Pilot projekt izgradnje sigurne školske Microsoft mrežne infrastrukture u Željezničkoj tehničkoj školi u Zagrebu

Jurković Vilim, MCP

Izgradnja nove računalne mreže Škole

- **Cilj projekta:** Uspostaviti sigurnu školsku mrežnu infrastrukturu baziranu na MS Windows Server 2003 koja bi trebala poslužiti kao ogledni primjer za implementaciju i u drugim školama
- **Projekt realiziran u suradnji s** Microsoft Hrvatska (u okviru programa PIL – Partners In Learning)
- Stručna pomoć i podrška – tvrtka TechEd (MS partner)

Microsoft®

Stanje “stare” računalne mreže

- Više od 80 računala
- Više od 1000 korisnika računala
- Više lokalnih mreža (radnih grupa) koje međusobno ne komuniciraju
- Ne postoji sustavno administriranje računala
- Mrežna infrastruktura je izuzetno nestabilna
- Spora veza na Internet
- Učenička i profesorska računala nisu fizički odvojena
- Otežano održavanje i zaštita računala
- Ne postoji dijeljenje resursa

Fizičko odvajanje profesorske i učeničke mreže

- Uvođenje novih switcheva
- Umrežavanje računala koja nisu bila na mreži
- Fizičko odvajanje profesorske i učeničke mreže
- Dvije odvojene računalne mreže

Nabava hardvera

- Nabavljena su 3 serverska računala – za potrebe ISA servera, i 2 za potrebe kontrolera profesorske i učeničke domene
- Konfiguracije serverskih računala – IBM xSeries 206
  - Intel Pentium 4, HT, 3,2 GHz
  - 512 MB RAM
  - 2 x 75 GB SATA diskovi
  - Implementiran je RAID 1 (mirroring) na diskovima

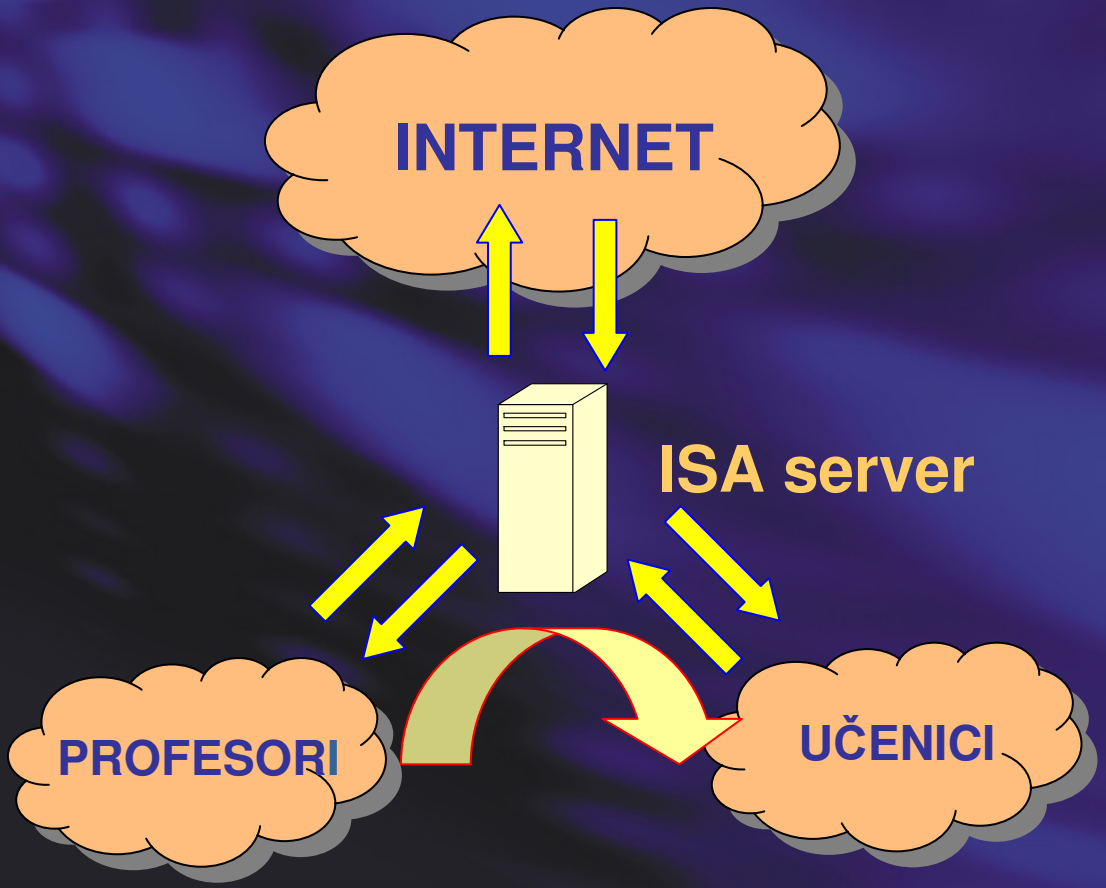
Preduvjeti za realizaciju

- Brza konekcija na Internet - u veljači 2006. 100 Mbps veza na Internet preko CARNeta
- Cijela škola prelazi na CARNET link – svi prijašnji načini povezivanja na Internet postaju redundantni
- Početkom 2005. pohađanje MOC seminara Managing and Maintaining a Microsoft Windows Server 2003 Environment (stručno usavršavanje u okviru Microsoft PIL programa).
- Adekvatna edukacija bitan je preduvjet za realizaciju i održanje rezultata Projekta

Uspostava ISA servera

- MS ISA Server 2004 (Internet Security and Acceleration Server)
- Baziran na MS Windows Server 2003
- Definirane su mreže (profesorska i učenička) i jednosmjerni promet iz profesorske u učeničku mrežu
- Implementiran je firewall (vatrozid)

Funkcionalnost ISA servera



Funkcionalnost ISA servera

- Kontrolira “promet” podataka između mrežnih segmenata i Interneta
- Kreirana su pravila (rule)
- Iz profesorske mreže na Internet – svi protokoli
- Iz učeničke mreže na Internet – samo osnovni protokoli
- Dozvoljen je pristup iz profesorske u učeničku mrežu
- Definirane su iznimke (prema IP adresama)

Značaj ISA servera

- Kontrola prometa između mrežnih segmenata
- Sigurnost od upada u školsku mrežu izvana
- VPN pristup školskoj mreži
- Brži pristup Internetu

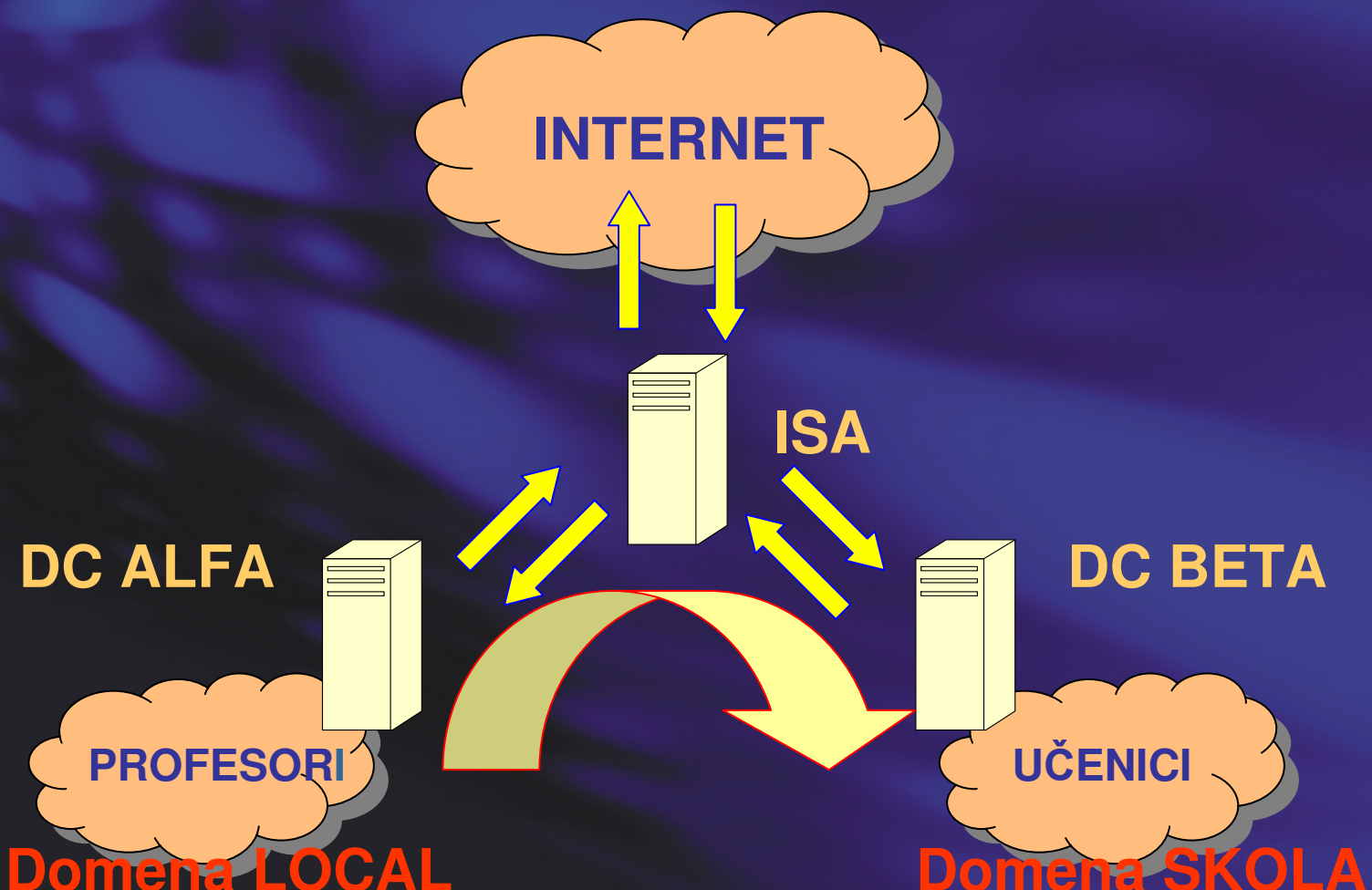
Nezamislivo je održavanje sigurnosti računalne mreže pri tako brzim pristupima Internetu bez implementacije kvalitetnog firewalla (ISA server).

Velike probleme imat će škole priključene na ADSL, a bez implementiranog kvalitetnog firewall-a.

MS Windows 2003 domena

- Napušta se koncept radnih grupa (workgroup)
- U obje mreže uvodi se rad u domeni
- Svaka domena ima svoj mrežni poslužitelj – domenski kontroler (domain controller DC)
- Domenu čine skupovi računala, korisnika i grupa koje je definirao administrator u Active Directory AD imeničkom servisu
- Server ALFA - DC domene LOCAL
- Server BETA – DC domene SKOLA

Domene


INTERNET
ISA
DC ALFA
DC BETA
PROFESORI
UČENICI
Domena LOCAL
Domena SKOLA

MS Windows 2003 domena

- Domenski objekti organiziraju se u organizacijske jedinice OU
  (npr. učenici nekog odjeljenja čine jednu OU)
- Implementacija grupnih politika (Group Policy)
- Centralizirana administracija korisničkih računa
- Centralizirano upravljanje resursima
- Centralizirano upravljanje pravima korisnika i sigurnosnim postavkama

Implikacije uvođenja domene

- Svaki se korisnik prijavljuje u mrežu korištenjem svog korisničkog imena i lozinke
- Prijavom u domenu korisnik ima prava koja su mu dodijeljena, bez obzira sa kojeg se računala prijavio
- Svaki korisnik ima svoj diskovni prostor na disku poslužitelja – osigurava se sigurnost podataka
  Učenik ima inicijalno 20 MB za podatke na mrežnom disku Z

Računala u domeni

- Primijenjena je jedinstvena konvencija imenovanja računala i korisnika u domeni
- Učeničko računalo broj 5 u kabinetu 30 – s30r5
- Olakšan pristup dijeljenim mapama i diskovima pojedinih računala u školi
- Na svim se računalima primjenjuje Windows Update koji će biti centraliziran na serveru
- Na svim se računalima primjenjuje Sophos Antivirus koji će se također nadograđivati centralizirano – SUS

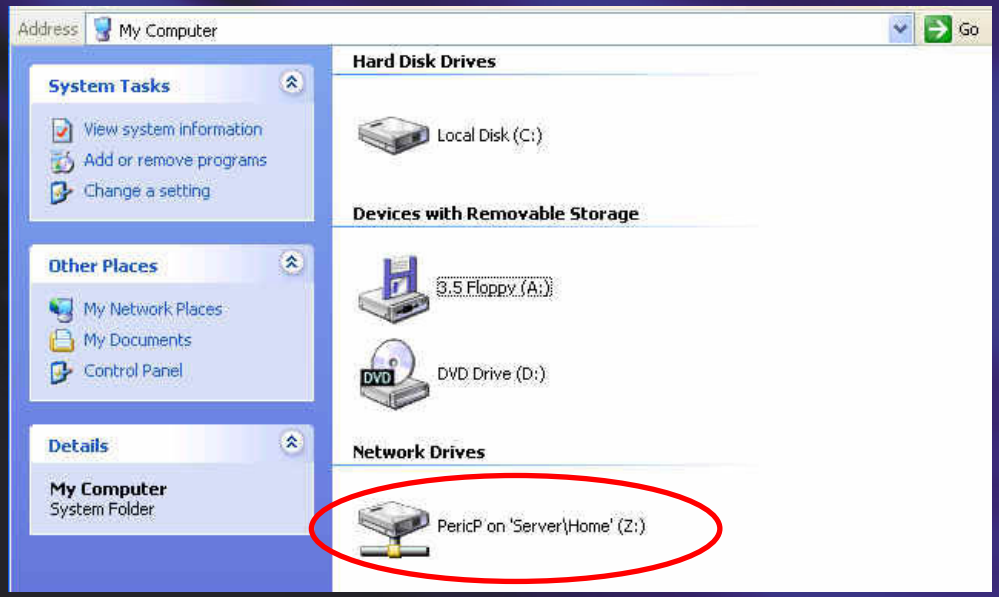
Korisnički profili

- Sadržaj korisničkog profila:
  - My Documents
  - Application data
  - Desktop
  - Favorites
  - Local Settings
  - Cookies
  - Start Menu
  - i drugo

S obzirom da profil korisnika može enormno narasti (i na više GB) izbjegavat će se uporaba roaming profila koji je spremljen na serveru i kopira se često na lokalno računalo.

Pristup mrežnom disku

- Primjenom diskovnih kvota svaki korisnik u domeni ima određnu količinu diskovnog prostora na poslužitelju ALFA ili BETA
- Pristup mrežnom disku Z (My Computer)



Problem zaštite učeničkih računala

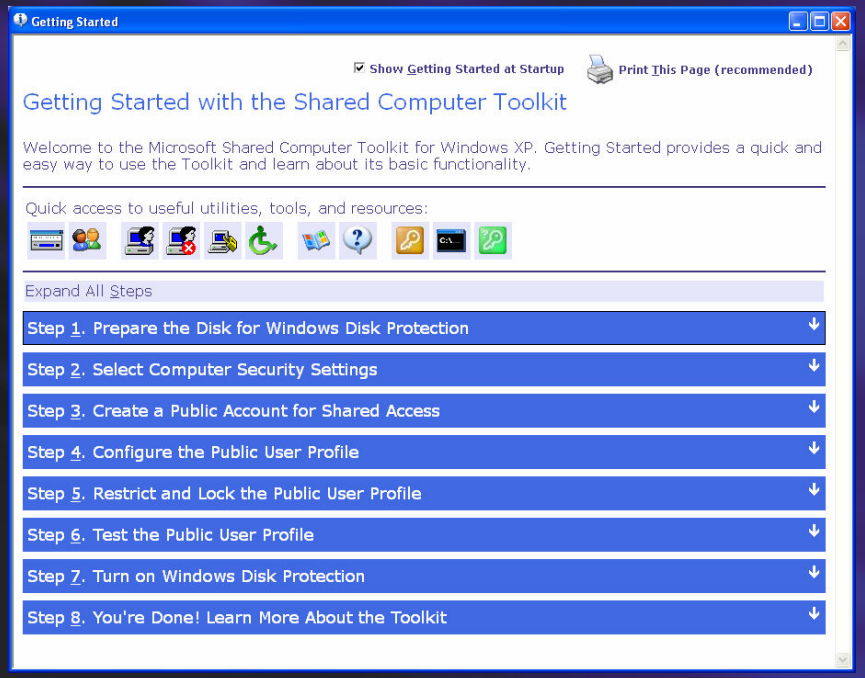
- Nužnost zaštite učeničkih računala od “opasnog” sadržaja koji se lako može prenijeti sa Interneta – instalacije softvera, virusa, spayware-a, adware-a i neprimjerenog sadržaja
- Zaštita računala od promjene radnog okruženja (desktop, ikone, opcije programa, rezolucija,…)
- Idealno rješenje – Microsoft Shared Computer Toolkit for Windows XP

MS Shared Computer Toolkit

- Novi besplatan Micorosoft skup alata kojem je jedna od uloga zaštita sistemskog diska od promjena
- Može se implementirati na MS Windows XP SP2
- Implementiran je na svim računalima koja koriste učenici
- Učenik može instalirati bilo kakav softver, izvršiti bilo kakve promjene na sistemskom disku. Nakon sljedećeg pokretanja računala vraća se izvorna (ispravna) slika diska i sve je na računalu u savršenome redu. Dogradnje sistemskog i aplikativnog softvera (MS update) ostaju sačuvane!

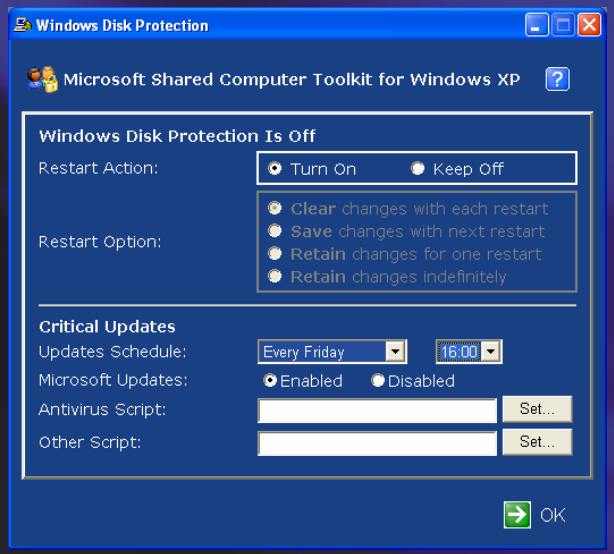
MS Shared Computer Toolkit

- **MS SCT može potrebu za održavanjem računala u kabinetima svesti na minimum, a učenici imaju uvijek čisto radno okruženje**



MS Shared Computer Toolkit

- Kada administrator računala ima potrebu izvršiti neke izmjene na računalu jednostavno isključi zaštitu sistemskog diska (Disk Protection), izvrši promjene, uključi Disk Protection i nakon sljedećeg restarta računala, računalo je opet zaštićeno.



Problemi u našim školama

- Neadekvatne mrežne infrastrukture
- Brze konekcije na Internet mogu donijeti više problema no koristi zbog nesigurnosti računalne mreže
- Nepostojanje i needuciranost sistem administratora
- Mišljenje kako nabava hardvera i softvera rješava sve probleme

Što i kako dalje?

- Računalna mreža ne služi sama sebi
- Kvalitetna i sigurna računalna infrastruktura predstavlja preduvjet razvoja moderne škole
- Mogućnost primjene cijelog niza novih mrežnih tehnologija i servisa u nastavi, pouzdano i efikasno
- Obrazovanje tehničara za računalstvo
- Pilot projekt trebao bi olakšati školama izgradnju sigurnih i kvalitetnih mrežnih infrastruktura

Hvala na pažnji !

vilim.jurkovic@ri.htnet.hr