TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Úloha 1 - síťové příkazy

Datum zpracování: 18.3.2022

Zpracovali: Daniel Knespl

Zadání

Vaším úkolem je vyzkoušet si příkazy, které souvisejí se sítí. Pokud není uvedeno jinak, pracujte v hlavním operačním systému. Některé dílčí úlohy mohou vyžadovat i spuštěný virtuální počítač (image disku, nekomprimovaný image). Spusťte jej před zahájením práce na úlohách.

1. Příkaz ip a (ip je příkaz, a přepínač) vypíše nastavení vašich síťových rozhraní
    - zjistěte a do protokolu zkopírujte kompletní nastavení všech sítových adaptérů
    - okomentujte jednotlivé položky
    - proveďte totéž pomocí příkazu ifconfig, porovnejte výstupy a krátce okomentujte
    - nápověda: man ifconfig, ip help
2. Příkaz ip n vypíše MAC adresy okolních počítačů a jejich přiřazení k IP adresám a kanonickým jménům
    - vložte výstup
    - pomocí online zdrojů zjistěte z MAC adres výrobce zjištěného síťového hardware
    - proveďte totéž pomocí příkazu arp, porovnejte výstupy a krátce okomentujte
    - nápověda: ip help
3. Příkaz ss vypíše provoz na síťových rozhraních
    - vypište a okomentujte seznam aktuálních **síťových** spojení
    - vypište a okomentujte seznam otevřených portů
    - na závěr cvičení vypište souhrnné statistiky všech **síťových** protokolů (tcp, udp, ...) a hlavní bloky okomentujte
    - totéž proveďte příkazem netstat
    - nápověda: man ss, man netstat

4. Příkaz ping - zkusí kontaktovat konkrétní server a zjistí čas jeho odpovědi. Tato hodnota vypovídá o vzdálenosti k serveru, jeho vytížení, případně o vytížení datové linky, kterou jste připojení.
    - Zjišťujte odezvu na servery www.tul.cz, www.seznam.cz, www.google.cz, www.facebook.com za následujících podmínek: (a porovnejte výsledky)
        - při odesílání paketů velkých 1024 bajtů (jedním z parametrů pingu lze nastavit velikost odesílaných paketů (nejběžnější jsou 64 B velké).

- Zjistěte pokusy, jak maximálně velký datový paket lze odeslat pomocí PING. (Větší už neprojdou sítí a tedy na ně nepřijde odpověď). Zdůvodněte velikost limitů.
- nápověda: ping -h, ping --help nebo man ping

5. Příkaz traceroute - zjistí cestu k danému serveru, tedy směrovače, které jsou po cestě.
   - Proveďte trasovaní k www.zoznam.sk.
   - Odhadněte cestu, kudy data prochází. Využijte k tomu web společnosti Ripe NCC, kde můžete zadat libovolnou Evropskou adresu a databáze Vám vrátí záznam, komu IP adresa patří a jakou má adresu.
   - nápověda: traceroute, traceroute --help nebo man traceroute

Elaborát zpracujte do šablony v záhlaví kruzu, odevzdávejte v souladu instrukcemi (formát PDF, pojmenování, etc.).

Pro v případě nutnosti vzdáleného připojení do učebny A3 využijte návod.

Virtuální počítač, pokud je na stanicích spuštěn, je přístupný na IP adrese 192.168.56.100, jméno student, heslo 123456TUL.

Příkazy ip a ss jsou moderními variantami některých výše uvedených příkazů, které jsou považovány za zastaralé, nicméně stále jsou využívány.

Postup

Úloha 1

Ip a	1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever
ifconfig	lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 64 bytes 5536 (5.4 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 64 bytes 5536 (5.4 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
popis	Loopback – odkaz na sebe, často používán pro testování a simulování síťového provozu

Ip a	2: p2p1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000 link/ether b4:96:91:26:1a:60 brd ff:ff:ff:ff:ff:ff
ifconfig	p2p1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 ether b4:96:91:26:1a:60 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device memory 0xee100000-ee1fffff
popis	Interní síťová karta bez připojeného kabelu, nejspíš používané pro připojení do LAN v učebně.

Ip a	3: enp0s31f6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000 link/ether 54:bf:64:62:cb:a1 brd ff:ff:ff:ff:ff:ff inet 147.230.78.90/21 brd 147.230.79.255 scope global noprefixroute dynamic enp0s31f6 valid_lft 39175sec preferred_lft 39175sec inet6 fe80::7ffe:8963:bc14:f9ce/64 scope link tentative noprefixroute dadfailed valid_lft forever preferred_lft forever inet6 fe80::6671:3582:2c7e:c8ac/64 scope link tentative noprefixroute dadfailed valid_lft forever preferred_lft forever inet6 fe80::53df:8fde:4335:467/64 scope link tentative noprefixroute dadfailed valid_lft forever preferred_lft forever
ifconfig	enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 147.230.78.90 netmask 255.255.248.0 broadcast 147.230.79.255 inet6 fe80::7ffe:8963:bc14:f9ce prefixlen 64 scopeid 0x20<link> inet6 fe80::6671:3582:2c7e:c8ac prefixlen 64 scopeid 0x20<link> inet6 fe80::53df:8fde:4335:467 prefixlen 64 scopeid 0x20<link> ether 54:bf:64:62:cb:a1 txqueuelen 1000 (Ethernet) RX packets 1164092 bytes 175963882 (167.8 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 177022 bytes 175877123 (167.7 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device interrupt 20 memory 0xee300000-ee320000
popis	Ethernetová interní síťová karta, dle inet: 147.230.78.90 se dá předpokládat, že je připojena do LIANE sítě

Ip a	4: wlp2s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000 link/ether 56:ec:8b:af:d7:a1 brd ff:ff:ff:ff:ff:ff
ifconfig	wlp2s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 ether 56:ec:8b:af:d7:a1 txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
popis	Wi-Fi karta

Ip a	5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:ee:b3:da:d7 brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 scope global docker0 valid_lft forever preferred_lft forever
ifconfig	docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 172.17.0.1 netmask 255.255.0.0 broadcast 0.0.0.0 ether 02:42:ee:b3:da:d7 txqueuelen 0 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
popis	Virtuální můstek který si vytvořil Docker

Ip a	6: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000 link/ether 52:54:00:b8:63:ee brd ff:ff:ff:ff:ff:ff inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0 valid_lft forever preferred_lft forever
ifconfig	virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255 ether 52:54:00:b8:63:ee txqueuelen 1000 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
popis	Virtuální můstek používaný pro překlad síťových adres (NAT)

Ip a	7: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast master virbr0 state DOWN group default qlen 1000 link/ether 52:54:00:b8:63:ee brd ff:ff:ff:ff:ff:ff
Ifconfig	
Popis	Virtuální můstek mezi fyzickou síťovou kartou a síťovou kartou virtuálních počítačů (VM)

Mezi příkazy jsou pouze minimální rozdíly. Největším rozdílem je, že ifconfig nám umí také vyslat packety a zjistit, zda je síťové připojení bez chyb. Ifconfig také nezobrazuje virbr0-nic, nejspíš je to způsobeno tím, že virbr0 je v ip a označen jako master.

Úloha 2

Ip n	147.230.77.233 dev enp0s31f6 lladdr 10:98:36:a2:75:fb REACHABLE
Arp	share.nti.tul.cz ether 10:98:36:a2:75:fb C enp0s31f6
Výrobce	Dell Inc.

Ip n	147.230.72.250 dev enp0s31f6 lladdr d0:c7:89:a9:d2:80 STALE
Arp	router-b.tul.cz ether d0:c7:89:a9:d2:80 C enp0s31f6
Výrobce	Cisco Systems, Inc

Ip n	147.230.77.30 dev enp0s31f6 lladdr 10:65:30:d6:2c:d6 STALE
Arp	dockms.nti.tul.cz ether 10:65:30:d6:2c:d6 C enp0s31f6
Výrobce	Dell Inc.

Ip n	fe80::d2c7:89ff:fea9:d280 dev enp0s31f6 lladdr d0:c7:89:a9:d2:80 router STALE
Arp	
Výrobce	Cisco Systems, Inc

Zdá se, že příkaz ip n vypisuje jak ipv4 tak ipv6 záznamy a arp pouze ipv4. To by vysvětlovalo, proč nevypisuje pro poslední ze záznamů.

Úloha 3

Ss -tudw

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
tcp	ESTAB	0	0	147.230.78.83:42304	147.230.18.154:ldaps
tcp	ESTAB	0	0	147.230.78.83:42302	147.230.18.154:ldaps
tcp	ESTAB	0	0	147.230.78.83:42308	147.230.18.154:ldaps
tcp	ESTAB	0	0	147.230.78.83:42310	147.230.18.154:ldaps
tcp	ESTAB	0	0	147.230.78.83:hyperwave-isp	147.230.77.233:nfs
tcp	ESTAB	0	0	147.230.78.83:42306	147.230.18.154:ldaps
tcp	ESTAB	0	192	147.230.78.83:ssh	147.230.11.47:53088

Netstat -tudw

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	a0312.nti.tul.cz:42304	ldap-proxy.nti.tu:ldaps	ESTABLISHED
tcp	0	0	a0312.nti.tul.cz:42302	ldap-proxy.nti.tu:ldaps	ESTABLISHED
tcp	0	0	a0312.nti.tul.cz:42308	ldap-proxy.nti.tu:ldaps	ESTABLISHED
tcp	0	0	a0312.nti.tul.cz:42310	ldap-proxy.nti.tu:ldaps	ESTABLISHED
tcp	0	0	a0312.nti:hyperwave-isp	share.nti.tul.cz:nfs	ESTABLISHED
tcp	0	0	a0312.nti.tul.cz:42306	ldap-proxy.nti.tu:ldaps	ESTABLISHED
tcp	0	200	a0312.nti.tul.cz:ssh	vpn047.tul.cz:53088	ESTABLISHED

Zdá se, že většina komunikace probíhá v síti LIANE.

Ss -tuwl

```
Netid  State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
raw    UNCONN     213504 0           [::]:ipv6-icmp              [::]:*
udp    UNCONN     0      0        127.0.0.1:323                 *:*
udp    UNCONN     0      0             *:hmmp-op                *:*
udp    UNCONN     0      0             *:58911                  *:*
udp    UNCONN     0      0             *:mdns                   *:*
udp    UNCONN     0      0     192.168.122.1:domain                    *:*
udp    UNCONN     0      0        *%virbr0:bootps                 *:*
udp    UNCONN     0      0             *:bootpc                 *:*
udp    UNCONN     0      0             *:sunrpc                 *:*
udp    UNCONN     0      0           [::1]:323                  [::]:*
udp    UNCONN     0      0           [::]:hmmp-op               [::]:*
udp    UNCONN     0      0           [::]:sunrpc                [::]:*
tcp    LISTEN     0      100      127.0.0.1:smtp                  *:*
tcp    LISTEN     0      128           *:sunrpc                 *:*
tcp    LISTEN     0      5     192.168.122.1:domain                    *:*
tcp    LISTEN     0      128           *:ssh                    *:*
tcp    LISTEN     0      128      127.0.0.1:ipp                   *:*
tcp    LISTEN     0      100         [::1]:smtp                 [::]:*
tcp    LISTEN     0      128         [::]:sunrpc                [::]:*
tcp    LISTEN     0      128         [::]:ssh                   [::]:*
tcp    LISTEN     0      128         [::1]:ipp                  [::]:*
```

Netstat -tuwl

```
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 localhost:smtp         0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:sunrpc         0.0.0.0:*              LISTEN
tcp        0      0 a0312.nti.tul.cz:domain 0.0.0.0:*             LISTEN
tcp        0      0 0.0.0.0:ssh            0.0.0.0:*              LISTEN
tcp        0      0 localhost:ipp          0.0.0.0:*              LISTEN
tcp6       0      0 localhost:smtp         [::]:*                 LISTEN
tcp6       0      0 [::]:sunrpc            [::]:*                 LISTEN
tcp6       0      0 [::]:ssh               [::]:*                 LISTEN
tcp6       0      0 localhost:ipp          [::]:*                 LISTEN
udp        0      0 localhost:323          0.0.0.0:*
udp        0      0 0.0.0.0:hmmp-op        0.0.0.0:*
udp        0      0 0.0.0.0:58911          0.0.0.0:*
udp        0      0 0.0.0.0:mdns           0.0.0.0:*
udp        0      0 a0312.nti.tul.cz:domain 0.0.0.0:*
udp        0      0 0.0.0.0:bootps         0.0.0.0:*
udp        0      0 0.0.0.0:bootpc         0.0.0.0:*
udp        0      0 0.0.0.0:sunrpc         0.0.0.0:*
udp6       0      0 localhost:323          [::]:*
udp6       0      0 [::]:hmmp-op           [::]:*
udp6       0      0 [::]:sunrpc            [::]:*
raw6  213504      0 [::]:ipv6-icmp         [::]:*
```

Pomocí přepínače -n lze zkontrolovat, čísla portů. Všechny porty krom 58911 jsou vyhrazené, například smtp (Simple Mail Transfer Protocol) slouží pro přenos elektronické pošty. Používá se pro odchozí poštu. ssh (Secure SHell) slouží pro šifrovanou komunikaci mezi sítěmi. Například vzdálené připojení k počítači. Ipv6-icmp (Internet Control Message Protocol for IPv6) – protokol požívaný pro diagnostiku sítě. Příkladem mohou být příkazy ping.

Ss -s	Total: 687 (kernel 0) TCP: 17 (estab 7, closed 1, orphaned 0, synrecv 0, timewait 0/0), ports 0 Transport Total IP IPv6 * 0 - - RAW 1 0 1 UDP 11 8 3 TCP 16 12 4 INET 28 20 8 FRAG 0 0 0
Netstat -s příklad	Tcp: 2145 active connections openings 6 passive connection openings 87 failed connection attempts 25 connection resets received 7 connections established 463408 segments received 740480 segments send out 2617 segments retransmited 0 bad segments received. 734 resets sent

Jelikož netstat -s vypisuje asi dvě stránky výpisu, dovolil jsem si ho zkrátit pouze na TCP výstup. Ss -s je rozhodně lépe čitelnější. Jediná věc, kterou mají oba výše uvedené výpisy společné, je počet established připojení TCP.

Úloha 4

server	Počet odeslaných packetů	Ztracené packety	Průměrná odezva [ms]	Maximální velikost packetu [B]
www.tul.cz (147.230.18.195)	32	0	0.384	65507 (65535)
www.seznam.cz (77.75.75.172)	32	0	4.043	65507 (65535)
www.google.com (142.251.36.67)	32	0	3.789	1472 (1500)
www.facebook.com (157.240.30.18)	32	0	3.827	1472 (1500)

Zdá se, že tul a seznam mají omezenou velikost pingu pouze příkazem ping. Naopak google a facebook byly omezeny na 1500 B a google navíc neposílal zpět packety stejné velikosti ale pouze 76 B. Google a facebook (Meta) jsou na rozdíl od TUL a seznamu mnohem větší cíle pro internetové darebáky a tedy dává perfektní smysl proč by jejich ochrana vůči vnějšímu světu byla větší.

Úloha 5

IP adresa	Adresa	vlastník
147.230.72.250	Liberec	Technicka univerzita v Liberci
147.230.250.18	Liberec	Technicka univerzita v Liberci
147.230.250.49	Liberec	Technicka univerzita v Liberci
195.113.235.99	Praha 6	CESNET z.s.p.o.
91.210.16.23	CZ	NIX.CZ z.s.p.o.
87.197.252.238	SK	Slovak Telecom, a. s.
213.81.185.168	Bratislava	Slovak Telecom, a. s.

Data prochází z našeho počítače do LIANE ze které putují do Prahy do CESNETu. Pokračují do NIX.CZ (sdružení internet service providerů v čr) odkud jsou poslány do Slovenska. Nakonec by měli skončit v Bratislavě na www.zoznam.sk, to nám ale traceroute již nepoví. Zdá se, že traceroute implicitně používá UDP porty a je možné, že ty jsou na zoznamu zablokovány.

Závěr

Postup pro všechny úlohy byl v podstatě

- *podívat se do dokumentace*
- *spustit příkaz s nějakými přepínači*
- *zkopírovat výstup*
- *analyzovat výstup s pomocí google*

Nejvíce času rozhodně zabrala 3.úloha zabývající se příkazy ss a netstat. S největší pravděpodobností to bude tím, že k ostatním byly zadány přepínače a že jsem s nimi ve větší míře dříve pracoval.