Primjena sigurnosne politike

Autor: Aco Dmitrović
Recenzija: Dinko Korunić
siječanj 2004.

srce

Prije svega

- Nužno je imati sigurnosnu politiku
  - Prilagođenu, službeno usvojenu, objavljenu
  - Zaposleni potpisom potvrđuju da su upoznati
  - Studenti pri otvaranju korisničkog računa
- Pravila koja vrijede za sve korisnike
- Pravila za zaposlene, ali i honorarce
- Pravila administriranja i korištenja računala

Pravila za korisnike

- Politika prihvatljivog korištenja
- Javni dokument
  - Objaviti ga na web stranicama
  - Link sa naslovnice
- Vrijedi za sve koji koriste informacijske sustave

Pravila prihvatljivog korištenja

- Treba poštovati
  - Zakone
    - Na pr. autorska prava!
  - Druge korisnike
    - Bez vrijeđanja i omalovažavanja
    - Bez uzurpiranja resursa
  - Bez preuzimanja tuđeg identiteta
  - Bez ispitivanja ranjivosti, skeniranja mreže, provaljivanja

Pravila za zaposlenike

- Za zaposlene
  - Prihvatljivo korištenje
  - E-mail
  - Password policy
  - Rukovanje povjerljivim podacima
- Glavni korisnik
  - Odgovoran za aplikaciju i podatke

Pravila za informatičare

- Administriranje računala
  - Posebna grupa zaposlenih

- Upravljanje mrežom
- Pravila administriranja računala
- Pravila za nadzor
- Intervencije i postupak ponašanja pri incidentima

Upravljanje sigurnošću

- Voditelj sigurnosti informacijskih sustava
  - Dvostruki talent
    - Dobar u struci
    - Komunikator, organizator
  - Piše politike, organizira provođenje i nadzor
- Povjerenstvo za sigurnost
  - Predstavnici uprave i informatičara
  - Podržava inicijative voditelja
  - Odobrava trošak

Fizička sigurnost

- Javne zone
- Samo za zaposlene
- Samo za grupe zaposlenih

- Provjera na liniji razdvajanja

- Prostorije za kritičnu računalnu opremu
  - nadzor, fizička zaštita

Administriranje

- Svako računalo mora imati administratora
  - Korisnik
  - Profesionalac
  - Administratori pojedinih servisa
  - Demonstratori za učione
- Ustanova održava ažurnu listu računala i njihovih administratora

Sigurnosni minimum - poslužitelji

- Redovno instaliranje zakrpa
- Obavezna protuvirusna zaštita
  - Centralna instalacija + neprestana dogradnja
- Ugasiti nepotrebne servise
- Liste pristupa
  - Na razini individualnih servisa
  - Cjelokupnog računala
- Firewall, IDS

Sigurnosni minimum - osobna računala

- Redovno instaliranje zakrpa
- Ne smiju se instalirati javni servisi
  - Web stranice na poslužitelju
  - Nikakav proxy!
  - P2P
- Protuvirusna zaštita
  - Automatska dogradnja
- Licenciran software

Incidenti

- Korisnici imaju obavezu prijave incidenta
- Moraju znati kome ga prijaviti
  - Kontakt lista (osoba, tel., e-mail…)
  - Najbolje jedna kontakt adresa, *helpdesk*
    - Dežurni preusmjerava problem specijalistima
- Obrazac za prijavu incidenta?

Nadzor

- Tko ima pravo nadzora?
  - Specijalist/tim
- Povremene provjere
  - Najavljeno
  - Nenajavljeno?
- Otkrivanje neprihvatljivog korištenja
  - Korisnika iznutra
  - Napada izvana

Nadzor…

- Kolike su ovlasti osobe koja provodi nadzor?
  - Hoće li samo prijaviti incident ili ima pravo poduzeti akcije?
  - Na pr. zatvaranje korisničkog računa
  - Mogućnost zabune
    - username ne mora biti sam korisnik, račun može biti provaljen
    - Obavezan razgovor s korisnikom i provjera dokaza

Istraga

- Formirati ERT *(Emergency Response Team)*
- Forenzička obuka
  - Ili zatražiti pomoć od CARNeta
- Definirati procedure za istragu:
  - Jedan provodi istragu, ali uz svjedoka
  - Bilježenje svih radnji
- Zapisnik je povjerljiv dokument

Sankcije

- Definirati kazne za nepridržavanje pravila sigurnosne politike
- Vezati ih na lokalne zakone i propise
  - Stegovni postupak
  - Premještaj na drugo radno mjesto
  - Otkaz?
  - Zakon o radnim odnosima
- Od zaposlenika se traži da potpišu izjavu da su upoznati s politikom

Primjena politike

Prvi koraci

Primjena politike…

- Tek kada je politika donesena, imamo pokriće za akcije, promjene
- Prije svega treba napraviti inventuru
  - Da bismo znali čime raspolažemo
- Raspodjela računala u grupe
  - Segmentiranje mreže

Inventura mreže

- Nacrt mreže
  - Popis svih priključaka
  - Numeriranje
- Što je priključeno na pojedine utičnice?
  - U svakom trenutku morali bi znati odgovor
  - Mrežni parametri napisani na računalima?

Inventura računala

- Inventura računalne opreme
  - Poslužitelja
  - Korisničkih računala
  - Dodatni U/I uređaji (štampači, skeneri, modemi…)
- Hardware, adrese (IP, MAC, FQDN)
  - Servisi
  - Administratori
    - OS-a, rezervni admin
    - Servisa i aplikacija

Inventura softvera

- Popis instaliranog softvera
- Licenciranje

- Pravila za instaliranje:
  - Tko smije instalirati programe?
  - Tko odgovara za licenciranje?
  - Obrasci: zahtjev za instalaciju
  - Tko ima pravo nadzora?

Grupiranje poslužitelja

- Izdvajanje kritičnih računala
  - Sadrže povjerljive podatke (Xice, računovodstvo..)
  - Obavljaju javne funkcije (web poslužitelj, mail poslužitelj, DNS…)
- Definiranje sigurnih zona
  - Ograničen pristup
  - Porta: tko može dobiti pojedini ključ
    - Evidencija izdavanja ključeva/pristupa prostorijama

Grupiranje osobnih računala

- Grupiranje korisnika
- Zaposleni
  - Referada
  - Računovodstvo
  - Profesorski kabineti..
- Studenti
  - Računalne učione
  - Računala bez nadzora (hodnici, predvorja…)
  - Prenosiva računala

Grupiranje osobnih računala…

- Gosti i suradnici
  - Računala bez nadzora (hodnici, predvorja…)
  - Prenosiva računala
  - Bežični i hibridni uređaji
  - Antivirusna zaštita?

- Zaseban segment mreže
  - Ograničen pristup važnim računalima

Gostujuća računala

- Da li je dozvoljeno priključivanje u mrežu
  - Notebooka
  - Bežičnih uređaja
  - Kome?
    - Zaposleni
    - Studenti
  - Pod kojim uvjetima
    - Bez prijave, s prijavom (obrazac, MAC adresa)
  - Tehnički standardi (odvojen VLAN, DHCP, autorizacija…)

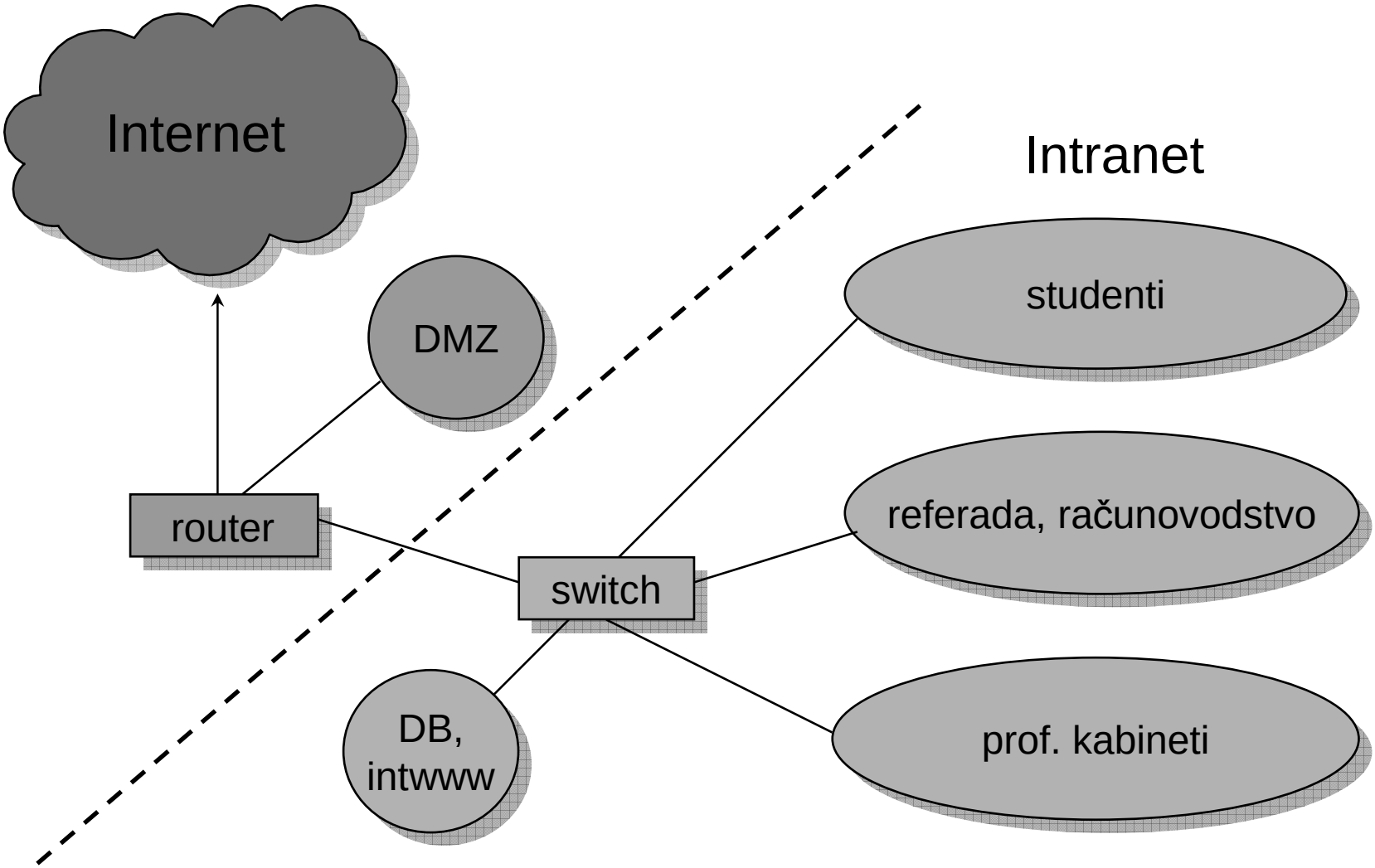
Demilitarizirana zona

- Ničija zemlja
  - Na pr. pojas između Sjeverne i Južne Koreje ☺
- Izvan zaštićene mreže
- Dostupna s Interneta
  - Štićena zona, ali izložena “neprijatelju”
  - Dozvoljen promet samo prema određenim servisima, nikad "svima sve"
- Zona javnih servisa

Zaštićena mreža

- Intranet
- Interni poslužitelji
  - Za cijelu ustanovu
  - Za pojedine odjele
- Korisnička računala
  - Razdvojena po grupama

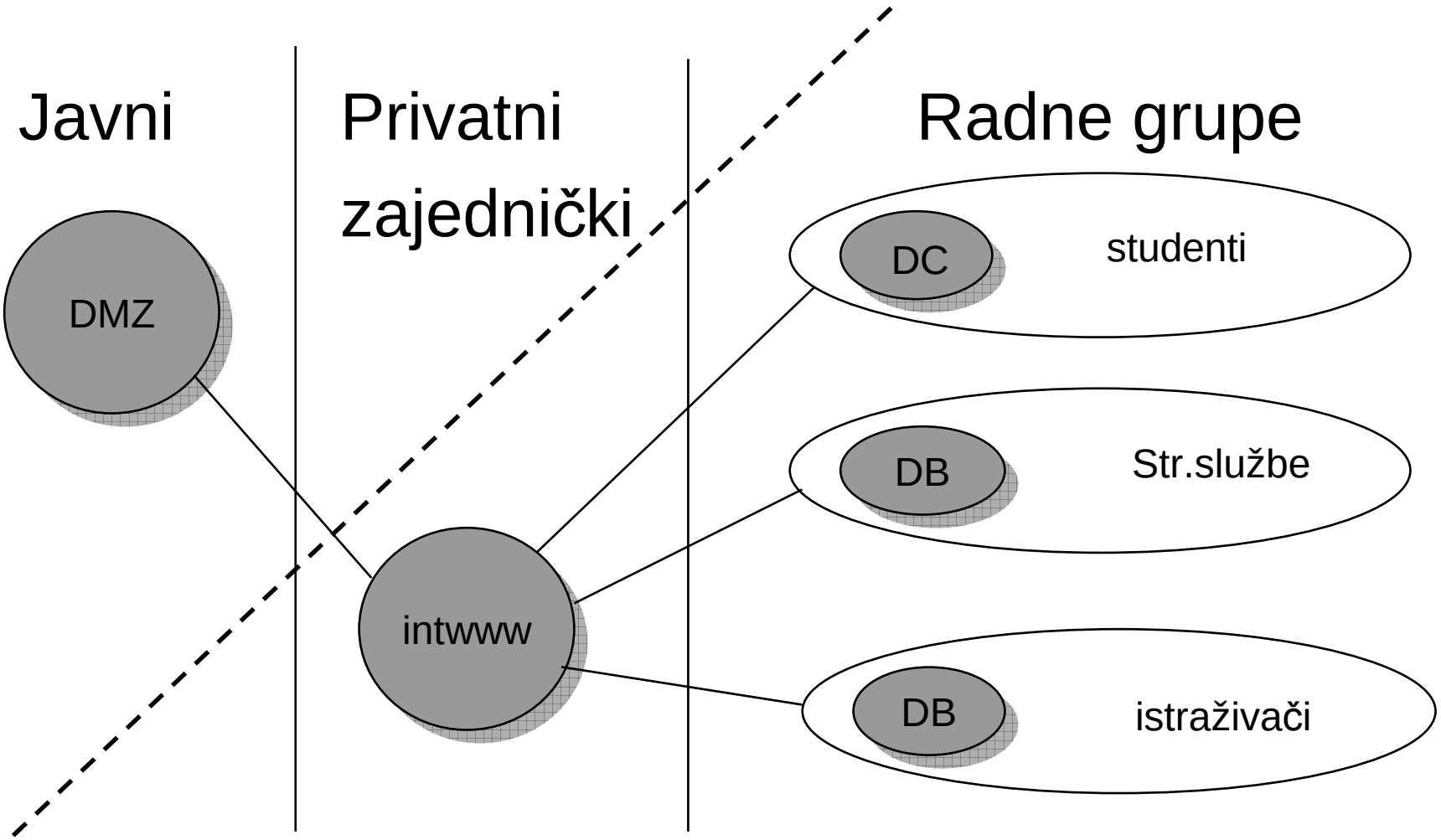
Podjela na sigurnosne zone



Extranet

- Prolaz u Intranet
  - Samo za povlaštene korisnike
  - Spaja udaljene lokacije (Intranete)
  - Interni modemski ulazi
    - Vanjski ulazi + VPN?
  - Partnerske tvrtke, prema ugovoru
    - Npr. SRCE, Xice, ISVU
    - Web dizajneri
    - Proizvođači softvera (dogradnja database aplikacije…)
    - Ugovorom ih obavezati na poštivanje politike

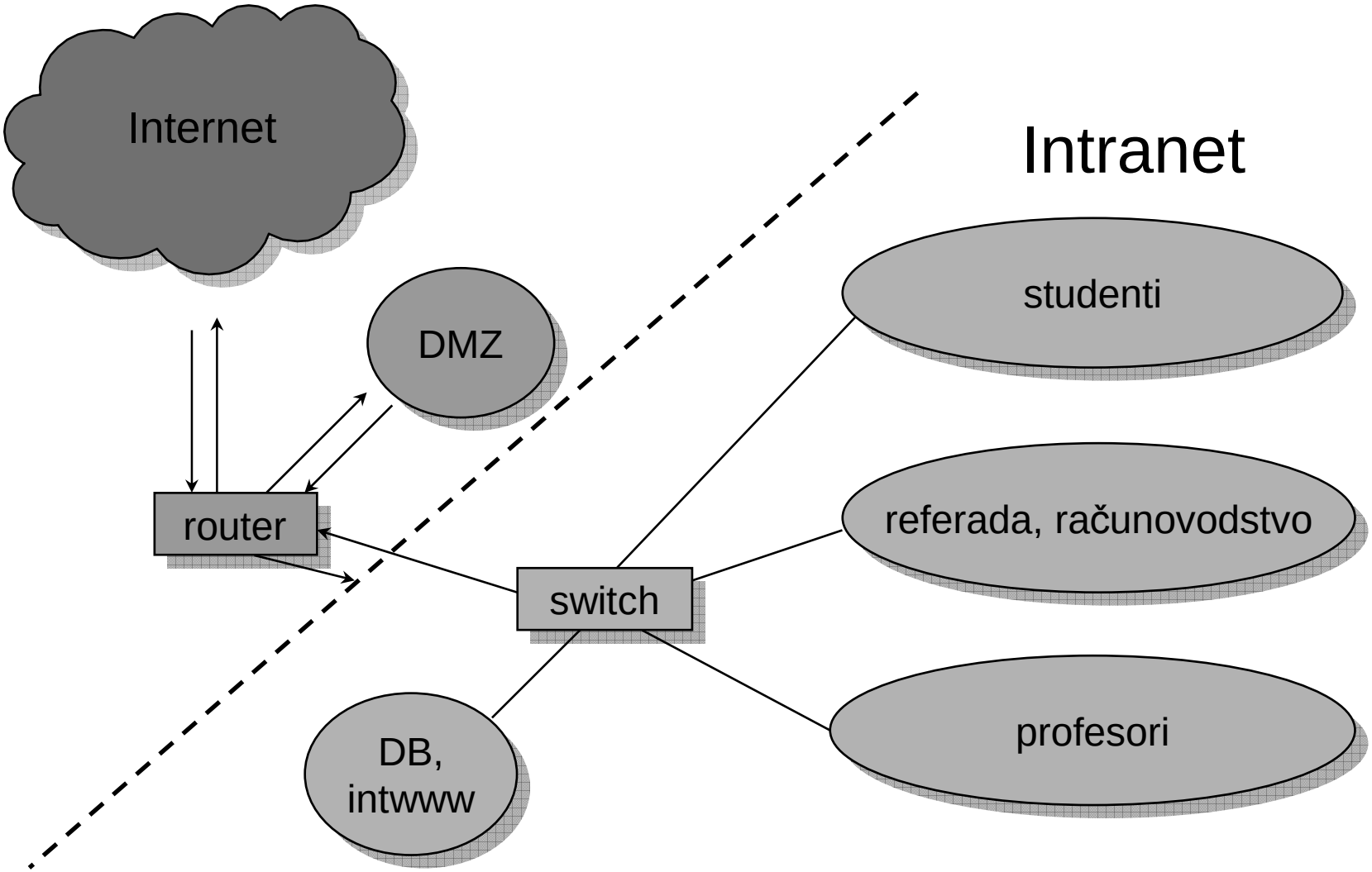
Smještaj poslužitelja



Osobna računala

- Bez javnih servisa!
- Kako to provesti?
  - Na liniji razdvajanja blokirati ulazne SYN pakete
    - Što s UDP, ICMP paketima?
  - SMB
    - Blokirati portove (135-139,445…)
  - Firewall
    - Puštati pakete samo ako su dio već uspostavljene konekcije, inicirane iznutra
    - Ključna riječ: stateful analiza - established veze
  - NAT!!!

Blokiran promet izvana



Spoofing

- Općenito:
  - Pokušaj neautoriziranog entiteta da dobije autoriziran pristup sustavu pretvarajući se da je autoriziran korisnik
- IP Spoofing
  - Napadač izvan naše mreže pretvara se da je legalan i autoriziran korisnik
    - Koristeći IP adresu koja pripada našoj mreži
    - Koristeći IP adresu koja pripada povjerljivom partneru koji ima osiguran legalan pristup resursima

Anti-spoofing pravila

- Pravila:
  - Izvana ne može ući paket s izvornom adresom našeg LAN-a
  - Iznutra ne smije izaći paket kojem izvorna adresa nije iz našeg LAN-a
- U oba smjera blokiraju se adrese:
  - Privatne: 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16
  - Lokalne: 127.0.0.1/8
  - Provjera SA (izvorišne adrese) - RP filter

Anti spoofing na routeru

- Izvana blokiraj privatne adrese i adrese iz LAN-a
- LAN: 161.53.x.0/24, interface serial 0

```
access list IN ...
deny   ip 10.0.0.0 0.255.255.255 161.53.x.0 0.0.0.255
deny   ip 172.16.0.0 0.15.255.255 161.53.x.0 0.0.0.255
deny   ip 192.168.0.0 0.0.255.255 161.53.x.0 0.0.0.255
deny   ip 127.0.0.0 0.255.255.255 161.53.x.0 0.0.0.255
deny   ip 161.53.x.0 0.0.0.255 161.53.x.0 0.0.0.255
permit ip any any
```

Anti spoofing na routeru…

- Na izlazu iz LAN-a, dozvoli samo izvorišne adrese koje pripadaju LAN-u
- Interface ethernet 1

```
access list OUT ...
permit ip 161.53.x.0 0.0.0.255 any
deny   ip any any log
```

Anti spoofing na Linuxu

- LAN: 192.168.33.0/24 na eth0
- WAN: 161.53.x.3/32 na eth1
- Omogući SYN kolačiće i SA provjeru:

sysctl -w net.ipv4.conf.all.rp_filter=1

sysctl -w net.ipv4.tcp_syncookies=1

- Blokiraj privatne adrese koje dolaze izvana

iptables -i eth1 -s 10.0.0.0/8 -j DROP

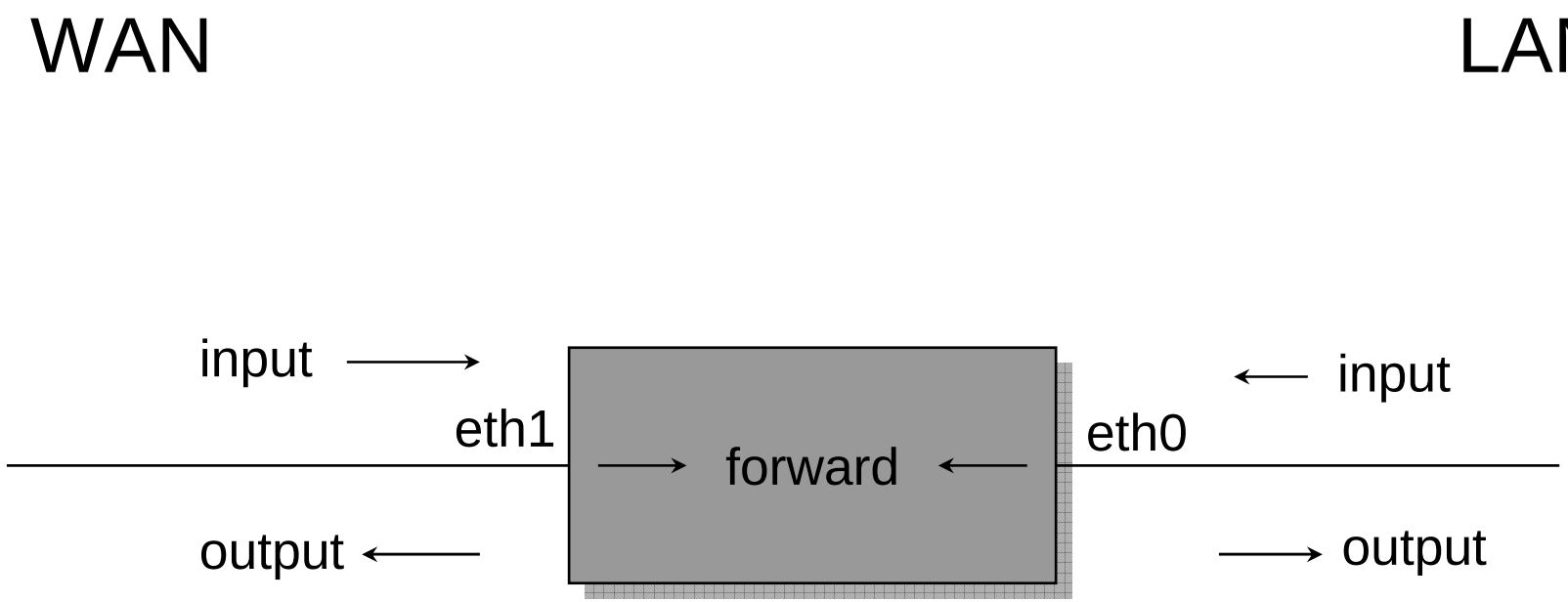
iptables -i eth1 -s 172.16.0.0/12 -j DROP

iptables -i eth1 -s 192.168.0.0/12 -j DROP

- Iznutra puštaj samo samo adrese iz LAN-a

iptables -i eth0 **!** -s 192.168.x.0/24 -j DROP

Smjer kretanja paketa



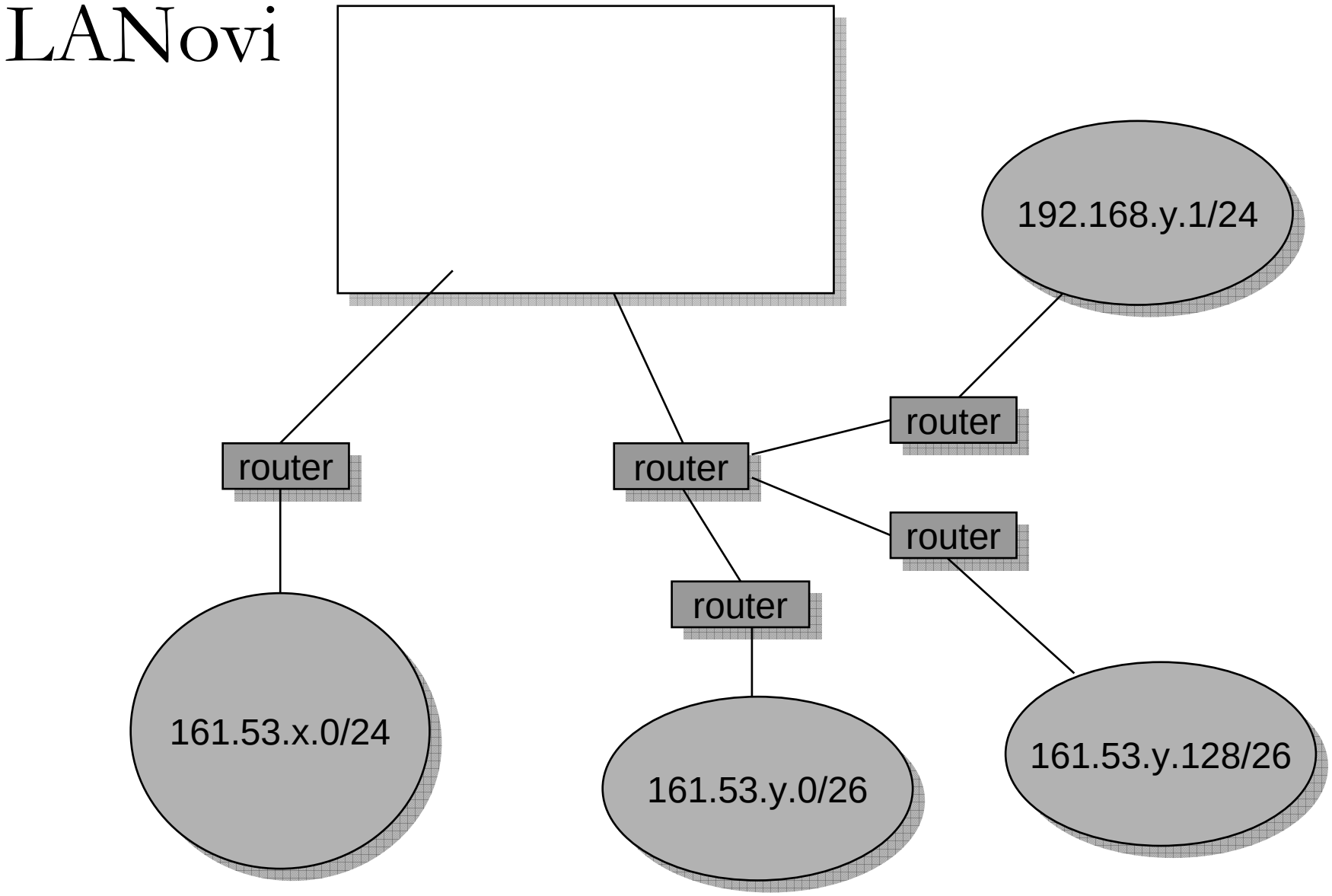
Kako grupirati računala?

- VLAN
- Multihomed host
- Firewall

LAN

- Klasični LAN-ovi su fizički odijeljene mreže, povezane routerima
- LAN je *broadcast* domena
  - *Collision domain*
- Adrese unutar klase ili segmenta klase
- Treća OSI razina
- Router dodaje latenciju, kašnjenje paketa

LANovi


192.168.y.1/24
router
router
router
router
router
161.53.x.0/24
161.53.y.0/26
161.53.y.128/26

Segmentiranje

- IP adresa: 32 bita, 4 bajta
- 161.53.53.3 ili binarno:
- 10100001.00110101.00110101.00000011
- 161.53.x.0/24 ili
- network 161.53.x.0 netmask 255.255.255.0
- /24 znači:
  - Prva 24 bita su adresa mreže
  - Ostalih 8 adrese hostova

C klasa

- 161.53.53.0/24

10100001.00110101.00110101.00000011

-------- -------- --------|

network

----

host

- 8 bitova za računala
- $2^8 = 256 – 2 = 254$

Dva segmenta

- 161.53.53.0/26 (dva segmenta)

10100001.00110101.00110101.00000011

-------- -------- -------- --

network

------

host

- dva subneta = 2 bita (1 bit + 1 rezerviran)
- 6 bitova za računala ($2^6 – 2 = 62$ računala)

Segmenti

- samo 2 subneta od teoretski mogućih 4
- gubi se jedan bit:
  - ne koriste se gornji /26 i donji /26 segment

- standardna IP routing pravila:
  - ne smije se koristiti subnetove sa svim 0 ili 1 u mrežnom dijelu!
  - najnovija oprema omogućuje da koristimo sve!

Prva podmreža

- Subnet:
  - CIDR zapis: 161.53.53.64/26
  - network: 161.53.53.64
  - netmask: 255.255.255.192 = 26
  - broadcast: 161.53.53.127
  - broj računala: 62
  - iskoristive adrese: 161.53.53.65 - 161.53.53.126

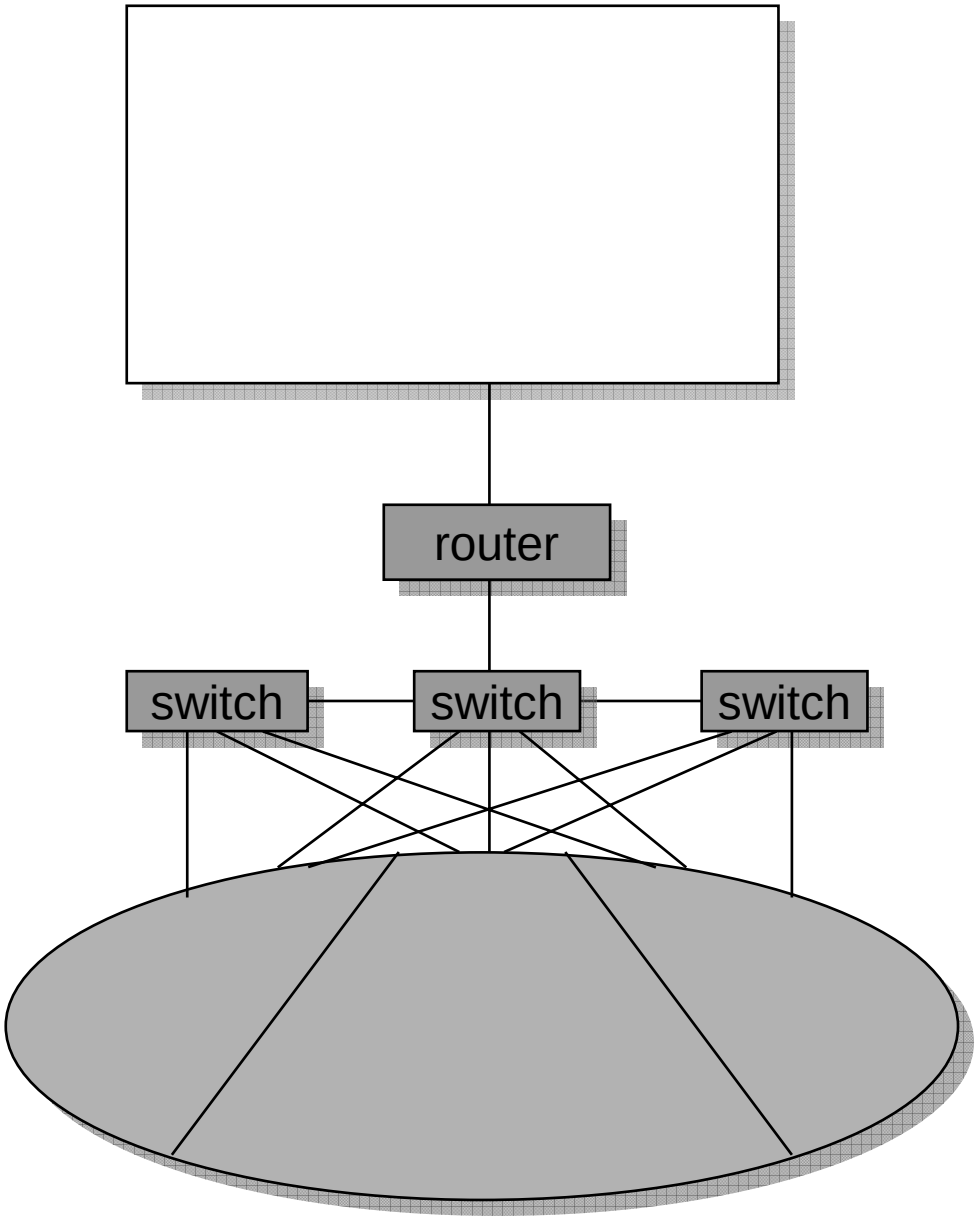
Druga podmreža

- Subnet:
  - CIDR zapis: 161.53.53.128/26
  - network: 161.53.53.128
  - netmask: 255.255.255.192 = 26
  - broadcast: 161.53.53.191
  - broj računala: 62
  - iskoristive adrese: 161.53.53.129 - 161.53.53.190

VLAN

- Virtualni LAN
- Logički odvojeni LAN-ovi na preklopniku *(switchu)*
- Svaki port dodijeljen je nekom VLAN-u
- Druga razina OSI modela
  - MAC adrese ethernet kartica

VLAN



Prednosti

- IP adrese postaju nebitne
- Ne mora se segmentirati klasa adresa
  - Ne gube se IP adrese
- Olakšano administriranje mreže
  - Preseljenje računala u druge prostorije
  - Prebacivanje računala u drugi VLAN
- Smanjuje se *broadcast* domena bez povećanja latencije
- Cijena: preklopnik je jeftiniji

VLAN tagging

- Tag – oznaka, etiketa
  - VLAN tag u Ethernet frame
  - Standard 802.1q
    - Cisco je ranije koristio vlastiti standard
      - Cisco ISL *(Inter Switch Linking)*
    - Nova Cisco oprema podržava oba, ili samo 802.1q
  - Linux ga podržava

VLAN trunking

- Da bi proširili VLAN preko više preklopnika *(switcheva)*
- Port na preklopniku pretvorimo u trunking port i dodjelimo mu VLANove
- Povežemo preklopnike preko trunking portova
- Ethernet frame se enkapsulira u trunking protokol

Promet između VLANova

- Paketi ne prolaze u susjedne VLANove
- Ponekad moramo propustiti određen promet
  - Na pr. do zajedničkog poslužitelja
- trebamo uređaj treće OSI razine
  - *router* je član svih domena
  - *Access* liste određuju koji promet puštamo
  - Layer 3 switch

Literatura o VLAN-u

- University of California, Davis, Projekt novog LAN-a

http://net21.ucdavis.edu/newvlan.htm

- Standard 802.1q, PDF dokument, 211 str.

http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf

- Implementacija na Linuxu

http://www.candelatech.com/~greear/vlan.html

Napravite plan

- Plan koji će dugo izdržati bez promjena
  - Koliko VLAN-ova?
  - Koliko portova na *switchu* po VLAN-u?
- Zahtjev NOC-u na Srcu
- Dogovor oko termina
  - Dan D
  - Prespajanje patch kablova na switchu
  - Promjena IP adresa na računalima
    - Na pr. ako prelazimo na NAT

Problemi s VLAN-om

- SANS otkriva ranjivosti u implementaciji VLAN-a
- Moguć neželjen prolaz paketa između VLAN-ova
  - napad koristeći umjetne VLAN tagove i sl.

- http://www.sans.org/resources/idfaq/vlan.php

Dual homed host

- Linux na računalu s dvije ethernet kartice
  - Ili više!
  - Vanjska adresa – javna
  - Unutarnja adresa – privatna
- NAT (Network Address Translation)
  - Dinamički – *masquerade*
  - SNAT, DNAT - precizniji, kompliciraniji

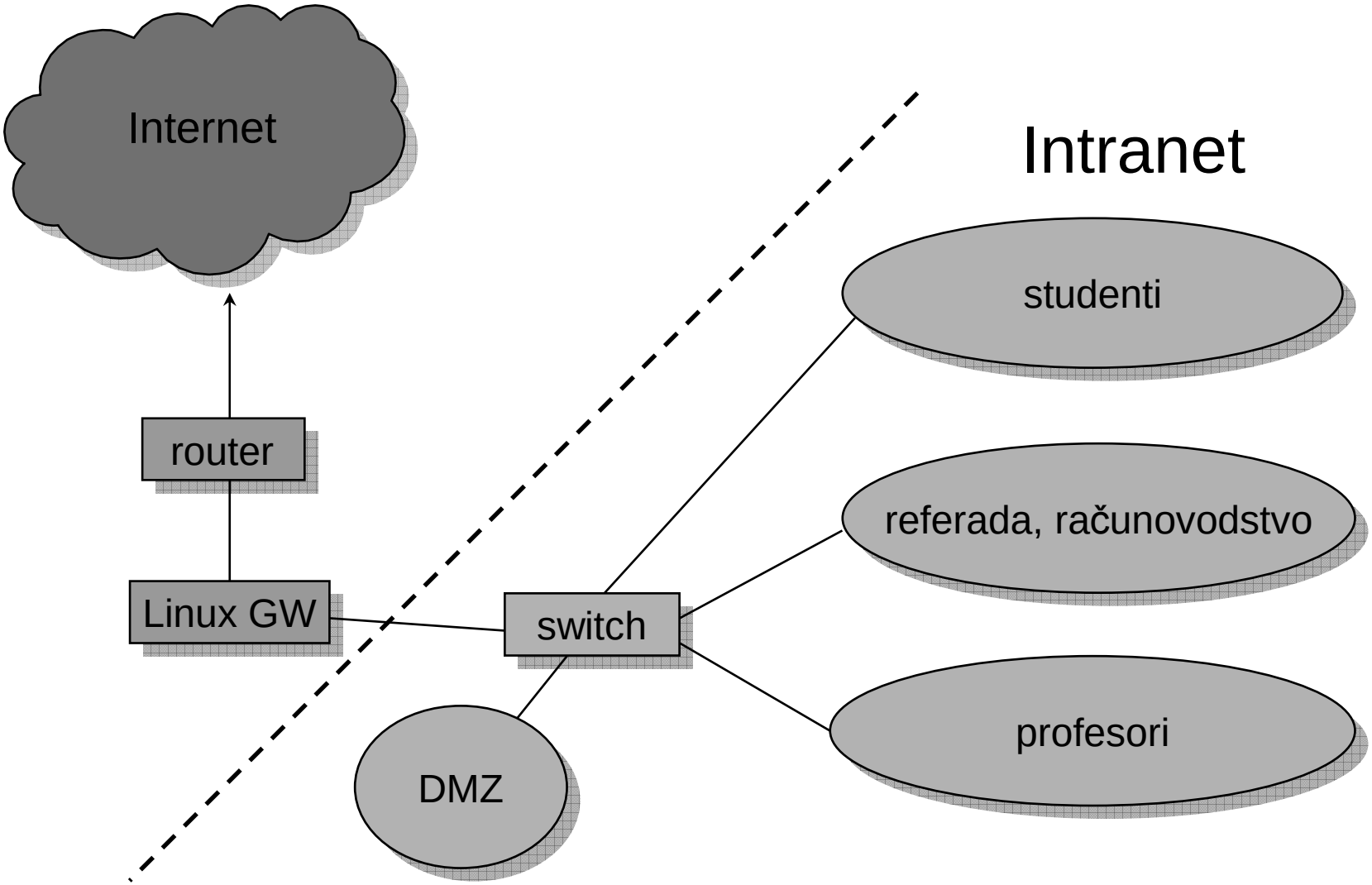
NAT na Linuxu

```
# ukljuciti forwarding
sysctl -w net/ipv4/ip_forward=1

# forwarding i NAT
iptables -t nat -A POSTROUTING -o $INET_IFACE -j SNAT -to-source
    $INET_IP

# maskerada (dobro je dodati i -s ili -i, mozda ne
# zelite sve maskirati)
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

DMZ u LAN-u

- Javne poslužitelje možemo staviti iza firewalla, na privatne adrese
- DNS-u ih prijavimo na javnoj adresi firewalla
- Firewall radi redirekciju prometa
  - Promet na port koji pripada servisu preusmjerava na isti taj port poslužitelja na privatnoj adresi
  - Izbjegava se direktna komunikacija
  - Omogućava se pregled paketa i njihovo testiranje ispravnosti!

Zaštićen DMZ



DNAT i port forwarding

- Web poslužitelj skriven na privatnoj adresi
- Istovremeno dostupan izvana, na jednom portu

```
iptables -t nat -A PREROUTING -p tcp -d 161.53.x.3 \ --dport 80 -j
    DNAT --to $INT_SRV:80
```

- Isto je moguće i za ostale servise

Linux vatrozid

- Specijalizirane distribucije
  - Guarddog
  - Mason
  - SINUS Firewall
  - SmoothWall
  - Firestarter

- Ili uradi sam:
  - netfilter!

Kakav HW?

- Firewall: kao router, ali mnogo više posla!
- Kritični resursi
  - Brza sabirnica
  - CPU (UP, SMP sustavi)
  - Ethernet
    - Dobar driver za Linux
    - Primjer: e100, e1000 - NAPI, device polling
    - Tehnologije otpornosti na SYN i sl. napade

Propusnost sabirnice

- Frekvencija * br.bitova
- PCI
  - 33 MHz x 32 bita = 1Gb
    - Propusnost dijele priključeni uređaji
  - 66 MHz
- PCI-X
  - 66, 133, 266, 533 MHz

FYI

- PCI-X site

http://www.pcisig.com/specifications/pcix_20

- Ethernet kartica sa 4 porta

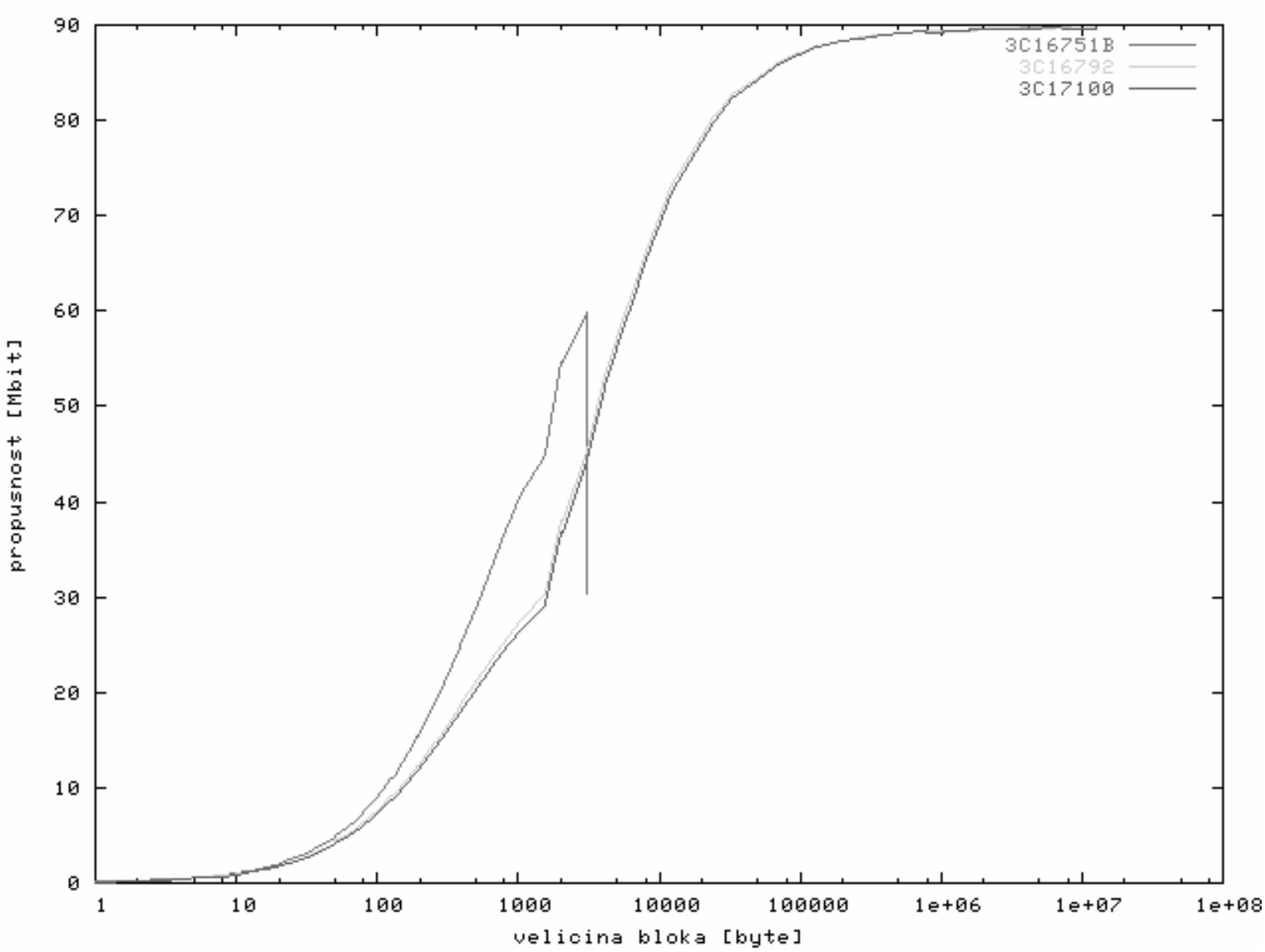
http://www.intel.com/network/connectivity/products/pro1000mt_quad_server_adapter.htm

Praktična mjerenja

- HP ProLiant DS 380 G3
- 2 x PCI-X Gigabit NIC
- Test tvrtke StoneSoft
  - StoneGate FW
  - 18.12.2002.

- Propusnost obrnuto proporcionalna veličini paketa

Frame size	Packets/ sec	Bandwidth Mbps
64	111608	57,14
128	109650	112,28
256	122550	250,98
512	129132	528,92
768	129668	796,68
1024	113636	930,91
1280	109650	1123,82
1518	110718	1344,56


3C16751B
3C16792
3C17100
propusnost [Mbit]
velicina bloka [byte]
0
10
20
30
40
50
60
70
80
90
1
10
100
1000
10000
100000
1e+06
1e+07
1e+08

Nadzor

- Kako osigurati nadzor?

- IDS *(Intrusion Detection System)*
  - Prepoznavanje uzoraka
  - Statistički IDS (npr. Snort + ACID)

- NIDS – mrežni IDS
- Host based

- Gdje postaviti IDS?
- Koji softver koristiti?

- CARNetovi projekti
  - Snort centrala
  - ARMS

- Više o tome na narednom tečaju!

Neprekinutost poslovanja

- Unaprijed predvidjeti kvarove na poslužitelju
  - Dvije identične ethernet kartice u poslužitelju
    - Obje konfigurirane, jedna aktivna
  - Dva napajanja
    - Odvojeni "pametni" UPS-ovi, napajanje iz različitih mreža
  - RAID
    - OS barem na RAID 1
    - Podaci nužno na RAID 5
  - Backup

Zaštitne kopije

- Backup
  - Tjedni, mjesečni
    - koliko se dugo čuva?
  - Dnevni inkrementalni
  - Softver
    - Amanda, Taper, itd.
  - Automatski backup važnih podataka
  - Obučiti korisnike da sami rade kopije svojih podataka

Vježbe

- Moguće je imati *backup*, ali nemati *restore*!
- Povremeno treba isprobati ispravnost traka

- Organizirati vježbu
  - Ne na produkcijskim računalima!
  - Simulacija kvara, reinstalacije i vraćanja podataka

Ponavljanje

- It’s deja vu all over again

  -- Yogi Berra
- Primjena sigurnosne politike na malo drugačiji način
- Američka škola mišljenja
  - pragmatizam
- Zaštita i povećanje profita kao najvažniji motivi za bavljenje sigurnošću

Upravljanje sigurnošću

- Savjeti časopisa Tech Republic
  - www.techrepublic.com
- Za komercijalno okruženje
  - Korisni savjeti i za našu akademsku sredinu
- Za plavuše:
  - Šest jednostavnih koraka ☺

Šest lakih komada

- Odredi i vrednuj informacijsku imovinu
- Procjena rizika
- Odredi procedure

  (Define Security Practices)
- Primjena pravila
- Nadzor, reakcija na povredu pravila
- Preispitivanje

Odredi i vrednuj imovinu

- Tri vrste imovine
  - Fizička
    - računala, programi, zgrade, sefovi…
    - Odredi razine sigurnosti:
      - Na pr. javno, povjerljivo, ograničen pristup
  - Informacije
  - Ljudi
    - pojedinci koji obavljaju ključne poslove
    - čije bi se odsustvo odrazilo na obavljanje posla

Procjena rizika

- Pažljivo procijenite koliko sigurnosti trebate
  - Premalo: sustav će biti lako kompromitirati, namjerno ili nenamjerno
  - Previše: teško za korištenje, pad performansi
  - Sigurnost je obrnuto proporcionalna upotrebljivosti !
    - Ako želite 100% sigurnosti: zabranite korištenje!
  - Prihvatljivi rizici
    - Mala vrijednost imovine
    - Mala vjerojatnost kompromitiranja
  - Neprihvatljivi rizici
    - Ulaganje prilagoditi vrijednosti imovine

Define Security Practices

- Pravila za određivanje sigurnosnog rizika
- Pravila za određivanje prihvatljivosti rizika
- Vlasništvo imovine (dodjela odgovornosti)
- Politika – nepridržavanje
- Kako se prijavljuju incidenti
- Edukacija
- Sigurnosni nadzor: nenajavljene provjere

Implement Security Practices

- Očekujte otpor!
- Primjena po fazama
  - Po odjelima
  - Prema poslovnoj aktivnosti
  - Po lokacijama
  - Prema ulogama
    - odozgo prema dolje (vlastitim primjerom)

Nadzor i sankcije

- Provjeravati ponašanje
  - Bez nadzora - prekršaji postaju češći i ozbiljniji
  - Stiču se loše navike
- Treba nedvosmisleno znati:
  - Tko može pristupati i rukovati imovinom
  - Kako se obavlja autentikacija
  - Kako se ograničava pristup

Nadzor…

- Tko ima pravo nadzirati sustave?
- Tko je pokušao učiniti nešto izvan pravila prihvatljivog korištenja?
- Izvještaji za upravu
- Smisao:
  - Sticanje dobrih navika
  - Sprečavanje većih incidenata

Revizija

- Imovine i rizika
- Procedura i pravila

- Poticaji:
  - Incidenti su prečesti
  - Tvrtka se restrukturira
  - Mijenja se poslovno okruženje
  - Mijenja se tehnologija
  - Smanjuje se proračun ☹

Na kraju

Malo zdravog razuma…

Yogi Berra

- The future ain't what it used to be.

Savjet

- Politika ne treba služiti za proganjanje i sputavanje ljudi
- Srednji put
- Vlast poštuje kreativnost i slobodu pojedinca
- Ali mu brani da naškodi drugima

Savjet…

- Ne treba zaboraviti zašto Mreža postoji u sveučilišnoj sredini

- Radi podučavanja, istraživanja
- Radi učenja
  - Individualnog napretka, samorazvoja

Savjeti…

- Sigurnost više ovisi o ljudima nego o tehnologiji
- Politika treba imati odgojnu, usmjeravajuću ulogu
- Sankcije čuvajte za nepopravljive
- Stvarajte saveznike, ne neprijatelje
- Napadač iznutra je opasniji

Za radoznale…

- CISCO Network Security Glossary

  http://business.cisco.com/glossary/

- CISCO Design Implementation Guide

http://www.cisco.com/warp/public/cc/pd/si/casi/ca3500xl/prodlit/lan_dg.htm

- IBM Multisegment LAN Design Guidelines

http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/gg243398.html