

Administrace Unixu a sítě

```
inet6-adr: fe80::210:a4ff:fe01:9e5d/64 Rozsah:Linka
AKTIVOVÁNO VŠESMĚROVÉ_VYSÍLÁNÍ BĚŽÍ MULTICAST MTU:1500 Metrika:1
RX packets:66690 errors:0 dropped:0 overruns:0 frame:0
TX packets:100149 errors:0 dropped:0 overruns:0 carrier:0
kolizí:0 délka odchozí fronty:0
RX bytes:21490419 (20.4 MiB) TX bytes:10545763 (10.0 MiB)
```

6. Síťování, základy

```
bug:/home/qiq# getent passwd | grep -v ^$
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
Debian-exim:x:102:102::/var/spool/exim4:/bin/false
qiq:x:1000:1000:Miroslav Spousta,/,/,/home/qiq:/bin/bash
sshd:x:100:65534::/var/run/sshd:/bin/false
identd:x:101:65534::/var/run/identd:/bin/false
messagebus:x:103:104::/var/run/dbus:/bin/false
gdm:x:104:105:Gnome Display Manager:/var/lib/gdm:/bin/false
hal:x:106:106:Hardware abstraction layer,/,/,/var/run/hal:/bin/false
saned:x:109:109::/home/saned:/bin/false
bind:x:105:110::/var/cache/bind:/bin/false
smmta:x:107:111:Mail Transfer Agent,/,/,/var/lib/sendmail:/bin/false
smmsp:x:108:112:Mail Submission Program,/,/,/var/lib/sendmail:/bin/false
test:x:1001:1001:Test User,/,/,/home/test:/bin/bash
postfix:x:110:115::/var/spool/postfix:/bin/false
```

Miroslav Spousta

2006

<http://www.ucw.cz/~qiq/vsfs/>

Xen

- virtuální servery (<http://www.cl.cam.ac.uk/Research/SRG/netos/xen/>)
- budete mít rootovská oprávnění ve virtuálním serveru
- přístup je po dobu výuky
- OS: Debian 3.1
- RAM: 32 MB, swap: 128 MB (/dev/sda2), root: 512 MB (/dev/sda1)
- několik síťových karet (eth0, eth1, ...)
- Síťové karty jsou propojeny virtuálními přepínači

Přístup k virtuálním serveru:

- **ssh login@kozel.vsfs.cz**
- **xencons localhost 90xx**
- xx je číslo serveru (login: **root**, heslo: žádné)

Sít'ové rozhraní

- neboli interface, HW: sít'ová karta
- v OS se přes sít'ové rozhraní přistupuje ke kartě
 - vlastně reprezentuje dané fyzické zařízení
- je to spojnice mezi vyššími protokoly a fyzickým zařízením
- V Linuxu:
 - Ethernet: eth0, eth1, ...
 - WLAN: wlan0, wlan1, ...
 - IrDA: irda0, irda1, ...
- jedna sít'ová karta může mít více rozhraní
- rozhraní mohou být virtuální
- diagnostika sít'ového rozhraní (Ethernetu): **mii-tool**, **mii-diag**
 - umožňují detekovat a nastavovat parametry linky (full/half-duplex, rychlost, ...)

MAC adresy

- adresy na linkové úrovni
- 48 bitů velké, tvaru 11:22:33:44:55:66
- z prvních tří byte se dá zjistit výrobce zařízení
 - v prvním byte ještě uni/multicast, globálně/lokálně přidělená
- každý síťový interface má přiřazenou MAC adresu
- zjistíme příkazem **ifconfig**
 - umožňuje zjišťovat a nastavovat mnohem více: IP adresy, stav rozhraní, MTU, statistiku paketů/dat, ...
- **ifconfig -a**

IP adresy

- v IP adrese jsou zakódované dvě složky: adresa sítě a adresa počítače v síti
- původně 5 tříd: A, B, C, D, E
 - pro různé velikosti sítě, multicast, ...
 - udávaly, kde je hranice mezi síťovou a lokální částí
- dnes: CIDR bloky (beztrídní)
 - pořad je nutné znát hranici, již ji nelze zjistit z adresy
 - ke každé adrese je třeba přidat, kde je hranice
- jak hranici zadat?
 - prefix = počet bitů od začátku adresy, které patří síťové části
 - netmask = nastavené bity určují, kam až sahá síťová maska
- příklad:
 - 148.231.53/24, 195.113.31.123/26
- multicast adresy

ifconfig

- ovládání síťového rozhraní
 - umožňuje nastavit IP adresu rozhraní (také MAC adresu)
 - nastavení MTU (Maximum Transfer Unit)
 - multicast, broadcast, ...
- **ifconfig interface adresa netmask maska up**
 - nastaví IP adresu pro interface a aktivuje („nahodí“) interface
 - také nastaví cestu ve směrovací tabulce pro danou síť
- **ifconfig interface down**
 - deaktivuje interface
- alternativa: příkaz **ip** (swiss knife)
 - **ip addr add adresa dev interface**
 - **ip link set interface up**



nastavte si na eth0 adresu 10.0.0.xx/24 a na eth1 10.0.1.xx/24

ping

- testování dostupnosti rozhraní (IP adresy)
 - v pozitivním případě se dozvíme, že IP vrtstva rozhraní je v pořádku (rek. spočetnost :-))
- využívá ICMP protokol (zprávy Echo Request a Echo Reply)
- nejjednodušší a velmi účinný diagnostický nástroj
- příkaz ping:
 - **ping ip_adresa**
- další možnosti:
 - **-s packet_size** umožňuje nastavit velikost datagramu, který se bude posílat (64B)
 - **-i interval** nastavuje, jak často se bude posílat Echo Request (1s)
 - **-f** flood ping, posílá pakety a za každý Request vykreslí tečku, po příchodu Reply ji zase smaže. Zobrazuje počet ztracených paketů.



zkuste ping na rozhraní některého svého souseda

tcpdump

- packet sniffer
- přepne rozhraní do promiskuitního (:-)) módu
- odchytává všechny pakety na rozhraní, i ty, které nepatří této stanici
 - ve switchované síti většinou neuvidíme provoz sousedů
- zobrazuje hlavičky (a dekoduje je)
- **tcpdump -i eth0**
 - **-i interface** rozhraní
 - **-v** zobrazí více informací z hlaviček
 - **-w file zapisuje sebrané pakety do souboru**
 - další filtrování toho, co se zobrazuje: viz man tcpdump



podívejte se pomocí **tcpdump -v -i eth0** na provoz na interface eth0

ARP

- Address Resolution Protocol
- překládá adresy IP -> MAC
- stanice, která chce komunikovat po lokální síti, musí znát MAC adresu příjemce (zná IP adresu)
- pracuje přímo nad IP protokolem
- vysílá se (linkovým) broadcastem (aby přišel všem v síti)
- dotyčná stanice odpovídá tazateli (unicastem)
- každá stanice si udržuje cache mapování, položky časem vyprší
 - je také možné „ručně“ nastavovat (měnit, mazat) položky

arp

- vypisuje arp tabulky kernelu
 - tabulky překladu adres IP adresa -> MAC adresa
 - umožňuje nastavovat záznamy
 - chceme-li získat MAC adresu, pingneme stroj a pak vypíšeme adresu pomocí **arp**

- příkaz **arping**

- umožňuje získat MAC adresu přímo, pošle ARP dotaz



zjistěte, se kterými kolegy jste komunikovali

- síťové karty mívaly adresy pevně zadrátované (v ROM), dnes jsou v registrech, dají se většinou měnit
 - není to dobrý prostředek pro zabezpečení sítě
- jak si nastavit MAC adresu (*interface nesmí být aktivní*):
- **ifconfig interface hw ether XX:XX:XX:XX:XX:XX**
- **ip link set address XX:XX:XX:XX:XX:XX dev interface**

Směrování v IP

- směrovače po cestě se zajímají výhradně o síťovou část IP adresy
 - vědí, na kterých rozhraních mají kterou síť
 - vědí také o sousedních směrovačích
- koncové uzly znají síť na svém rozhraní a default gateway
- směrovací tabulka: tam jsou uvedeny známé cesty
 - prohledává se od specifitějších k méně specifickým adresám
- příkaz **route** (nebo **netstat -r**) vypíše směrovací tabulku
- default gateway = směrovač, který přijde na řadu, pokud datagram není lokální
- přidání záznamu pro default gateway
- **route add [-net|-host] *addr/prefix gw gateway interface***
- **ip route add to *addr/prefix via gateway dev interface***



přidejte defaultní cestu přes adresu brány 10.0.0.100

- vyzkoušejte, že funguje připojení do Internetu (pomocí ping)

traceroute, tracepath

- příkazy, které umožňují sledovat, kudy paket v dané síti prochází
- využívají k tomu položku TTL v hlavičce IP datagramu
 - která se snižuje po průchodu každým směrovačem
 - po klesnutí na 0 se daný paket zahodí a vytvoří se speciální zpráva (ICMP) o zahození, která se pošle odesilateli
- používají buď Echo Request nebo UDP pakety
- tracepath navíc zobrazuje MTU, případné asymetrie v TTL



pusťte si `tcpdump -v -i eth0` a poté `traceroute`, podívejte se, zda `traceroute` používá UDP, nebo ICMP zprávy

```
# traceroute 195.113.31.123
traceroute to 195.113.31.123, 30 hops max, 38 byte packets
 1 10.0.0.100 (10.0.0.100) 2.254 ms 0.130 ms 0.067 ms
 2 atrey (195.113.31.123) 0.187 ms 0.226 ms 0.167 ms
```

DHCP

- RFC 2131, Dynamic Host Configuration Protocol
- rozšíření BOOTP protokolu
- umožňuje automatickou konfiguraci sítě stanic
- centrální přidělování IP adres a dalších informací o síti
 - DNS server, maska sítě, default router, WINS server
- tyto informace se periodicky obnovují
- klient i server si pamatují minulý stav => klient dostává stejnou IP adresu



řekněte si o adresu (IP) přes dhcp protokol

- hint: man dhclient
- abyste od serveru získali IP adresu, musíte si změnit MAC adresu síťového rozhraní eth0 na adresu tvaru 00:11:22:33:44:xx



zjistěte MAC a IP adresu DHCP serveru

Nastavení DNS

- `/etc/resolv.conf`
 - definice nameserveru: (nameserver 10.0.0.1), definice domény, která se zkouší připojit (search domain.cz)
- `/etc/hosts`
 - statický překlad jméno -> IP adresa (pouze A záznamy)
- `/etc/nsswitch.conf`
 - řídí pořadí, v jakém se bude vyhledávat překlad a odkud se budou brát informace
 - files, LDAP, NIS, ...
 - nejen DNS, ale i passwd databáze, group, ...
- někdy může běžet nscd (name services caching daemon)
 - cachuje překlady (DNS, passwd, ...)
 - zrychluje odezvu, ale může způsobovat problémy