Vsebina

[Storitve in strežniki 2](#_Toc135673135)

[Spletni strežnik 2](#_Toc135673136)

[Imenski strežnik 3](#_Toc135673137)

[Poštni strežnik 5](#_Toc135673138)

[DHCP strežnik 7](#_Toc135673139)

[Tiskalniški strežnik 8](#_Toc135673140)

[Datotečni strežnik in omrežno shranjevanje 10](#_Toc135673141)

[Datotečni strežnik 10](#_Toc135673142)

[LAN strežniki 11](#_Toc135673143)

[Skupna raba 11](#_Toc135673144)

[FTP strežniki 12](#_Toc135673145)

[Omrežno shranjevanje 12](#_Toc135673146)

[Kaj je NAS in kaj je SAN 13](#_Toc135673147)

[Razlika med NAS in SAN 13](#_Toc135673148)

[Tipična NAS arhitektura 14](#_Toc135673149)

[Izboljšana NAS arhitektura 15](#_Toc135673150)

[Tipična SAN arhitektura 15](#_Toc135673151)

[Imeniški strežnik 16](#_Toc135673152)

[LDBP in LDAP 16](#_Toc135673153)

[Požarni zidovi 17](#_Toc135673154)

[Kaj je požarni zid 17](#_Toc135673155)

[Delitev glede na uporabo 18](#_Toc135673156)

[Osebni požarni zid 18](#_Toc135673157)

# Storitve in strežniki

* Storitve opravljajo servisi v namenskih strežnikih, zato jih po servisih imenujemo (spletni strežnik, imenski strežnik, poštni strežnik…)
* Vsak servis je nameščen na svojem sistemu
* Lahko jih je tudi več na enem sistemu
* Na en strežnik po navadi obesimo eno storitev

## Spletni strežnik

* Omogoča nam spletne storitve
* Deluje na osnovi protokola http (hyper text transfer protocol)
* Omogoča prenos datotek spletnih strani, ki so zapisane s HTML jezikom
* Danes lahko prenaša tudi druge datoteke, ki opisujejo zgradbo spletnih strani z besedili
* Strežnik se odziva na **vratih (port) 80**
* Zahteva stranke podaja absolutni naslov datoteke, ki je pripet k IP št. strežnika
* Strežnik izlušči le naslov datoteke in jo poišče v drevesni strukturi
* Servis (aplikacijo), ki deluje kot spletni strežnik je potrebno namestiti
* Po namestitvi je potrebna konfiguracija spletnega strežnika in zagon servisa
* Pri konfiguraciji pomembna:
  + Nastavitev korenske mape spl. Servisa
  + Nastavitev imena datoteke domače strani (index.html, dafault.asp…)
  + Možne tudi nastavitve »alias-ov« - povezav do »navideznih map«…
* Spletni strežniki omogočajo različne storitve:
  + WWW – svetovni splet
  + Blog – spletni dnevniki
  + Forum – spletne razprave
  + Iskalniki – iskalniki po spletnih straneh (google)
  + Imeniki – spletni imeniki
  + RSS – kratka spletna sporočila
  + …
* Prenosi podatkov niso kriptirani in varovani
* Za varovanje podatkov uporabljajo protokol https (s pomeni secure – varovan) – **vrata 443** (https omogoča kriptiranje)
* Ta protokol je omogočil razvoj dodatnih e storitev, ki jih danes podpirajo spletni strežniki:
  + e – učilnica
  + e – trgovina
  + e – bančništvo
  + e – davki
  + e – uprava
  + …
* Pri teh storitvah je nujna vzpostavitev varne povezave in predstavitev z identifikacijskimi elementi
* 100% varnosti ni

Slika, ki vsebuje besede diagram

Opis je samodejno ustvarjenSpletni strežnik

# Imenski strežnik

* Za vsako domensko ime rabimo unikaten IP naslov
* Strežnikov, ki ponujajo svoje storitve, je v internetnem omrežju vse več
* Vsak izmed njih mora imeti svoj unikatni IP naslov za predstavljanje v omrežju
* Storitve je veliko laže povezati z imeni ponudnikov kot IP številom
* Sistem domenskih imen (Domain Name System = DNS) omogoča uporabo nadomestnih imen (domen), ki nadomestijo IP št. strežnikov
* Internetne domene morajo biti registrirane in organizirane po skupinah
* Skupine so deljene po namenu:
  + .com – komercialne
  + .edu – izobraževalne
  + .gov - vladne
  + .org – organizacijske
  + .si, .de, .jp – državne
* Oznaka skupine je vedno zadnji del zapisa domene
* Domenska imena strežnikov so običajno sestavljena iz treh delov (npr. [www.arnes.si](http://www.arnes.si)):
  + www. – predstavlja ime računalnika – strežnika
  + arnes – (običajno) predstavlja ime podjetja, organizacije ali ustanove
  + si – ime skupine domen
* Domenska imena ne vsebujejo presledkov in posebnih znakov
* Strežnik domen se odziva na zahteve uporabnikov – brskalnikov
* Je servis, ki se odziva na zahteve poslane na vrata 53
* Servis DNS v osnovi ni zahteven, saj za delovanje potrebuje »le« tabelo z vpisi o domenah in pripadajočih IP številih
* Uporabnik potrebuje IP naslov DNS
* Nastavimo ga v omrežnih nastavitvah
* DNS server prejeto poizvedbo z domeno primerja z vpisi v tabeli
* Če najde ekvivalenten vpis, vrne nadomestno IP število
* Zahteva je lahko tudi obratna – prejme IP in vrne domensko ime
* Če iskane domene ni v tabeli, jo preda »nadrejenemu« DNS strežniku
* Če domene ne najde, pride do prekinitve komunikacije zaradi prekoračitve časa
* S pomočjo imenskih strežnikov, namesto IP naslovov, vpišemo le domensko ime in DNS nam vrne IP naslov
* Pridobivanje podatkov s spletnega strežnika poteka v naslednjih korakih:
  + Vpis URL (domenskega) naslova v brskalnik
  + Izločitev domene in njeno pošiljanje v DNS
  + Iskanje zapisa in vrnitev pripadajočega IP naslova brskalnika
  + Zahteva za spletno stran iz preostalega dela naslova za pridobljen IP
  + Vračanje dokumenta s spletno stranjo s strežnika
  + Prikaz vsebine dokumenta v brskalniku
* Pridobivanje IP naslova preko DNS servisa je za uporabnika neviden, saj to nalogo opravi zanj prog. Oprema

Slika, ki vsebuje besede diagram

Opis je samodejno ustvarjenImenski strežnik

# Poštni strežnik

* Klasično pošto obvladuje in premaguje, ima pa tudi določene slabosti
* Problem je predvsem nekriptiran prenos sporočil
* Za prenose skrbi aplikacija poštnega strežnika
* Prejemnik mora imeti na matičnem strežniku poštni predal
* Slednjega predstavlja mapa v datotečnem sistemu (v njej se hranijo sporočila)
* Poštni predal je poimenovan z uporabniškim imenom, ki se navezuje na poštni naslov:
  + uporabnik@ponudnik.domenska sk.
* Do predala dostopa uporabnik z ustrezno aplikacijo
* Za opravaljanje vseh funkcij mora poštni strežnik opravljati tri storitve:
  + Pošiljanje pošte – drugim uporabnikom (poštni strežnik bo naprej poslal pošto iz mojega računalnika)
  + Prejemanje pošte – za svoje uporabnike (»moj« poštni strežnik mora prejeto pošto dati v moj pošni predal
  + Posredovanje pošte – svojim uporabnikom (strežnik posreduje prejeto pošto k meni)
* V ta namen uporablja tudi različne protokole za prenos poštnih sporočil:
  + SMTP (Simple Mail Transport Protocol) – za pošiljanje in prejemanje sporočil (protokol, ki omogoča, da pošta potuje naokoli, prenaša sporočila nekriptirano)
  + POP3 (Post Office Protocol V3) – za prenos sporočil med poštnim predalom in uporabnikom (omogoči, da se predstavimo, da smo res lasntiki), sporočila se shranijo direktno na rač
  + IMAP (Internet Message Access Protocol) – za prenos med poštnim predalom in uporabnikom (sporočila se na strežniku ne zbrišejo, le preberemo jih in ne shranjujemo na računalnik), sporočila se shranijo na poštni predal
* Pošiljanje sporočila strežniku se vrši preko **vrat 25**
* Prejeto sporočilo se shrani v poštni nabiralnik uporabnika
* Prenos sporočil iz nabiralnika teče s POP3 protokolom preko **vrat 110**
* Sporočila se privzeto prenesejo na uporabnikov računalnik
* V nabiralniku na strežniku kopija ne obstaja

POP3/SMTP email client and server

Slika, ki vsebuje besede besedilo, pismo

Opis je samodejno ustvarjen

* Prenos sporočil iz nabiralnika lahko opravimo z IMAP protokolom
* Ta uporablja **vrata 143**
* Sporočila se ohranjajo na strežniku
* Uporabnik jih mora sam izbrisati

IMAP4/SMTP email client and server

Slika, ki vsebuje besede besedilo, pismo

Opis je samodejno ustvarjen

* Potovanje pošte lahko predstavimo z naslednjimi koraki:
  + U porabnik sestavi sporočilo v svojem rač.
  + Sporočilo pošlje preko SMTP protokola do strežnika svojega ponudnika IS
  + Glede na prejemnikov poštni naslov se strežnik odloči, če mora sporočilo poslati naprej do naslednjega strežnika
  + Če da, ga pošlje preko SMTP protokola
  + Končni poštni strežnik shrani sporočilo v poštni nabiralnik uporabnika
  + Če je uporabnik »na zvezi«, strežnik posreduje sporočilo uporabniku (POP 3 ali IMAP – kot je nastavljena aplikacija)
  + Če uporabnika ni »na zvezi«, sporočilo počaka v nabiralniku do uporabnikove prijave
* Pri spletnih odjemalcih se prenosi vršijo preko spletnih protokolov

Slika, ki vsebuje besede diagram

Opis je samodejno ustvarjen

# DHCP strežnik

* Omogoča nam avtomatsko nastavitev omrežnih lastnosti omrežnih naprav
* Za komunikacijo v IP omrežju potrebujejo naprave lasten IP, prehod in za brskanje po spletu še IP DNS
* Deluje na osnovi protokola DHCP (Dynamic Host Configuration Protocol) – po njem tudi ime
* Uporabimo lahko enega ali več strežnikov, tudi v majhnih omrežjih
* Centralno opravi nastavitve namesto administratorja ob vsakem zagonu omrežne naprave.
* Strežnik se odziva na **Vratih 67**
* Za delovanje potrebujemo DHCP strežnik in omrežno napravo, ki je konfigurirana za uporabo DHCP storitve
* Administrator DHCP strežnika mora pripraviti:
  + Začetni naslov področja dinamičnih IP naslovov
  + Velikost naslovnega področja – št. dinamičnih IP naslovov
  + Čas veljavnosti dodeljenega IP naslova
* Večina DHCP servisov ima možnost tabeličnega pregleda klientov:
  + MAC naslov ime naprave
  + Dodeljeni IP
  + Čas veljavnosti
  + Omrežni vmesnik (Ethernet WLAN)
* Naprava ob zagonu vpraša po pridobitvi omrežnih nastavitev
* Strežnik po povpraševanju ponudi podatke, ki zajemajo;
  + IP prehoda
  + Domensko ime
  + IP DNS
  + Časovni strežnik
  + Omrežno masko
  + IP število
* Obstajajo 3 različne metode delovanja IP naslovov:
  + Dinamično:
    - Strežnik pripravi IP naslov, ki po določenem času poteče. Naprava mora poslati novo zahtevo. IP je lahko isti ali pa ne
  + Avtomatično
    - Strežnik hrani zapise IP naslovov naprav, da lahko po preteku veljavnosti IP naslova, napravi ponovno zagotovi isti IP naslov
  + Statično
    - Strežnik ima seznam naprav (MAC naslovi) in njim pripadajočih IP naslovov. IP naslovi so tako rezervirani za naprave in le te jih lahko dobijo
* Naprava po prejemu ponudbe izbere (če jih je več) eno in pošlje strežniku zahtevo
* Strežnik vrne potrditev veljavnosti uporabe dodeljenega IP naslova
* Komunikacija z uporabo protokola UDP in broadcast prenosa podatkov – naprava nima svojega IP
* Prenos podatkov se usmerja z MAC naslovi
* Po pridobitvi IP naslova mora naprava preveriti njegovo unikatnost
* Omrežna konfiguracija se izvrši v 4 korakih:
  + Naprava poda zahtevo za pridobitev IP
  + DHCP strežnik vrne ponudbo (IP offer)
  + Naprava zahteva IP (IP request)
  + DHCP strežnik potrdi dodelitev IP (IP lease acknowledgement)

Slika, ki vsebuje besede diagram

Opis je samodejno ustvarjen

# Tiskalniški strežnik

* Je naprava, ki povezuje tiskalnike z delovnimi postajami preko omrežja
* Realiziran je lahko na tri načine
  + Strežnik: računalnik namenjen le tiskanju na priključen tiskalnik
  + Delovna postaja s tiskalnikom v skupni rabi: tiskalnik uporaben za več uporabnikov z več delovnih postaj
  + Tiskalniška naprava: posebna namenska naprava vključena v omrežje
* Nameščena posebna prog. oprema – tiskalniški servis (že vgrajen v OS, za delovanje tiskalnika)
* Z opravljanje naloge uporabljajo ti servisi različne protokole
* Odziv na tiskalniška opravila uporabnikov se vrši na **vratih 35**
* Servis sprejema tiskalniška opravila uporabnikov, ki jih mora posredovati do ustreznih tiskalnikov
* Praviloma servisirajo več uporabnikov
* Tiskalniki so počasne naprave, zato servisiranje tiskanja ene datoteke traja kar neka časa
* V tem času servis ne bi bil dosegljiv drugim uporabnikom
* Za preprečevanje zasedenosti servisa uporabljajo slednji tiskalniške vrste:
* Pri uporabi tiskalniške vrste se tiskalniški servis deli na dva dela:
  + Sprejemni del: sprejema podatke za tiskanje v vrsto (mora biti vedno na razpolago)
  + Tiskalni del: tiska podatke na tiskalniku
* Sprejemni del se odziva na zahteve uporabnikov:
  + Sprejme zahtevo za tiskanje
  + Izbere pravo tiskalniško vrsto glede na zahtevani tiskalnik
  + Zapiše datoteko in vse ostale potrebne lastnosti v vrsto
  + Shrani podatke za tiskanje v začasno delovno področje na disku
* Nalogo lahko opravlja paralelno za več uporabnikov
* Tiskalni del skrbi za tiskanje na tiskalnikih
* Sestavljajo ga:
  + Rutine OS za tiskanje v ozadju
  + Gonilnik za posamezni tiskalnik
* Tiskalniške vrste lahko delujejo na dva načina:
  + Tiskanje po sprejetju podatkov:
    - Vsi podatki za tiskanje morajo biti preneseni in shranjeni v celoti preden se lahko tiskanje prične (slabost: čakanje, prednost: tiskanje lahko prekinemo)
    - Napake med prenosom se odpravljajo sproti
    - Če uporabnik prekine tiskanje, se vpis avtomatsko izbriše (prednost)
    - Tiskanje se izvede šele po vpisu v vrsto in uspešnem prenosu podatkov
  + Tiskanje med sprejemanjem podatkov
    - Vpis v vrsto in tiskanje se začne že po prejemu prvega paketa podatkov
    - Tiskanje se izvaja sproti med prejemanjem podatkov (prednost: hiter odziv, slabost: v primeru napak pri prenosu se tiskanje prekine, zato je natisnjen le del dokumenta)

Slika, ki vsebuje besede diagram, shematično

Opis je samodejno ustvarjen

# Datotečni strežnik in omrežno shranjevanje

## Datotečni strežnik

* Je računalnik za nameščenim datotečnim servisom, ki omogoča delovnim postajam dostop do svojega datotečnega sistema
* Priključen v omrežje, preko katerega imajo delovne postaje dostop
* Osnovni namen – zagotavljanje diskovnega prostora za skupno rabo
* Z njim shranjujemo datoteke
* Njihova vsebina je zelo različna
  + Dokumenti
  + Slike
  + Filmi
  + Podatkovne baze
  + Zvočne datoteke
  + …
* Uporabniku določimo omejeno velikost datotek
* Datotečni strežnik se nam predstavi kot dodatni disk
* Nanj praviloma ne shranjujemo velikih datotek
* Strežnikova vloga je omogočanje najhitrejšega dostopa in prostora datotečnega sistema delovnim postajam
* Uporabljamo jih v pisarnah, šolah, ustanovah, doma…
* Datotečni strežniki so lahko
  + Namenski: zasnovan le za »datotečne storitve« do delovnih postaj
  + Nenamenski: opravlja tudi druge servise (tiskalniški, dhcp)
* Za zagotavljanje servisa mora imeti na disku nameščen datotečni sistem
* Zanj skrbi os – je njegov del
* Zapisani podatki se delijo na:
  + Drevesno strukturo
  + Uporabnikove podatke – datoteke
  + Podatke o datotekah – lastnosti, pravice…
* Najpomembnejše so lastnosti:
  + Enostavnost uporabe
  + Zmogljivost in hitrost
  + Sposobnost upravljanja z datotekami različnih velikosti
* V vseh datotečnih sistemih morajo delovati osnovne funkcije:
  + Zapis in branje datoteke
  + Brisanje datoteke
  + Premik datoteke
  + Ustvarjanje in odpiranje mape
  + Brisanje mape
  + Premik mape
  + (nastavlanje pravic)
* Datotečne strežnike lahko razdelimo po dostopni metodi do datotek (realiziramo na več načinov):
  + LAN strežniki
  + Skupna raba
  + FTP strežniki
* Vsak uporaben v svojem okolju, lahko pa skrbijo za iste datoteke
* Slabost: rabimo svoj računalnik, za katerega moramo skrbeti
* Prednost: imamo kopije datotek na enem kupu

## LAN strežniki

* So namenski računalniki v LAN omrežju za hranjenje podatkov
* Imajo strežniški OS za hitro odzivanje
* Kot pomnilnik uporabljajo polja diskov (RAID) – uporabljajo se kot NAS ali SAN
* Za povečevanje hitrosti imajo večjo količino predpomnilnika (cache) – hitrejši od magnetnih diskov
* Administrator bdi nad delovanjem in vzdržuje sistem
* Administrator ureja uporabnike in jim dodeluje pravice
* Uporabniki dobijo dostop do svojega dela pomnilniškega prostora
* Adminstrator lahko pripravi tudi skupne mape za več (vse) uporabnike
* Podatki shranjeni varno (poskrbljeno za varnostne kopije)
* Za komuniciranje se najpogosteje uporablja NFS (Network File System)
* Protokol omogoča prikaz in delo z oddaljenim datotečnim sistemom kot z lokalnim
* Danes obstaja več različnih platform, ki so nameščene v OS
* V Windows je v ta namen nameščen Windows Networking

## Skupna raba

* Je princip deljenja virov delovne postaje z drugimi uporabniki
* V skupno rabo lahko damo želeni del datotečnega sistema (tudi optični pogon) kot tudi tiskalnike v lokalnem omrežju
* Za skupno rabo skrbi OS delovne postaje – ni posebej prilagojen za hiter odziv
* Administrator delovne postaje mora poskrbeti za pravice dostopa ko tudi za uporabnike na sistemu
* Uporabniki so lahko le lokalni ali tudi z drugih sistemov
* Vsakega mora sistem poznati (problem št. uporabnikov) – priprava skupnega uporabnika
* Vzdrževanje in nadzor mora opravljati administrator delovne postaje ali eden od uporabnikov z dovolj pravicami
* Za deljenje virov v skupno rabo poseben postopek

## FTP strežniki

* So datotečni strežniki v internetnem (intranetnem) okolju
* Za komuniciranje uporabljajo ftp protokol
* Praviloma je potrebna prijava z uporabniškim imenom in geslom
* Na strežniku nameščen ftp servis, ki čaka na zahteve
* Zanj in za uporabnike skrbi administrator
* Prenos datotek je nekoliko počasnejši
* FTP – nevarovan / nekriptiran
* FTPS – varovana / kriptiran
* *Komunikacija:*

1. *Vrata 21*
2. *Dogovarjanje za vrata*

* Za delo moramo namestiti na delovno postajo ustrezno aplikacijo
* Komunikacija poteka preko dveh povezav
  + Kontrolne: preko vrat 21 v času celotne seje
  + Podatkovne: preko drugih vrat (odvisno od načina dogovora stranka-strežnik)
* Ukaze lahko pišemo ali jih generira ustrezen grafični vmesnik aplikacije

# Omrežno shranjevanje

* Omogočajo ga omrežne naprave za shranjevanje podatkov
* LAN datotečni strežniki zelo primerni:
  + Varovan dostop
  + Prostor za datoteke
  + Avtomatsko arhiviranje
* Shranjevanje preko interneta
  + Počasno, drago, posebni ponudniki
  + Primerno za manjše količine podatkov
* Vsak strežnik ima svoj disk za shranjevanje podatkov
* Težave s povezovanjem, vzdrževanjem

Slika, ki vsebuje besede besedilo, risanje, rokopis, skica

Opis je samodejno ustvarjenTežava

Rešitev problema

* Uvesti skupno pomnilno napravo
* Uporabna naj bo za vse aplikacije

Slika, ki vsebuje besede besedilo, rokopis, skica, risanje

Opis je samodejno ustvarjen Rešitev

Prednosti

* Povezovanje podatkov med seboj in vsi podatki bodo na enem mestu
* Cnetralizirano upravljanje
* Enostavna razširljivost
* Večja prožnost v primeru napak

## Kaj je NAS in kaj je SAN

* NAS (Network Attached Storage)
  + Pomnilne naprave dosegljive preko omrežja
  + Dostop s TCP/IP protokolom
  + Uporaba datotek z NFS, HTTP ali Windows Networking
* SAN (Storage Area Network)
  + Pomnilne naprave dosegljive preko stikala z optičnimi vlakni
  + Uporablja enkapsulirano SCSI tehnologijo

## Razlika med NAS in SAN

* Povezave:
  + NAS – TCP/IP (običajno UTP, lahko tudi optična vlakna)
  + SAN – optična vlakna
* Protokoli:
  + NAS – NFS, http (počasnejši od SAN)
  + SAN – enkapsuliran SCSI (zna prenašati samo bloke podatkov)
* Dostop do podatkov:
  + NAS: knjižnični
    - Datoteke, podatki o dovoljenjih, varnost
  + SAN: skladiščni
    - Grobi bloki podatkov

Slika, ki vsebuje besede besedilo, rokopis, skica, pisava

Opis je samodejno ustvarjen

* Pozicija datotečnega sistema
* Pri NAS na pomnilni napravi
* Pri SAN na aplikacijskih strežnikih

Slika, ki vsebuje besede besedilo, rokopis, skica, risanje

Opis je samodejno ustvarjen

## Tipična NAS arhitektura

* Dostop do pomnilniških naprav za vse »udeležence« v omrežju
* Ob gostem prometu v omrežju čakata tudi strežnika na dostop do pomnilnih naprav

Slika, ki vsebuje besede besedilo, rokopis, skica, risanje

Opis je samodejno ustvarjen

## Izboljšana NAS arhitektura

* Za doseganje višje hitrosti delovanja omrežnih servisov

Slika, ki vsebuje besede besedilo, skica, risanje, rokopis

Opis je samodejno ustvarjen

* Strežnika imata prednost pred ostalimi uporabniki v omrežju

## Tipična SAN arhitektura

* Zaradi drugačnega dostopa do pomnilnih naprav so ločene od LAN

Slika, ki vsebuje besede besedilo, skica, risanje, rokopis

Opis je samodejno ustvarjen

* **Združitev – prednosti obeh**

Slika, ki vsebuje besede besedilo, rokopis, skica, risanje

Opis je samodejno ustvarjen

# Imeniški strežnik

* Je servis, ki dostopa do podatkov v podatkovni bazi (TCP/IP vrata 389) – podatki o uporabnikih, napravah, programski opremi…
* Njihova uporaba v omrežjih je namenjena podatkom o uporabnikih, skupinah, računalnikih, programski opremi…
* Servis predstavlja centraliziran sistem za administracijo in varnost sistema
* Do podatkov dostopajo le pooblaščeni (skrbniki, strežniki)
* Odvisno od pravic uporabnika lahko slednji podatke
  + Prebirajo, pridobivajo, iščejo (strežniki)
  + Dopisujejo, popravljajo (skrbniki)
* Imeniški strežnik je s svojimi podatki odgovoren za:
  + Avtentifikacijo (prepoznava uporabnika)
  + Avtorizacijo (prepoznava pravic)
* Podatkovna baza je hiearhična
* Vsak objekt je zapisan s svojim vnosom (je enolično poimenovan)
* Običajno dobi tudi UUID (Unique User ID)
* Za opis objekta ima slednji več lastnosti – odvisne od vrste objekta
* Podatkovna baza je lahko porazdeljena tudi na več mestih
* Za dostop uporabljen LDAP protokol (Lightweight Directory Acces Protocol)

## LDBP in LDAP

* LDBP (Lightweight Directory Browsing Protocol) je predhodnik, ki je omogočal le pridobivanje podatkov iz baze podatkov
  + Zaradi porazdelitve podatkovne baze možni vpisi podatkov le v strežnikih
  + Težave z administracijo
  + Sprememba načina delovanja in poimenovanja protokola
* LDAP (Lightweight Directory Acces Protocol)
  + Postane protokol za dostopanje in vzdrževanje porazdeljenih baz imeniških storitev
  + Deluje preko protokolnega sklada TCP/IP

# Požarni zidovi

Razlogi za uvajanje požarnih zidov

* Za enostavnejšo komunikacijo med računalniki – računalniške mreže
* Z mrežami je omogočena izmenjava podatkov iz računalnika v računalnik
* Zahteve potujejo navzven
* Odgovori na zahteve prihajajo nazaj
* Komunikacija – dvosmerna
* Naša pot do informacij navzven omogoča drugim dostop do informacij v našem računalniku
* Dvosmerno komuniciranje je zaželeno in potrebno
* Določene podatke celo javno nudimo (svetovni splet)
* Določeni ljudje želijo priti do podatkov, ki niso za javnost (neetični hackerji)
* Računalnik je v mreži izpostavljen napadu
* Nelegalen dostop do podatkov je mogoč zaradi:
  + Slabo napisanega operacijskega sistema ali programske opreme
  + Naivnosti in nevednosti uporabnikov
* Napadalci izkoriščajo znane težave – slabosti predvsem OS
* Naloga vsakega uporabnika – sprotno posodabljanje sistemske in uporabniške prog. opreme
* Nevarnost preži tudi preko elek. pošte in na spletu
* Vdiralci napišejo razne programe in upajo, da jih bodo uporabniki pognali
* Uporabnik običajno ne ve, da gre za škodljivi program
* Programi posredujejo privatne podatke o žrtvi
* Sistem je potrebno zaščititi pred odtekanjem zaupnih informacij

## Kaj je požarni zid

* Je del računalnika, ki preprečuje nedovoljeno pretakanje podatkov in omogoča dovoljen pretok podatkov
* Preprečuje, da bi od zunaj nekdo prišel do podatkov v našem računalniku
* Njegovo delo je dovoljevati oz. zavračati komunikacijo glede na postavljena pravila
* Je poseben del, ki je zadolžen za mrežno varnost sistema (»od zunaj«)
* Izveden je lahko kot:
  + Strojna oprema
  + Programska oprema
  + Lahko tudi kombinacija
* Večinoma nameščen med javnim in privatnim omrežjem
* Integriran v usmerjevalniku
* Na računalnik namestimo ustrezno prog. opremo, ki opravlja nalogo požarnega zida
* V programski obliki je dandanes nameščen tudi na vsakem računalniku

Slika, ki vsebuje besede besedilo, rokopis, tabla, diagram

Opis je samodejno ustvarjen

## Delitev glede na uporabo

* Zaradi nujnosti zaščite uporabljen na vseh področjih
* Glede na namen uporabe delimo na:
  + Osebne požarne zidove
  + Kombinirane naprave
  + Požarni zidovi za profesionalno uporabo
* Glede na namen se odraža tudi zapletenost in zmožnosti požarnih zidov

### Osebni požarni zid

* Nameščeni na osebnih računalnikih
* Zagotavljajo varnost le enemu
* V tesni povezavi z OS in varnostjo
* Običajno združen v varnostni center
  + Nadzor nad »zunanjo« varnostjo
  + Nadzorovanje protivirusne prog. opreme za »notranjo varnost«
  + Skrb za posodabljanje OS
* Ne koristi brez varnostnih posodobitev

## Kombinirane naprave

* Predvsem za domačo uporabo
* Zaščita omrežja z večfunkcijsko napravo (usmerjevalnik, stikalo)
* Take naprave priključujejo domače omrežje v internet in opravljajo:
  + Vlogo usmerjanja prometa
  + NAT – preslikave omrežnih servisov
  + Funkcijo požarnega zidu (z omejenimi nastavitvami)

## Požarni zid za profesionalno rabo

* Usmerjevalniki z vgrajenim NAT in požarnim zidom
* Požarni zid z mnogo več funkcijami kot v kombiniranih napravah
* Osnova posebna strojna oprema (lahko tudi starejši rač.) s prirejenim OS Linux za opravljanje naloge požarnega zidu

## Delitev glede na delovanje

* Skozi razvoj posegajo v pretok informacij na različne načine
* Kljub poseganju morajo zagotavljati visoko pretočnost dovoljenih podatkov
* Delitev glede na delovanje
  + Paketni filtri
  + Aplikacijski usmerjevalnik
  + Sejni usmerjevalnik
  + Proxy strežnik
* Paketni filter
  + Preverjajo podatke (glave IP in TCP) in jih izločajo glede na postavljena varnostna pravila
  + Je najpreprostejša in tudi najmanj varna oblika zaščite
  + Ne preverja (ne) varnosti vsebine podatkov
  + Med javnim in domačim omrežjem – filtrira pakete, ki lahko vstopijo v naše omrežje in tiste, ki ne smejo
* Aplikacijski usmerjevalnik
  + Preverjajo varnostne mehanizme znotraj aplikacijskih protokolov (FTP, DNS…)
  + Njihova prednost je v »razumevanju« delovanja aplikacij in njihovih protokolov
  + Lahko zazna poseganje določenega protokola po nestandardnih vratih z namenom škodljivega dostopanja
  + Je veliko varnejši od paketnih filtrov
* Sejni usmerjevalnik
  + Preverjajo varnost ob vzpostavljanju TCP ali UDP povezave
  + Če povezava ustreza varnostnim pravilom, se nadaljuje preverjanje paketov seje ne izvaja več
  + Nevarni paketi znotraj vzpostavljene seje lahko ogrozijo varnost sistema
  + Je veliko varnejši od paketnih filtrov
* Proxy strežnik
  + Deluje na namenski strojni opremi ali kot programska oprema na računalniku
  + Prestreza pakete in jih sestavlja v celoto
  + Pregledajo vsebino in se glede na varnostna pravila odločajo o posredovanju vsebine (omejevanje dostopov)
  + Npr. paket trojanskega konja bo prepoznal in onemogočil prehod podatkov

## Primer vzpostavitve varnosti v LAN v podjetju (Z DMZ)

* Primer podjetja in zahtev omrežja
  + V podjetju LAN omrežje
  + Povezava v svet – internet
  + Postavitev lastnega WWW strežnika
  + Postavitev lastnega poštnega strežnika
  + Podatki v LAN so pomembni – potrebno dobro varovanje proti vdorom
  + Dostop do računalnika mora biti zunaj onemog očen
* Komunikacija stranka-strežnik (client-server) poteka v štirih korakih:
  + 1. Poizvedba stranke po strežniku (pozdrav)
  + 2. Odgovor strežnika – »vzpostavitev komunikacijskega kanala«
  + 3. Prenos strankine zahteve do strežnika
  + 4. Odgovor strežnika na zahtevo v dveh delih
    - (ne)uspešnost izvedbe zahteve
    - Zahtevani podatki
      * Sledi avtomatska prekinitev komunikacijskega kanala s strani strežnika zaradi sprostitve zasedenih virov
* Komunikacija med stranko in strežnikom sloni na komunikacijskem protokolu – rač. jeziku