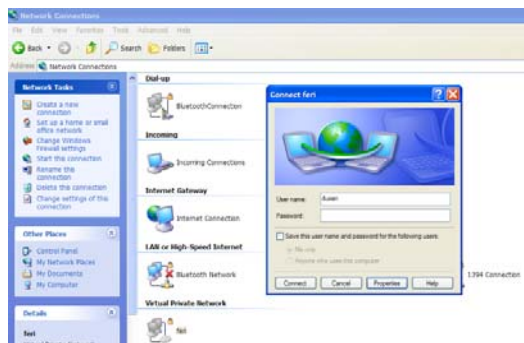
### Povezava na VPN strežnik

Start->All programs->Network Connections->Create New Connection

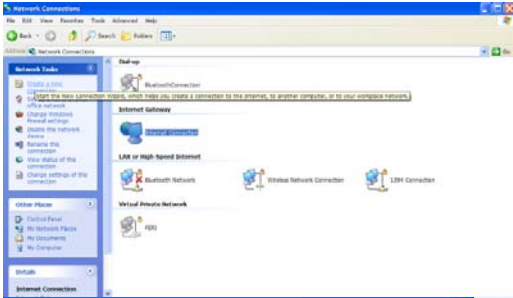




## Povezava



## Ustvarjanje VPN strežnika



The screenshot shows the Windows XP Network Connections window. The left pane shows 'Network Tasks' with options like 'Create a new connection', 'Change connection', and 'Change status of the connection'. The right pane shows 'Internet Gateway', 'LAN or High-Speed Internet', 'Bluetooth Network', 'Virtual Private Network', and 'VPN'. A tooltip is visible over the 'VPN' icon, stating: 'Click the VPN icon to create a connection to the Internet, to another computer, or to your corporate network.'

**New Connection Wizard**

**Network Connection Type**  
What do you want to do?

- Connect to the Internet  
Connect to the Internet so you can browse the Web and read email.
- Connect to the network at my workplace  
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
- Set up a home or small office network  
Connect to an existing home or small office network or set up a new one.
- Set up an advanced connection  
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

< Back Next > Cancel

---

**New Connection Wizard**

**Advanced Connection Options**  
Which type of connection do you want to set up?

Select the connection type you want:

- Accept incoming connections**  
Allow other computers to connect to this computer through the Internet, a phone line, or a direct cable connection.
- Connect directly to another computer**  
Connect to another computer using your serial, parallel, or infrared port.

< Back Next > Cancel

---

**New Connection Wizard**

**Devices for Incoming Connections**  
You can choose the devices your computer uses to accept incoming connections.

Select the check box next to each device you want to use for incoming connections.

Connection devices:

- HD(AUDIO) Soft Data Fax Modem with SmartCP
- Bluetooth Modem
- Direct Parallel (LPT1)

Properties

< Back Next > Cancel

---

**New Connection Wizard**

**Incoming Virtual Private Network (VPN) Connection**  
Another computer can connect to yours through a VPN connection

Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.

If you allow VPN connections, the system will modify the Windows Firewall settings to allow your computer to send and receive VPN packets.

Do you want to allow virtual private connections to this computer?

- Allow virtual private connections
- Do not allow virtual private connections

< Back Next > Cancel

---

**New Connection Wizard**

**User Permissions**  
You can specify the users who can connect to this computer.

Select the check box next to each user who should be allowed a connection to this computer. Note that other factors, such as a disabled user account, may affect a user's ability to connect.

Users allowed to connect:

- Administrator
- ASPNET (ASP.NET Machine Account)
- dusan (Dusan Gleich)
- Guest
- HelpAssistant (Remote Desktop Help Assistant Account)

Add... Remove Properties

< Back Next > Cancel