# Nastavenie počítačovej siete

- Základné pojmy
- Nastavenie sieťového rozhrania
- DNS záznamy
- Smerovanie
- Sieťové služby
- Firewall

# Počítačové siete

- Slúžia na komunikáciu medzi počítačmi,
- vzájomné zdieľanie ich zdrojov a informácií,
- Rôzne veľkosti,
- Rôzne topológie,
- Rôzne protokoly,
- Zameriame sa na TCP/IP siete

# Sieťové rozhrania (1)

- Typické pomenovania – môžu sa líšiť v závislosti od distribúcie a nastavení systému.
- Sieťové rozhrania sa typicky ovládajú prostredníctvom systémovej služby alebo tzv. “network manager-a” (na systémoch s GUI).
- Ethernetové rozhrania
  - `eth0, eth1, eth2, ...`
- Wifi rozhrania
  - `wlan0, wlan1, wlan2, ...`
-

# Sieťové rozhrania (2)

- USB interfaces
  - `usb0, usb1, usb2, ...`
- Bluetooth interfaces
  - `bnep0, bnep1, bnep2, ...`
- Point-to-point interfaces
  - `ppp0, ppp1, ppp2, ...`
- Serial interfaces
  - `ttyS0, ttyS1, ttyS2, ...`

# Nastavenia sieťového rozhrania - skriptom

- Konfiguračný súbor
  - `/etc/sysconfig/network-scripts/ifcfg-eth0`
- `DEVICE=eth0` # názov rozhrania
- `USERCTL=no` # zakázať používateľom iným ako root ovládať zar.
- `ONBOOT=yes` # spustiť rozhranie pri bootovaní
- `BOOTPROTO=dhcp` # spustiť DHCP protokol, príp. ‘none’ pre statickú adresu
- `IPADDR=` # IP adresa
- `NETWORK=` # adresa siete
- `NETMASK=` # maska
- `BROADCAST=` # broadcast-ová adresa

# Nastavenia sieťového rozhrania - skriptom

- Konfiguračný súbor
  - `/etc/sysconfig/network-scripts/ifcfg-eth0`
- Zapnutie / vypnutie / reštart siete
  - `/etc/init.d/network {start,stop,restart}`
  - `service network {start,stop,restart}`
  - `systemctl {start,stop,restart} network`
- Sieťová služba môže byť v závislosti od distribúcie inak pomenovaná, e.g. ‘networking’, ‘NetworkManager’, ...
- Zapnutie / vypnutie sieťového rozhrania na základe konf. súboru
  - `ifup eth0, ifdown eth0`

# Nastavenia sieťového rozhrania – manuálne

- Zobrazenie IP adresy
  - `ip addr, ip add, ip a`
- Pridanie statickej IP adresy sieťového rozhrania
  - `ip addr add 192.168.1.1/24 dev eth0`
- Odobratie IP adresy zo sieťového rozhrania
  - `ip addr del 192.168.1.1/24 dev eth0`
- Zapntuie / vypnutie sieťového rozhrania
  - `ip link set eth0 up`
  - `ip link set eth0 down`
- Zmena MAC adresy
  - `ip link set dev eth0 address XX:XX:XX:XX:XX:XX`
- Spustenie sieťového rozhrania s dynamickou IP adresou
  - `dhcpclient eth0, dhclient eth0`

# Nastavenia sieťového rozhrania – manuálne

- Na starších systémoch sa používa príkaz ‘ifconfig’
  - `ifconfig`
  - `ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up`
  - `ifconfig eth0 down`
  - `ifconfig eth0 hw ether XX:XX:XX:XX:XX:XX`

# Ďalšie možnosti konfigurácie

- Konfiguračný súbor
  - `/etc/sysconfig/network`
- Povoliť sieť
  - `NETWORKING=yes`
- Hostname uzla
  - `HOSTNAME=`
- Povoliť preposielanie paketov
  - `FORWARD_IPV4=yes`
- Nastavenie východzej brány
  - `GATEWAYDEV=`
  - `GATEWAY=`

# Smerovanie

- Zobrazenie smerovacích tabuliek
  - `/sbin/route`
  - `netstat –r`
  - `ip route`
  - `cat /proc/net/route`
- Pridanie smerovacej cesty
  - `route add –net 192.168.1.0 netmask 255.255.255.0 eth0`
  - `route add default gw 192.168.1.1 eth0`
- Pridanie cesty pomocou príkazu ‘ip’
  - `ip route add 192.168.1.0/24 dev eth0`
  - `ip route add default via 192.168.1.1 dev eth0`

# Názov uzla - Host Name

- Jednoznačný názov, podľa ktorého je uzol identifikovaný v sieti
  - `hostname`
  - `hostname –f (plný názov aj s doménou)`
- Jeden uzol môže mať viac názvov (aliasov)
  - `hostname –a`
- Zmena názvu uzla
  - `hostname computer`
  - `/etc/hostname`
  - `/etc/hosts`
- Nastavenie vlastných názvov pre iné uzly (bez DNS vyhľadávania)
  - `/etc/hosts`

# Nastavenia DNS

- Konfiguračný súbor `/etc/resolv.conf`
- DNS servery
  - `nameserver 1.2.3.4`
- Doména. Ak nie je zadaná, predpokladá sa od prvej bodky v názve uzla
  - `domain mydomain.local`
- DNS suffix, ktorý sa má prehľadávať pri vyhľadávaní pomocou DNS
  - `search fiit.stuba.sk`
  - `host www`

# Nastavenie vyhľadávania DNS

- Konfiguračný súbor `/etc/host.conf`
- Nastavenie poradia vyhľadávania záznamov.
  - `order hosts, bind, nis`
- Povolenie výstupu viacerých IP adries pre jeden uzol. Ak je vypnuté, knižnica resolv vráti len prvý záznam.
  - `multi off`
- Ďalšie voľby
  - `trim, spoof, nospoof, spoofalert, reorder`

# Nastavenia proxy

- (HTTP) Proxy server je server, ktorý sa nachádza medzi klientom a HTTP serveromr.
- Klient pošle webový dopyt na proxy, ktorý ho následne prepošle na cieľový HTTP server a vráti odpoveď.
- Viacero prípadov použitia, napr. riadenie prístupu na Internet, “web caching”, monitorovanie webovej komunikácie.
- Premenné prostredia v */etc/environment:*
  - `export http_proxy=“192.168.1.10:8080”`
  - `export no_proxy=“localhost,192.168.1.1”`

# Nastavenie systémových databáz

- Informácie ako zoznam používateľov, ich hesiel, uzlov a pod. sa môže nachádzať v rôznych databázach::
  - e.g. `files, dns, nis, ldap`
- Konfiguračný súbor určujúci povolené zdroje údajov a ich poradie
  - `/etc/nsswitch.conf`
- Compat je podobné ako files, ale povoľuje použitie špeciálnych znakov +/ pre zdroje passwd a group (`man nsswitch.conf`).
  - `passwd: compat`
  - `hosts: ldap dns files`

# Sieťové služby TCP/IP a IP protokoly

- Zoznam najznámejších a najpoužívanejších služieb nad protokolmi TCP a UDP
  - `/etc/services`
- Zoznam najznámejších a najpoužívanejších IP protokolov
  - `/etc/protocols`

# Netstat

- Slúži na zobrazenie sieťových spojení, smerovacích tabuliek a štatistík
- Zobrazenie všetkých TCP portov, na ktorých počúva nejaký program a jeho vypísanie
  - `netstat -tlp`
- Zobrazenie všetkých spojení v numerickom tvare (bez DNS prekladu):
  - `netstat -an`

# Nmap

- Nástroj na skúmanie a auditovanie sietí.
- Host discovery – ktoré uzly v sieti sú “hore”.
  - `nmap -sn 192.168.1.0/24 (ping scan)`
- Port scan – zistenie stavu portov..
  - `nmap -sS -p1-100 1.2.3.4 (SYN scan)`
- Service detection – služby, ktoré počúvajú na otvorených portoch a ich verzie.
  - `nmap -sV 1.2.3.4`
- OS detection – zistenie OS vzdialeného uzla.
  - `nmap -O 1.2.3.4`
- Zraniteľnosti, skripty, ...

# Netcat (1)

- “Švajčiarsky nožík pre TCP/IP sieť”
- Široké možnosti využitia v počítačových sieťach
- Umožňuje TCP a UDP spojenie na zvolený port
  - `nc [-u] hostname port`
- Online chat.
  - `nc -l -p 1234  // server, -l otvorí počúvajúci port`
  - `nc hostname 1234 // klient`

# Netcat (2)

- Prenos súborov. Po zistení EOF sa spojenie ukončí.
  - `nc -l -p 1234 > outfile`
  - `cat infile | nc hostname 1234 -q 0`
- Vzdialený prístup.
  - `nc -l -p 1234 -e /bin/bash`
  - `nc hostname 1234`

# ARP

- Slúži na zobrazovanie a nastavovanie ARP záznamov jadra
- Zobrazenie ARP tabuľky
  - `arp, arp –n`
- Nastavenie statického ARP záznamu (ochrana pred ARP útokmi typu man in the middle na prepínanej sieti)
  - `arp –s xx:xx:xx:xx:xx:xx`
- Vymazanie ARP cache
  - `arp –d 192.168.1.1`
  - `ip –s –s neigh flush all`

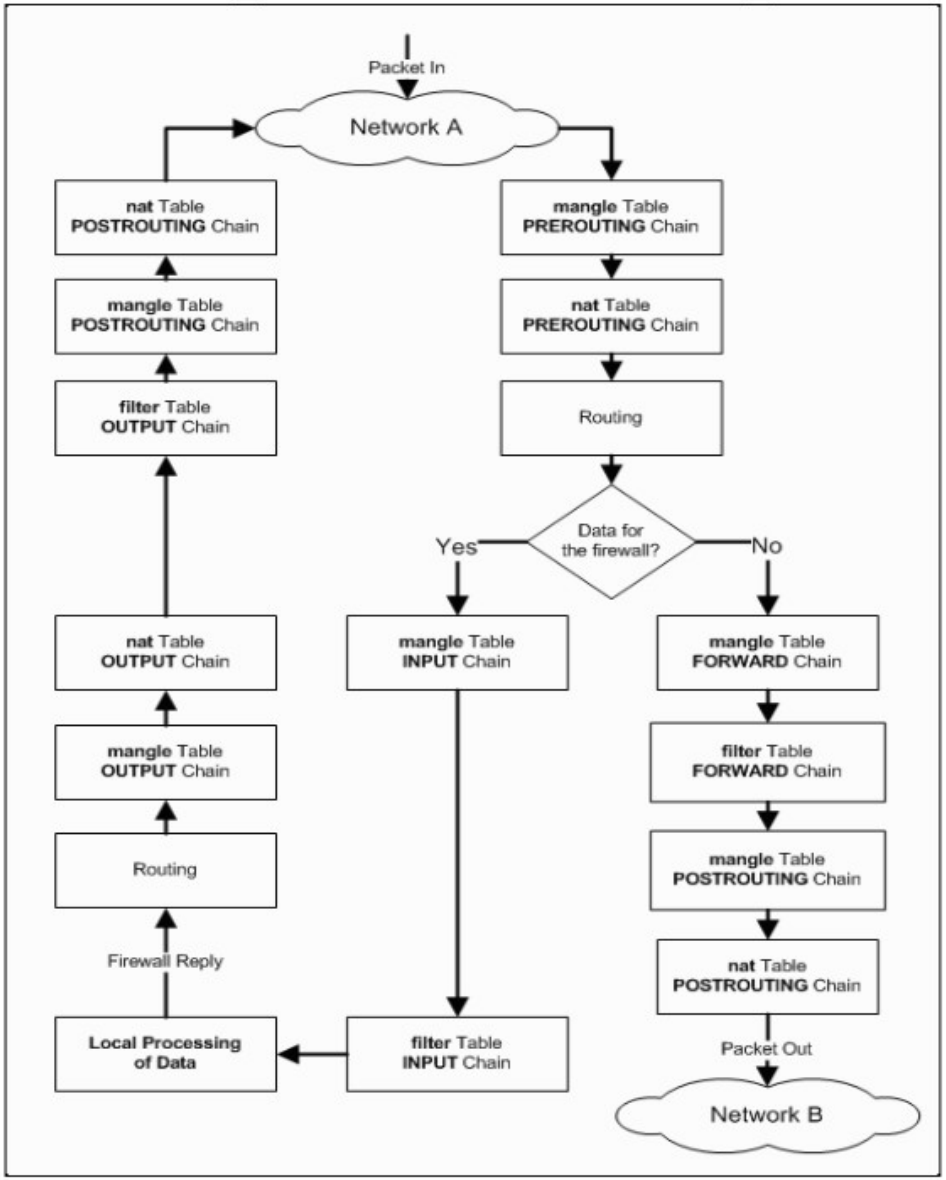
# Firewall

- Firewall zabudovaný priamo v jadre Linuxu - iptables. Zavedenie modulu do jadra. (v prípade potreby):
  - `modprobe ip_tables`
- Tri typy tabuliek s pravidlami.
  - `filter` – filtrovanie paketov na základe definovaných pravidiel.
  - `nat` – slúži na preklad IP adries (NAT).
  - `mangle` – uslúži na úpravu TCP hlavičiek, využíva sa predovšetkým na QoS
- Paket je spracovaný prvým pravidlom, ktorého podmienke vyhovie

# iptables – tabuľky a reťazce

- Každá tabuľka má niekoľko reťazcov pravidiel.
- NAT:
  - `PREROUTING –` vykoná sa pred smerovaním,
  - `POSTROUTING –` vykoná sa po smerovaní,
  - `OUTPUT –` aplikuje sa na odchádzajúce pakety.
- FILTER:
  - `INPUT –` prichádzajúce pakety určené pre tento uzol,
  - `OUTPUT –` odchádzajúce pakety z uzla,
  - `FORWARD –` pakety smerované na iné rozhranie (prechádzajúce uzlom).
- MANGLE: ako všetky predchádzajúce. Vykonáva sa vždy pred vstupom do konkrétneho reťazca tabuliek nat a filter-
- Možnosť vytvoriť vlastný reťazec (chain).

# Cesta paketu cez iptables



# iptables - ciele

- ACCEPT – paket je povolený.
- DROP – paket je zahodený.
- REJECT – Podobne ako DROP, ale
- odosielajúcemu uzlu odpovie správou, že paket bol odmietnutý. Default odpoveď::
  - `--reject-with icmp-port-unreachable`
- LOG – paket je zalogovaný syslogom (vyhodnocovanie pravidiel pokračuje ďalším pravidlom v poradí)
- RETURN – paket sa vráti do rodičovského reťazca (použitie pri vlastných reťazcoch).

# iptables – tabuľka NAT

- Akcie pre reťazce v tabuľke NAT.
- DNAT – preklad cieľovej adresy paketu.
  - `--to-destination <address>[:port]`
- SNAT – preklad zdrojovej adresy paketu.
  - `--to-source <address>[:port]`
- MASQUERADE – preklad zdrojovej adresy paketu, pričom ako zdrojová sa použije IP adresa sieťového rozhrania, na ktorom je aplikované pravidlo. Vhodné pre dynamické IP adresy.

# iptables – dôležité prepínače (1)

- `-t table` – tabuľka, ktorá sa upravuje.
- `-P target` – nastavenie default politiky.
- `-j target` – aká akcia sa má vykonať (jump)
- `-A chain` – pridať pravidlo na koniec reťazca (Append)
- `-I chain` – pridať pravidlo na koniec reťazca (Insert).
- `-F chain` – vymazať všetky pravidlá (flush).

# iptables – dôležité prepínače (2)

- `-p protocol` – protokol.
- `-s source_ip` – zdrojová IP adresa.
- `-d destination_ip` – cieľová IP adresa.
- `-i in_interface` – vstupné rozhranie.
- `-o out_interface` – výstupné rozhranie.
- `--sport src_port` – zdrojový port.
- `--dport dst_port` – cieľový port.

# iptables – použitie

- `iptables -P INPUT DROP`
- `iptables -A INPUT -i eth0 -s \ 147.175.92.1 -p TCP --dport 22 \`

  `-j ACCEPT`
- `iptables -A INPUT -i eth0 -p ICMP \`

  `--icmp-type echo-request -j ACCEPT`
- `iptables -A INPUT -i eth0 -m state \`

  `--state ESTABLISHED,RELATED -j ACCEPT`
- `iptables -A INPUT -j LOG`

# iptables – vysvetlenie predchádzajúceho príkladu

- Nastavenie default politiky pre reťazec INPUT na DROP. Všetky pakety, ktoré neprejdú povolenými pravidlami budú zahodené.
- Povolenie SSH len z IP adresy 147.175.92.1.
- Povolenie ICMP len typu `echo-request`.
- Povolenie paketov, ktoré prichádzajú od nadviazaných spojení (ak by sme ich zakázali, nemohli by sme komunikovať ani my smerom von).
- Všetko ostatné sa loguje a následne zahadzuje.
- `dmesg | tail` – zobrazenie posledných 10 systémových správ (logov).

# iptables – správa

- Zobrazenie aktuálnych pravidiel
  - `iptables -vnL [-t table]`
- Zmazanie pravidiel (pozor na default politiku!)
  - `iptables -F INPUT`
- Uloženie stavu
  - `service iptables save`
- Obnovenie uloženého stavu
  - `service iptables reload`

# Ďalšie užitočné nástroje

- Testovanie siete
  - `ping, traceroute, arping`
- Zachytávanie paketov (sniffing)
  - `tcpdump, wireshark, ettercap`
  - `iftop, nettop`
- Intrusion Detection System
  - `snort, suricata`

# Literatúra a zdroje

- Manuálové stránky
  - https://linux.die.net/man/
- ip command cheat sheet
  - https://access.redhat.com/articles/ip-command-cheat-sheet
- Linux Networking HOWTO
  - https://tldp.org/HOWTO/NET3-4-HOWTO-5.html
- iptables HOWTO
  - https://www.netfilter.org/documentation/HOWTO/packet-filtering-HOWTO-7.html