VARNOST SISTEMA

Varnost sistema delimo na dve področji:

- ZANESLJIVOST SISTEMA(pomeni zagotavljanje pogojev za delovanje regularnih storitev in za dostop uporabnikov do njih)
- ZAŠČITA SISTEMA(onemogoča izvajanje nelegalnih storitev in preprečuje dostop nelegalnim (neregistriranim) uporabnikom do sicer legalnih storitev in drugih virov sistema(podatkov))

PREDSTAVITVENA PLAST

-leži med aplikacijsko in plastjo seje.

1. zagotavlja združljivost podatkov (predstavitve tipov podatkov)
2. zagotavlja združljivost podatkov kodnih strani (črk in številk)
3. storitve kompresije podatkov
4. storitve, ki zagotavljajo varnost podatkov (kriptiranje in kodiranje – dekodiranje)

ASN.1 (zapis abstraktne informacije 1) – standard univerzalne sintakse, primer prenos podatkov iz stare baze v novo.

KLASIČNA SUBSTITUCIJSKA METODA

Abeceda je pomaknjena za nekaj mest

Primer:

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	S	š	t	u	v	u	ž
u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	N	o	p	r	s	š	t

JULUA → NAPAD

VIEGENERJEV DIAGRAM

Pri Viegenerjevem diagramu potrebujemo geslo po katerem bomo kriptirali. Kriptiramo sd pomočjo tabele ki je za slovensko abecedo velika 25x25

Primer :

Kot geslo vigenerjevega diagrama vzemimo VSEZAVERODOMCESARJA
Kriptirali pa bomo FINANČNA ZAKONODAJA J…

v	s	e	Z	a	v	e	r	o	d	o	m	c	e	s	a	r	j	a
f	i	n	A	n	č	n	a	z	a	k	o	n	o	d	a	j	a	j

Ključ: ČCŠZNAŠRMDBČPTVACJA

a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž
b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a
c	č	D	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b
č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c
d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č
e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d
f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e
g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f
h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g
i	j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h
j	k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i
k	l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j
l	m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k
m	n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l
n	o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m
o	p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n
p	r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o
r	s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p
s	š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r
š	t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s
t	u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š
u	v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t
v	z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u
z	ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v
ž	a	b	c	č	d	e	f	g	h	i	j	k	l	m	n	o	p	r	s	š	t	u	v	z

Viegenerjeva matrika za slovensko abecedo

PORTERJEV DIAGRAM

Razširjen Viegnerjev diagram, le da potrebujemo za dekodiranje enega zanka dva simbola

	1	2	3	4
1	a	b	c	d
2	e	f	g	h
3	i	j	k	l
4	m	n	o	p

124334 → ELO

TRANSPOZICIJSKI KRIPTOGRAM

Način kodiranja, pri katerem so znaki med sabo premešani tako, da nimajo za vdiralca nobene vrednosti. Izberemo si ključ, v katerem ni dveh enakih črk. Sporočilo zapišemo v tabelo pod ključ, nato pa jemljemo stolpce iz te tabele po abecednem redu črk, ki sestavljajo ključ, le-te nize potem uvrščamo v niz. Dandanes nima neke vloge pri kriptiranju podatkov, na voljo so boljše rešitve.

ENKRIPCIJSKI STANDARD DES (Data Encription Standard)

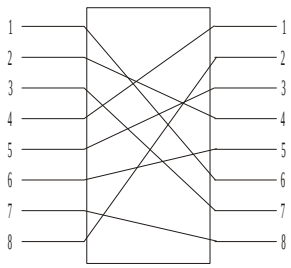
- standard za zakrivanje podatkov
- poznamo ga od leta 1977
- simetričen in ima substitucijske in transpozijciske lastnosti

PERMUTACIJA IN SUBSTITUCIJA

Transpozicijske metode so v računalniškem okolju permutacije, med te prištevamo redukcije in ekspanzije, substitucijske operacije pa ohranjajo svoje ime tudi v računalništvu. Osnovni gradniki kriptografskih metod, ki izvajajo substitucije in permutacije, imenujemo S in P - škatle.

Ključ permutacije – spremenjeno zaporedje vhodnih bitov, ki jih dobimo na izhodu P-škatle.

Primer:



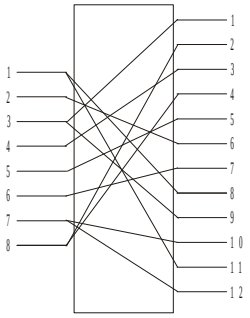
1	2	3	4	5	6	7	8
6	4	7	1	3	5	8	2

KLJUČ(4 8 5 4 2 6 3 7)

P – ŠKATLA:

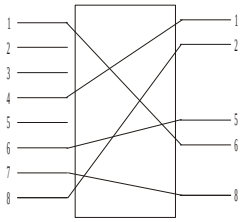
Funkcija P-škatle je, transpozicija vhodnih signalov. Delovanje osnovne P-škatle je prikazano na prejšnji sliki, pri primeru permutacije. Poznamo pa še dve različici P-škatle ekspanzijska in pa kompresijska

- EKSPANZIJA: v tem primeru se število izhodov škatle večje kot število vhodov. Nekateri biti se preslikajo na več izhodov.



Ključ(3 8 4 8 5 2 6 1 3 7 1 7)

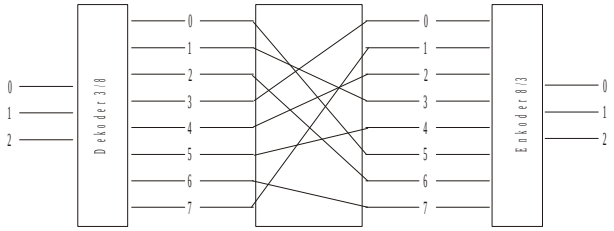
- REDUKCIJA: v tem primeru je število izhodov iz škatle manjše kot število vhodov. Nekateri vhodi ostanejo neuporabljeni. Če z nekim ključem reduciramo Vhod, za izhod biti, ki so prazni spoloh niso pomembni



Ključ(4 8 6 1 7)

S – ŠKATLA:

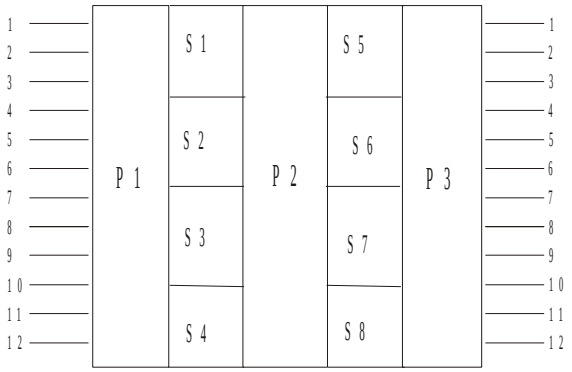
S-škatla izvaja substitucijske preslikave nad **nizom** bitov. Sestavljena je iz dekoderja, S-škatle in pa enkoderja.



Ključ(4 8 5 4 2 6 3 7)

Kombinacija S-škatel in P-škatel

Ko sestavljamo obe vrste škatel dobimo kaskado preslikav. Ključ celotnega sistema sestavlja množica ključev posameznih substitucij in permutacij.



OPIS ALGORITMA DES

Delovanje:

Podatkovni blok je dolg 64-bitov. 56-bitni osnovni ključ se pretvori (ekspandira) v 16 64-bitnih ključev, od katerih vsak sodeluje v eni od 16 substitucijskih peramutacijskih preslikavah v kaskadni povezavi. Algoritem je simetričen (enkripcijski in dekripcijski ključ sta enaka).

Obstaja tudi metoda enkratnega ključa, ki omogoča kodiranje toka podatkov (ne blokov, kot osnovni DES, opisan zgoraj). V ta namen se uporablja enkripcijski stroj. Poskrbeti je treba, da stroja na obeh straneh (sprejemnik, oddajnik) na začetku dobita isti ključ, prav tako morata biti sinhronizirana na bloke dolžine 64-bitov, ki predstavljajo »hrano« za generiranje neskončnega ključa.

Ključ(P1,P2,P3,S1,S2,S3,S4,S5,S6,S7,S8)

POMANJKLJIVOSTI DES ALGORITMOV

Prednosti:

Omogoča hitro enkripcijo, relativno trdoživ, preprost.

Pomanjkljivosti:

Vsi uporabniki morajo imeti isti ključ, komunikacijo tako otežkoča distribucija ključa. Uveljavi se tako imenovana metoda puzzles, ki pa je zelo ranljiva (3-4 ure nato je možno razbitje kode). Uveljavi se kriptografija z javnim ključem.

KRIPTIRANJE Z JAVNIM KLJUČEM

Vsi algoritmi so asimetrični (enkripcijski in dekripcijski ključ sta različna).

MIT – RSA

Najbolj znan algoritem za zakrivanje podatkov z javnim ključem, temelji na celoštevilski algebri in izkorišča lastnosti velikih praštevil. Iz dveh naključnih velikih praštevil generiramo tajni dekripcijski ključ, nato izračunamo javni enkripcijski ključ, podatke kriptiramo. Velja, da mora biti karseda težko razbiti algoritem iz znanih podatkov, uporabljenih pri kodiranju podatkov, za določanje tajnega dekripcijskega ključa.

Slabost alogritma je počasnost (potenciranje dveh velikih praštevil). Uporablja se v kombinaciji skupaj z DES (ključ se distributira, kriptiran z RSA, nato kriptiranje poteka po DES algoritmu).

ELEKTRONSKI PODPIS

Elektronski podpis je medsebojno identificiranje uporabnikov. Bistvo tega je, da oddajnik zapiše neko informacijo, ki je lastna le njemu samemu (tajni dekripcijski ključ D). S tem ključem je kriptirano sporočilo. Če ga sprejemnik razvozla z javnim ključem E, je identifikacija uspela. Da oddajnik ne bi mogel tajiti svoje verodostojnosti, se v ta namen rabi nekakšna oblika notarja, ki te ključe hrani za določen čas veljavnosti ključa. Elektronski podpis se uporablja za ugotavljanje verodostojnosti sporočila (tudi nekriptiranega), se pravi, da sporočilo med prenosom ni bilo spremenjeno.

Primer teh mehanizmov je varnostni sistem PGP (Pretty Good Privacy), ki zagotavlja postopke za iskanje velikih praštevil, izračunavanje javnih, tajnih ključev, generiranje elektronskega podpisa, itd.y), ki zagotavlja postopke za iskanje velikih praštevil, izračunavanje javnih, tajnih ključev, generiranje elektronskega podpisa, itd.

PREDSTAVITVENE STORITVE

Predstavitvene storitve usklajujejo in prevajajo med različnimi oblikami zapisa podatkov ter skrbijo za njihovo varnost.Storitve povezane s predstavitvijo podatkov delimo v štiri skupine:

1. Storitve, ki zagotavljajo združljivost predstavitve različnih tipov podatkov:

Računalniška sistema, ki v sodelovanju opravljata neko nalogo, imata pogosto različno kodirane podatke, ti podatki med seboj niso združljivi in jih je potrebno prevesti v ustrezno obliko. V porazdeljenem sistemu moramo za učinkovito prevajanje zagotoviti univerzalno sintakso, ki premošča razlike med binarnimi predstavitvenimi sistemi. Primer univerzalne sintakse za zagotavljanje združljivosti med predstavitvami je ASN.1 (zapis abstraktne sintakse št.1)

2. Storitve, ki omogočajo združljivost predstavitve črk in številk(kodne strani)

Kodna Stran je tabela v kateri vsakemu znaku(črkam, številkam, ločilom,..) ustreza enolično določeno število.

Računalnika na katerem delujeta aplikaciji (1 aplikacija uporablja kodno stran ASCII, 2 pa IBM-ov EBCDIC) se med seboj ne razumeta, čeprav uporabljata isti nabor znakov.

Za slovence predstavlja problem podobne vrste predstavitev naše abecede z različnimi kodnimi stranmi. Če 1 aplikacija uporablja 7-bitno YU-ASCII, 2 pa 8-bitni standard 852 ali 1250, bo prišlo do napak. Za pravilen izpis znakov ˝č,š,ž˝ moramo zagotoviti konverzijo oddajnikove kodne strani v kodno stran sprejemnika, uporabimo **storitev prevajanja kodnih strani.**

3.Storitev stiskanja podatkov(kompresije)

Se uporabljajo v primerih ko bi bila lahko kapaciteta transportnega sistema lahko prenizka in bi prenos podatkov med dvema aplikacijama lahko trajal predolgo.Storitve kompresije podatkov na oddajnikovi strani podatke komprimira, na sprejemnikovi strani pa jih dekomprimira.

4. Storitve zaščite vsebine podatkov

Storitve, ki omogočajo zaščito podatkov so storitve ENKRIPCIJE in DEKRIPCIJE, te storitve so bistvene za zagotavljanje varnosti poslovanja.

DVOTOČKOVNI PROTOKOL PPP

V začetku je bil namenjen enkapsulaciji IP številk prek dvotočkovnih povezav, danes pa omogoča veliko drugih protokolov kot npr. Novellov IPX, Dellov DEC-net, omogoča upravljanje z IP naslovi, konfiguracijo, testiranje, zaznavanje napak. Najbolj pogosto se uporablja na osebnih računalnikih z modemom. PPP je sestavljen iz HDLC protokola (visokonivojski nadzor podatkovne povezave), LCP protokola (protokola nadzora povezave) in skupine protokolov NCP (omrežni kontrolni protokoli).

HDLC protokol se uporablja za enkapsulacijo datagramov skozi serijske povezave. LCP protokol vzpostavi, nastavi in testira podatkovno povezavo, NCP protokol se uporablja za vzpostavitev in nastavitev enega ali več protokolov na omrežni plasti.

PPP protokol upravlja naprave tipa DCE, DTE (Data Communication Equipment, Data Terminal Equipment). Povezave med temi napravami mora biti dvosmerna (duplex) in mora potekati v sinhronem ali asinhronem načinu.

Shema PPP okvirja:

1 byte	1 byte	1 byte	2 byte	Spremenljivka	2 ali 4 byta
Oznaka začetka	NASLOV	NADZOR	PROTOKOL	PODATKI	FCS(frame check sequence)

HDLC

Visokonivojski nadzor podatkovne strukture (HDLC) je izpeljan iz nadzora sinhrone podatkovne povezave, protokola (SDLC), ki ga je razvil IBM. Iz tistega protokola je nastal standard ISO, imenovan HDLC protokol in kasneje standard IEEE 802.2

Shema HDLC protokola

1 byte	1 ali 2 byta	1 ali 2 byta	2 byta	SPREMENLJIVKA	2 ali 4 byti	1 byte
Oznaka začetka	NASLOV	NADZOR	PROTOKOL	PODATKI	FCS	Oznaka konca

HDLC podpira tri transportne načine:

- navadni odzivni način, kjer sekundarna postaja ne komunicira s primarno, dokler ne dobi dovoljenja
- asinhroni odzivni način
- pri asinhronem uravnoteženem načinu je dano vozlišče lahko primarna ali sekundarna postaja (kombiniran način)

LOGICAL LINK CONTROL

Nadzor logične povezave IEEE 802.2 LLC specifikacije se uporablja v omrežjih IEEE 802.2 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring). LLC omogoča vrsto storitev, imenovanih LLC1, LLC2, LLC3.

- LLC tip 1 je nepovezana storitev brez potrjevanja. Popravljanje napak prepušča protokolom, kot je TCP. Uporablja se zelo pogosto in ponuja dve oblike: DSAP (Destination Service Access Point), SSAP (Source….), kar pomeni ponorno in izvirna storitvena pristopna točka.
- LLC tip 2 je povezana storitev s potrjevanjem: to pomeni, da je med vozliščema vzpostavljena zanesljiva povezava, preden se pošljejo kakršnikoli podatki, ko se podatki pričnejo pošiljati se potrdi vsak bit, če kakšen bit ne prispe, se ponovno pošlje cel okvir. Tak tip povezave se redko uporablja.
- LLC tip 3 je kopromisni tip med 1 in 2, ni povezana storitev, je pa s potrditvijo.

BREZŽIČNA OMREŽJA

Omogočajo dvosmerne ali duplex povezave za prenos glasovne ali podatkovne komunikacije.

RADIJSKE FREKVENCE

So pogoste pri omrežjih, ker potujejo na dolge razdalje in prodirajo skozi stene. Relativno so poceni. Problem radijskih omrežij je v tem, da bosta dve napravi, ki uporabljata isto frekvenco motile druga drugo. Zaradi tega imajo države nadzor nad dodeljevanjem radijskih frekvenc. Določene frekvenčne pasove država licencira najboljšemu ponudniku, ostale pasove pa rezervira za javno uporabo na manjših močeh. Obnašanje radijskih valov je odvisno od frekvence. Nižje frekvence lažje prodirajo skozi fizične ovire, imajo pa manjšo pasovno širino. Višje frekvence prodirajo premočrtno in se odbijajo od ovir. Dosegajo pa večje razdalje z manjšimi močmi.

PASOVI RADIJSKIH FREKVENC
- VLF (zelo nizka) – 3 kHz – 30 kHz
- LF (nizka frekvenca) – 300 kHz – 3 Mhz
- HF (visoka) – 30 Mhz – 300 Mhz
- UHF (zelo visoke frekvence) – 300 MHz – 3 GHz

MIKROVALOVNE FREKVENCE

Mikrovalovi so skupina radijskih frekvenc, ki se začne pri 1 GHz, konča pa se pri 18 GHz. Pasovi pri 18 GHz se imenujejo milimetrski pasovi: oznaka mikrovalovnih frekvenc so povezane z oznakami v tabeli:

L – pas – 1 GHz
S – pas – 2 GHz
C – pas – 4-8 GHz
X – pas – 8-12 GHz
Kn – pas – 12-18 Ghz

Frekvenčni pas za javno rabo:
2.4 GHz – 2.484 GHz ….. IEEE 802.11b (2.4 GHz)

POIMENOVANJE IN NASLAVLJANJE

Je način, kako množico uporabnikov v sistemu razlikujemo (primer: telefonsko omrežje)

HIERARHIČNO POIMENOVANJE

SLO – NM – KRKA – WEB 01 // WEB01.NM.SI
PL – KR- KRKA – WEB 02 // WEB02.KR.PL

S pomočjo tabele vozlišč, ki se vzpostavi v vozliščih, podatek vidi tabele drugih vozlišč.

Gateway – prepakira podatke iz enega protokola v drugega in tam ponovno prepakira

Tabele sosedov so statične.

Večina omrežij se nanaša na določeno shemo naslavljanja, ki enovito poimenuje vsako od komunicirajočih entitet. Imenovalni sistem je namenjen človeški interakciji z omrežjem. Numerične naslavljalne sheme pa uporabljajo različne naprave v omrežju za komuniciranje druge z drugo. Pri ustvarjanju naslovov za sisteme je treba:

- Zagotoviti edinstven naslov
- Programska naslavljalna shema mora biti neodvisna ali hierarhičen oštevilčevalni sistem. Pri enoličnem naslavljevalnem sistemu vsaka naprava ima svojo edinstveno številko in vzdržuje tabelo, ki vsebuje pot in razdaljo ali skokov in časov potrebnih do vsake druge naprave v sistemu. Problem pri taki imenovalni strukturi je, da se pri dodajanju novih naprav velikost usmerjevalnih tabel zelo poveča in postane neobvladljiva (problem je tudi preimenovanje posamezne naprave).

Da bi ublažili takšne težave, se uporabljajo hierarhične oštevilčevalne sheme. Hierarhični oštevilčevalni shemi se ustvarijo segmenti omrežja po istem tipu skupne meje, določene geografsko ali prostorsko. V takem načinu združitve vsak segment vsebuje tabelo poti do drugih segmentov. Naprave v vsakem segmentu morajo poznati samo sistem v njihovi skupini (gruči), ki pošilja sporočila drugim omrežjem.

Bridge – segmentira del omrežja in hrani tabelo povezovanja

Taka vrsta konfiguracije se uporablja v večini omrežij. Naprava, ki v nekem segmentu skrbi za usmerjanje podatkov se imenuje mejni usmerjevalnik ali Border Router, ker s obnaša kot vstopna točka ali mejna kontrola v ali izven mejnega segmenta. Teki mejni usmerjevalniki se imenujejo tudi prehodi ali Gatewayi. Kadarkoli naprava želi poslati sporočilo nekemu drugemu sistemu izven svojega segmenta, pošlje sporočilo mejnemu usmerjevalniku, ki potem pošlje sporočilo na ciljno omrežje ali pot.

Z uporabo hierarhičnega načrta v kombinaciji z mejnimi usmerjevalniki in prehodi more mejni usmerjevalnik vzdrževati samo tabelo drugih sistemov, okolju, ni mu pa potrebno oštevilčevati si vseh naprav v vsakem omreženem segmentu. Taka shema bistveno zmanjša velikost tabel, ki se lažje nadzorujejo in spreminjajo, hkrati pa je prenos sporočil med omrežji manj učinkovit. Vendar se to nadomesti v bolj enostavnem usmerjanju.

Metoda uporabe enotne številke, ki predstavlja skupek naprav, se imenujejo KOPIČENJE (aggregation). Ta metoda se ne obnese v primeru strojnih naslovov omrežnih kartic. Naslavljalni sistem, ki ga uporabljajo Ethernet kartice je tak, da ima vsaka kartica unikaten fizični 48-bitni (6 bajtov) naslov. Vsak proizvajalec ima svojo kodo MAC (Media Access Code), kar lahko razumemo kot naslov za dostop do medija.

Organizacija IEEE nadzoruje dodeljevanje ponudniških šifer. Prve 3 bajte strojnega naslova je proizvajalčeva številka, zadnje 3 bajte določi proizvajalec za vsak adapter unikatno. V omrežju, ki vsebuje omrežne kartice različnih proizvajalcev ne obstaja del naslova, ki bi bil skupen vsem napravam. Glavni razlog, zakaj se MAC naslovi ne uporabljajo v usmerjevalnih tabelah, je povezan z obsežnostjo takih tabel.

INTERNET

Numerični naslovi, uporabljeni pri internetnem protokolu IP v internetnem omrežju, so uporabljeni pri vsakem omrežnem vnosniku, ki komunicira v omrežju. (vsaka internetna kartica mora imeti svojo IP številko, če želi komunicirati v omrežju). Obstajata dve obliki IP naslovov, ki se uporabljata v omrežjih, IPv4 in IPv6.