Nástroje práce se sítí

PB156cv - jaro 2020

Michal Šnajdr
snajdr@ics.muni.cz

Cíle cvičení

- získat přehled o nástrojích pro stav/nastavení sítě
- co vlastně hledáme?
- praktické vyzkoušení

Problémy na poslední míli

- 1. vrstva
  - Máme ten kabel opravdu zapojený?
  - Pracujeme se správným rozhraním?
- 2.vrstva
  - vidíme souseda/GW v ARP cache
- 3. vrstva
  - Mám správnou masku?
  - Mám nastavenu GW?
  - Funguje spojení s GW?

ethtool vypíše informace o 1 a 1.5 vrstvě:

```
$ ethtool enp2s0
Settings for enp2s0:
        Supported ports: [ TP MII ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Supported pause frame use: No
        Supports auto-negotiation: Yes
        Supported FEC modes: Not reported
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Half 1000baseT/Full
        Advertised pause frame use: Symmetric Receive-only
        Advertised auto-negotiation: Yes
        Advertised FEC modes: Not reported
        Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                             100baseT/Half 100baseT/Full
                                             1000baseT/Full
        Link partner advertised pause frame use: No
        Link partner advertised auto-negotiation: Yes
        Link partner advertised FEC modes: Not reported
        Speed: 1000Mb/s
        Duplex: Full
        Port: MII
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
Cannot get wake-on-lan settings: Operation not permitted
        Current message level: 0x00000033 (51)
                               drv probe ifdown ifup
        Link detected: yes
```

Utilita *ip* z balíku *iproute2* nahrazuje ulility *ifconfig*, *arp*, *route* ... z balíku *net-tools*[1]

Proč dále nepoužívat *net-tools*:

- zastaralé
- neudržované
- používají stará jaderná API
- např v Ubuntu označeno jako obsolete od 14.04 LTS
- v novějších vydání distribucí nebývá v základní instalaci (Ubuntu 18.04 LTS)

[1] https://dougvitale.wordpress.com/2011/12/21/deprecated-linux-networking-commands-and-their-replacements/

Příklad zastaralosti *net-tools*, více adres na rozhraní:

```
$ ip addr
...
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:24:d7:ec:0e:c0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.11/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp3s0
       valid_lft 1818sec preferred_lft 1818sec
    inet 10.10.10.10/24 scope global wlp3s0
       valid_lft forever preferred_lft forever
    inet6 fe80::870c:98a8:89de:79cc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

$ ifconfig
...
wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.11  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::870c:98a8:89de:79cc  prefixlen 64  scopeid 0x20<link>
        ether 00:24:d7:ec:0e:c0  txqueuelen 1000  (Ethernet)
        RX packets 49987738  bytes 51783673883 (51.7 GB)
        RX errors 0  dropped 261916  overruns 0  frame 0
        TX packets 38191566  bytes 21548892979 (21.5 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

ip addr výstup obsahuje L1, L2 i L3 informace

```
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 8d:67:45:e7:56:89 brd ff:ff:ff:ff:ff:ff
    inet 147.251.1.70/26 brd 147.251.1.65 scope global eth0
    inet6 fe80::8d67:45ff:fee7:5689/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether e4:1f:13:e5:41:82 brd ff:ff:ff:ff:ff:ff
    inet 172.31.5.147/24 brd 172.31.5.255 scope global eth1
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 34:40:b5:a6:d3:98 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3640:b5ff:fea6:d398/64 scope link
       valid_lft forever preferred_lft forever
5: eth3: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
    link/ether 34:40:b5:a6:d3:9a brd ff:ff:ff:ff:ff:ff
    inet6 fe80::3640:b5ff:fea6:d39a/64 scope link
       valid_lft forever preferred_lft forever
6: eth4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:1b:21:bd:0c:e0 brd ff:ff:ff:ff:ff:ff
    inet 10.254.87.63/24 brd 10.254.87.255 scope global eth4
    inet6 fe80::21b:21ff:febd:ce0/64 scope link
       valid_lft forever preferred_lft forever
7: eth5: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 00:1b:21:bd:0c:e1 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::21b:21ff:febd:ce1/64 scope link
       valid_lft forever preferred_lft forever
```

2. a 3. vrstva - routovací tabulka

- jaké sítě v ní vidíme?
- z kterého rozhraní budeme přistupovat do Internetu?

```
$ ip route
default via 147.251.255.1 dev enp0s25 proto dhcp metric 100
default via 147.251.44.1 dev wlp3s0 proto dhcp metric 600
147.251.255.0/26 dev enp0s25 proto kernel scope link src 147.251.255.16 metric 100
147.251.44.0/22 dev wlp3s0 proto kernel scope link src 147.251.44.81 metric 600
169.254.0.0/16 dev wlp3s0 scope link metric 1000
8.8.8.8 via 147.251.44.1 dev wlp3s0
```

2. a 3. vrstva - dostupnost zařízení

Který z následujících výstupů je funkční LAN (GW je 192.168.255.1)?

```
$ ping 192.168.255.1
PING 147.251.255.1 (147.251.1.1) 56(84) bytes of data.
^C
--- 192.168.255.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2032ms

$ ip neigh
192.168.255.1 dev eth0 lladdr 00:14:4f:e2:17:c4 REACHABLE
```

```
$ ping 192.168.255.1
PING 147.251.255.1 (147.251.255.1) 56(84) bytes of data.
^C
--- 192.168.10.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2032ms

$ ip neigh
192.168.255.38 dev eth0 lladdr 00:28:4f:e2:46:e7 REACHABLE
192.168.255.1 dev eth0  INCOMPLETE
```

Protokol ICMP

Slouží k:

- reportování chyb přenosu
- kontrole dostupnosti (ping)
- přesměrování na jiný router

V IPv6 převzal roli protokolu ARP + přidáno oznámení směrovače (SLAAC).

Druhy zpráv ICMP

Type	Name	Reference
0	Echo Reply	[RFC792]
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	[RFC792]
4	Source Quench (Deprecated)	[RFC792][RFC6633]
5	Redirect	[RFC792]
6	Alternate Host Address (Deprecated)	[RFC6918]
7	Unassigned	
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Solicitation	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]
13	Timestamp	[RFC792]
14	Timestamp Reply	[RFC792]
15	Information Request (Deprecated)	[RFC792][RFC6918]
16	Information Reply (Deprecated)	[RFC792][RFC6918]
17	Address Mask Request (Deprecated)	[RFC950][RFC6918]
18	Address Mask Reply (Deprecated)	[RFC950][RFC6918]
19	Reserved (for Security)	[Solo]
20-29	Reserved (for Robustness Experiment)	[ZSu]
30	Traceroute (Deprecated)	[RFC1393][RFC6918]
31	Datagram Conversion Error (Deprecated)	[RFC1475][RFC6918]
32	Mobile Host Redirect (Deprecated)	[David_Johnson][RFC6918]
33	IPv6 Where-Are-You (Deprecated)	[Simpson][RFC6918]
34	IPv6 I-Am-Here (Deprecated)	[Simpson][RFC6918]
35	Mobile Registration Request (Deprecated)	[Simpson][RFC6918]
36	Mobile Registration Reply (Deprecated)	[Simpson][RFC6918]
37	Domain Name Request (Deprecated)	[RFC1788][RFC6918]
38	Domain Name Reply (Deprecated)	[RFC1788][RFC6918]
39	SKIP (Deprecated)	[Markson][RFC6918]
40	Photuris	[RFC2521]
41	ICMP messages utilized by experimental mobility protocols such as Seamoby	[RFC4065]
42	Extended Echo Request	[RFC8335]
43	Extended Echo Reply	[RFC8335]
44-252	Unassigned	
253	RFC3692-style Experiment 1	[RFC4727]
254	RFC3692-style Experiment 2	[RFC4727]
255	Reserved	[JBP]

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

Kódy ICMP typ 3

Type 3 — Destination Unreachable

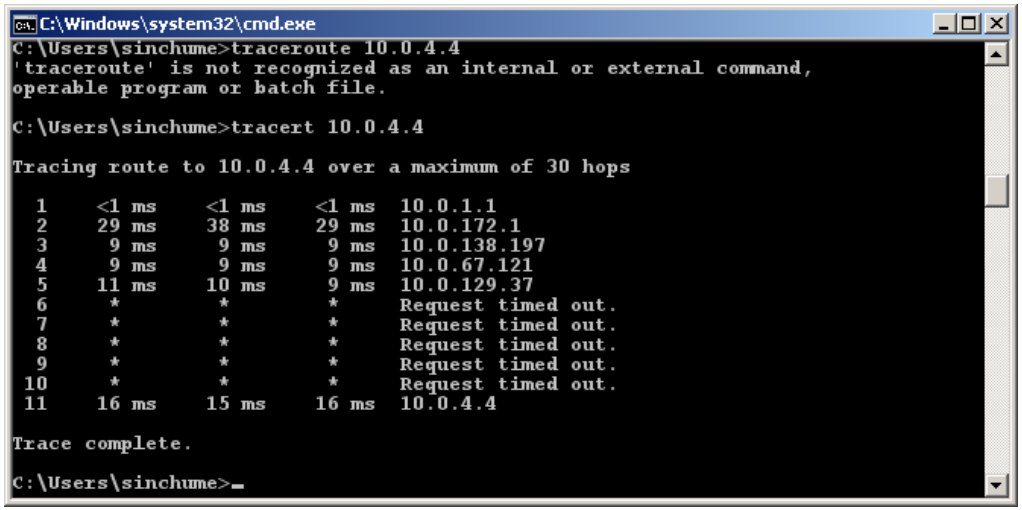
Registration Procedure(s)
IESG Approval or Standards Action
Reference
[RFC792][RFC2780]
Available Formats
csv

Codes	Description	Reference
0	Net Unreachable	[RFC792]
1	Host Unreachable	[RFC792]
2	Protocol Unreachable	[RFC792]
3	Port Unreachable	[RFC792]
4	Fragmentation Needed and Don't Fragment was Set	[RFC792]
5	Source Route Failed	[RFC792]
6	Destination Network Unknown	[RFC1122]
7	Destination Host Unknown	[RFC1122]
8	Source Host Isolated	[RFC1122]
9	Communication with Destination Network is Administratively Prohibited	[RFC1122]
10	Communication with Destination Host is Administratively Prohibited	[RFC1122]
11	Destination Network Unreachable for Type of Service	[RFC1122]
12	Destination Host Unreachable for Type of Service	[RFC1122]
13	Communication Administratively Prohibited	[RFC1812]
14	Host Precedence Violation	[RFC1812]
15	Precedence cutoff in effect	[RFC1812]

`https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-codes-3`

Traceroute

- postupně zasílá pakety se zvyšujícím se TTL
- podle příchozích ICMP zpráv reportuje kudy je paket směřován včetně RTT
- ve výchozím nastavení pousílá ICMP echo (Windows) nebo UDP pakety (Unix)
- utilita traceroute v Unix, tracert ve Windows



DNS utility

DNS kromě překladu jmen na IP adresy dokáže dát i další informace uložené v systému DNS

- server zpracovávající poštu pro stroj/doménu
- servery služeb
  - SIP (VoIP)
  - Kerberos
  - CalDAV
  - tiskárny
  - ...

Příklad informací z DNS:

```
$ host youtube.com
youtube.com has address 216.58.201.110
youtube.com has IPv6 address 2a00:1450:4014:801::200e
youtube.com mail is handled by 30 alt2.aspmx.l.google.com.
youtube.com mail is handled by 20 alt1.aspmx.l.google.com.
youtube.com mail is handled by 10 aspmx.l.google.com.
youtube.com mail is handled by 50 alt4.aspmx.l.google.com.
youtube.com mail is handled by 40 alt3.aspmx.l.google.com.
$ host 216.58.201.110
110.201.58.216.in-addr.arpa domain name pointer prg03s02-in-f14.1e100.net.
110.201.58.216.in-addr.arpa domain name pointer prg03s02-in-f110.1e100.net.
```

Příklad reálného využití informací z DNS při hledání chyby

```
$ host scmsadmin.thermofisher.com
scmsadmin.thermofisher.com is an alias for thermofisher.com.edgekey.net.
thermofisher.com.edgekey.net is an alias for thermofisher.com.edgekey.net.globalredir.akadns.net.
thermofisher.com.edgekey.net.globalredir.akadns.net is an alias for e1778.x.akamaiedge.net.
e1778.x.akamaiedge.net has address 23.38.80.158
```

Nmap

Nástroj pro mapování sítě/stroje. Mnoho různých skenů sítě.
Příklady:

```
$ nmap gitlab.ics.muni.cz

Starting Nmap 7.40 ( https://nmap.org ) at 2019-03-28 20:42 CET
Nmap scan report for gitlab.ics.muni.cz (147.251.6.102)
Host is up (0.00037s latency).
Other addresses for gitlab.ics.muni.cz (not scanned): 2001:718:801:406::102
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
9102/tcp open  jetdirect

# nmap -sP 147.251.1.64/26

Starting Nmap 7.40 ( https://nmap.org ) at 2019-03-28 20:44 CET
Nmap scan report for routics.ics.muni.cz (147.251.1.65)
Host is up (0.0013s latency).
Nmap done: 64 IP addresses (1 host up) scanned in 1.96 seconds
```

Rekapitulace

- 1. vrstva
  - ethtool
- 2. vrstva
  - ip neigh (ARP)
  - ip addr (MAC adresy)
- 3. vrstva
  - ip addr (adresy)
  - ip route (směrovací tabulka)
  - ping (oznamování chyb, testování)
  - traceroute (hledání cesty)
- 4. vrstva
  - nmap
- Aplikační vrstva
  - host, nslookup (DNS dotazy)

Firewall

Označní pro zařízení/software provádějící filtrování provozu.
Podle způsobu funkce je dělíme na:

- stavové - hlídají průbeh spojení
- bezstavové (filtry) - posuzují každý paket zvlášť

Takzvané Next Generation FW jsou kombinovány s funkcemi:

- IPS
- filtrování webových stránek
- antivirová kontrola
- detekce aplikací
- ochrana proti malwaru

IPtables

iptables je nástoj pro nastavování FW pravidel v linuxovém jádře. Práva pracovat s FW má v linuxu pouze superuživatel.
Pravidla jsou seřazeny v tzv. chain:

- INPUT - data určená pro danou stanici
- OUTPUT - data odesílána stanicí
- FORWARD - pokud stanice funguje jako router

Základní akce (target):

- ACCEPT - přijmout, poslat dál
- DROP - paket zahodit
- GOTO - dále zpracovat v jiném chain (vytvoření stromu)

Výchozí chování

Pokud paket není zpracován žádným z pravidel, uplatní je výchozí akce pro daný chain. Pravidla se vyhodnocují postupně podle pořadí.
U distribuje Kubuntu/Debian na počítačích cvičení je výchozí politikou vše povolit.

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   74  4972 ACCEPT     all  --  enp0s10 any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Příklady

Základní syntaxe:

```
iptables [tabulka] [akce] [chain] [ip_část] [match] [target] [target_info]
```

Nastavení výchozí politiky pro chain INPUT (zahodit):

```
iptables -P INPUT DROP
```

Další příklady:

```
\\povolení provozu z 192.168.0.1 přicházející na rozhraní eth0
iptables -A INPUT -i eth0 -s 192.168.0.1 -j ACCEPT

\\zahození všech tcp paketů které nepocházejí z  192.168.0.1
iptables -A INPUT -p tcp -s ! 192.168.0.1 -j DROP

\\přidání pravidla na řádek 2 pro povolení TCP/80 odkudkoliv
iptables -I INPUT 2 -p tcp --dport 80 -j ACCEPT

\\odebrání 5. pravidla
iptables -D INPUT 5

\\vypsání pravidel včetně očíslovaných řádků
iptables -L --line-numbers
```

Další informace viz `https://www.root.cz/serialy/vse-o-iptables/`

Úkol

Zadání v samostatném souboru *roomsheet-lab3.pdf* najdete ve studijních materiálech.