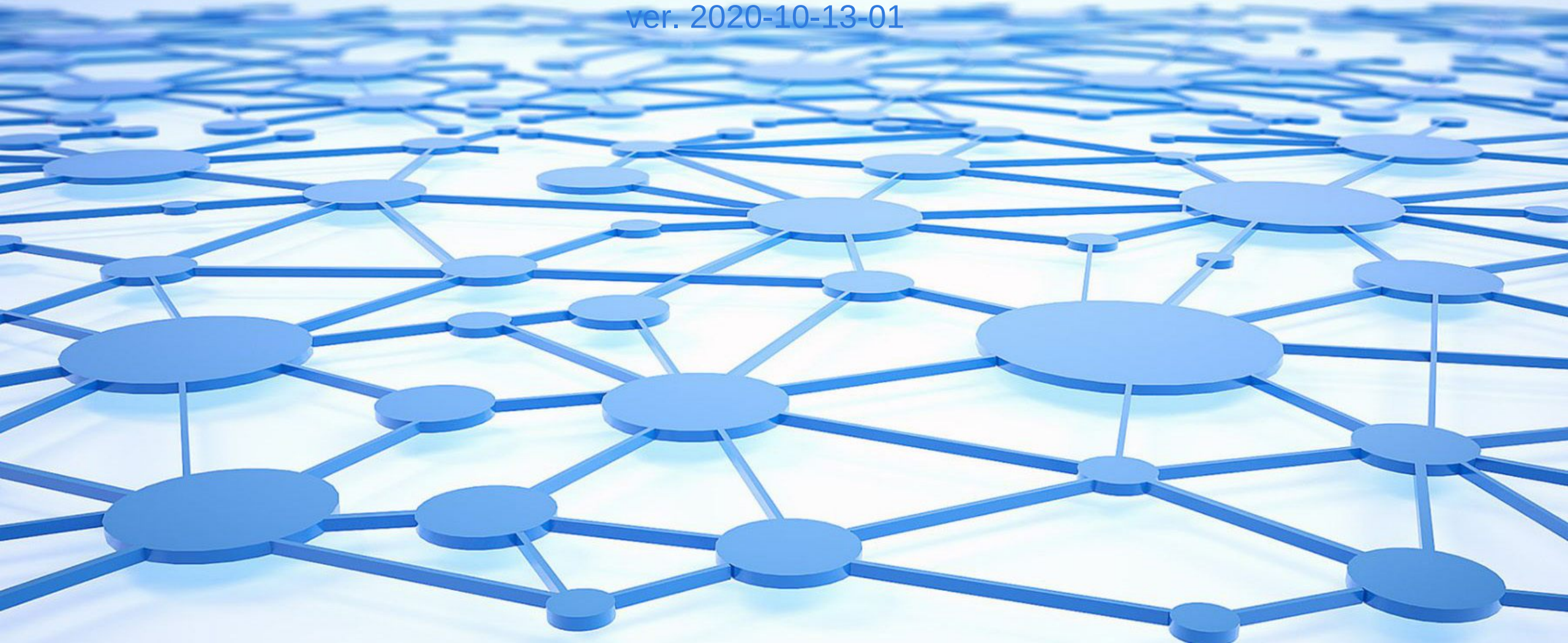


Úvod do počítačových sítí

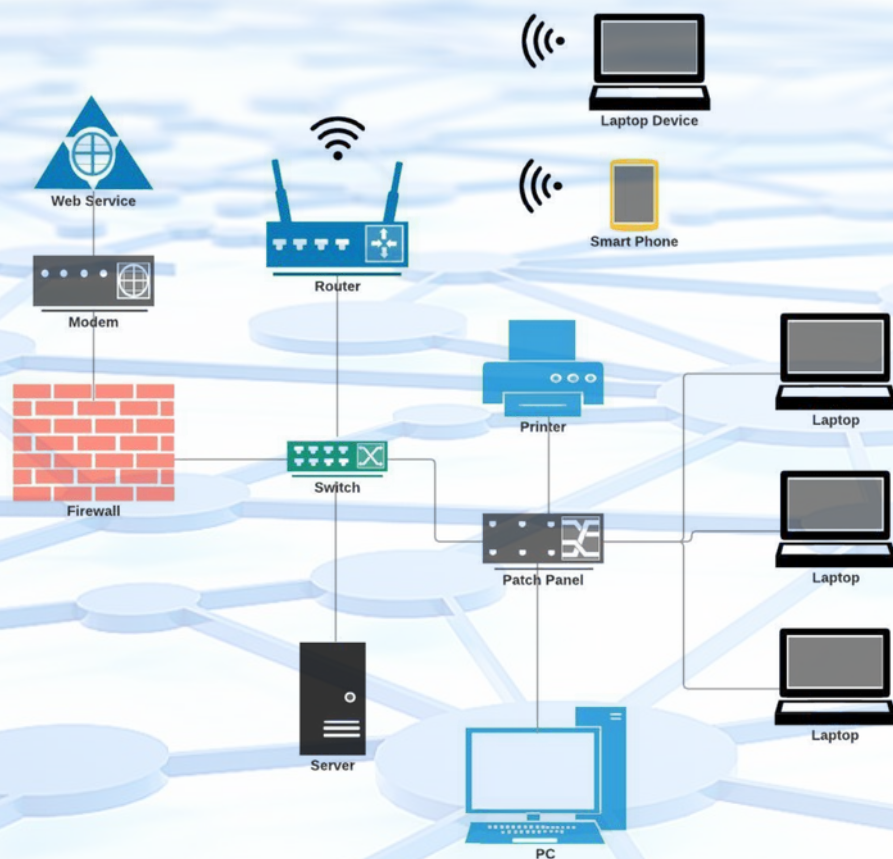
Přednáška 2

(2021/2022)

ver. 2020-10-13-01



Opakování: Běžná počítačová síť

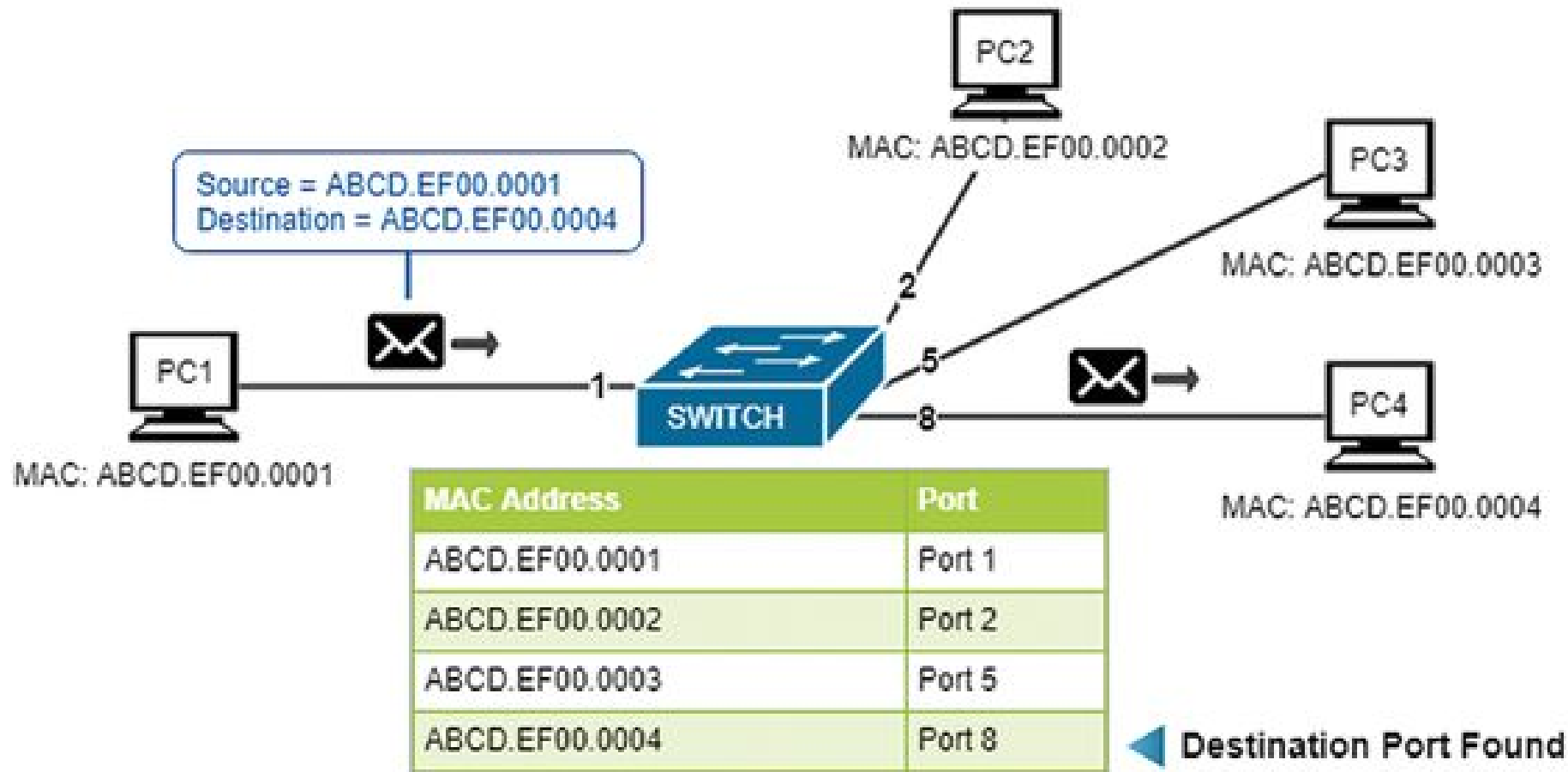


Zdroj: <https://www.itjones.com/blogs/2020/3/15/how-to-build-a-computer-network-for-your-small-business-part-1-the-basics>

Adresace zařízení v LAN (L2)

- Každé zařízení v LAN má svoji fyzickou adresu - MAC
- „Napevno“ spojena s konkrétním zařízením
 - Dnes už v ethernetu změnit jde, ale ve většině případů to není nutné ani vhodné
- V rámci jedné LAN musí být unikátní
- Šest dvojčiferných hexa čísel(48 bitů) – např 00:08:60:00:63:c9
 - První tři dvojice se označují jako VendorID a identifikují výrobce
 - Další tři trojice jsou volitel výrobcem – ale pořadí v rámci LAN musí být unikátní
- Speciální adresa – FF:FF:FF:FF:FF
 - Jedná se o broadcast – rámec s touto adresou bude doručen všem
 - V případě vytvoření smyčky může způsobit „broadcastovou“ bouři
- Pokud není v rámci LAN dodržena unikátnost MAC adres provoz začne „flapovat“
 - Část zařízení v síti komunikuje s jedním zařízením se stejnou MAC a jiná část s druhou
 - Tento stav se průběžně mění jak zařízení komunikují

Adresace zařízení v LAN – tabulka adres pro switch



Adresace zařízení v LAN – IP (L3)

- Nejběžněji se dnes používá protokol IP
 - IPv4 – délka adresy 32bitů
 - IPv6 – délka adresy 128 bitů
 - Délka není jediný rozdíl, IPv6 není zatím masivně využíváno
- Každé zařízení má alespoň jednu IP adresu, kterou se identifikuje v síti
- Má délku 32 bitů, příklad 69.89.31.226, celkem jich je 4 294 967 296
- IPv4 sítě se dle práce s IPv4 adresou rozdělují na:
 - Classfull
 - Používají jen třídy IP adres
 - Classless
 - Nepoužívají třídy IP adres, ale CIDR

69 . 89 . 31 . 226

↓ ↓ ↓ ↓

01000101 . 01011001 . 00011111 . 11100010

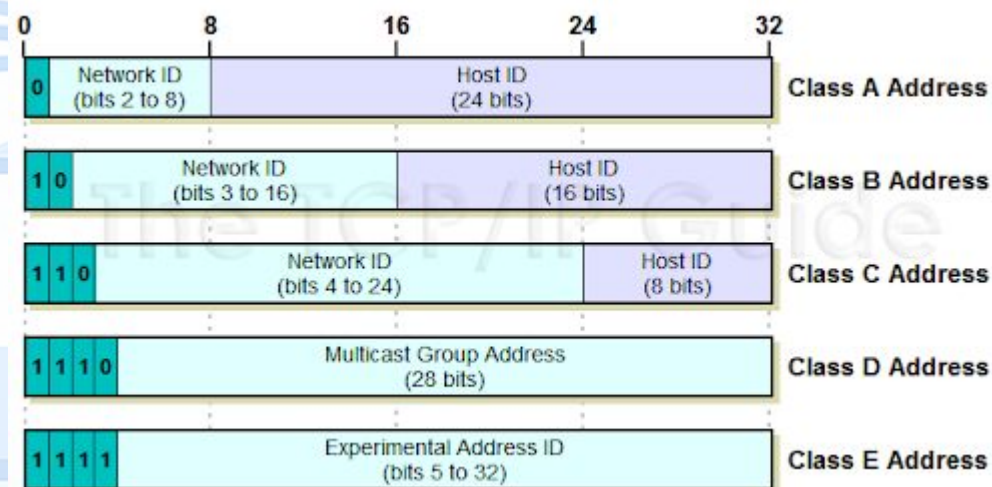
1st Octet 2nd Octet 3rd Octet 4th Octet

IPv4 Ip address (32 bits)

zdroj: <https://static.thegeekstuff.com>

IPv4 – třídy adres

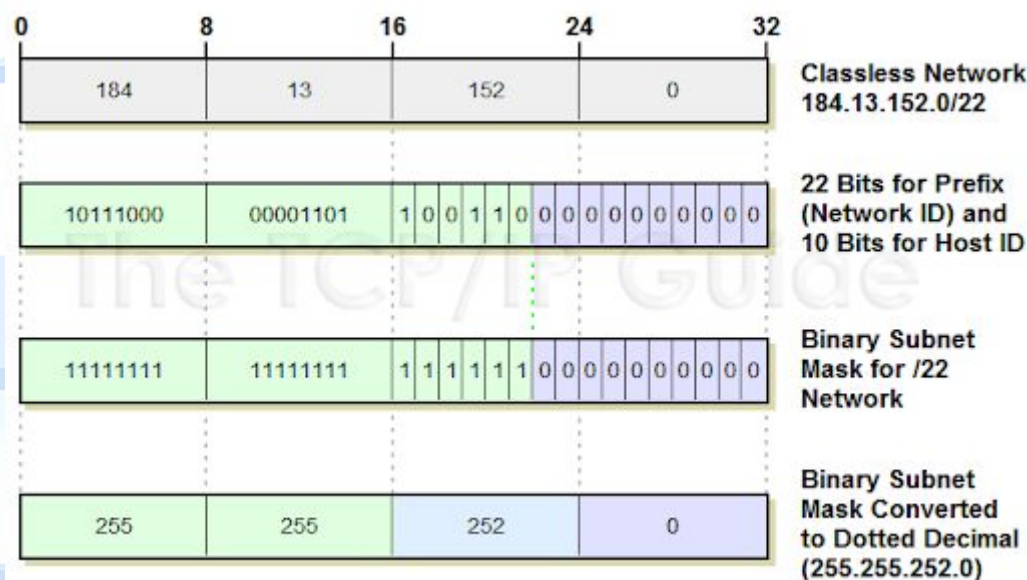
- Třídy adres definují adresní prostory a jsou přímo spjaté s „prefixem“ IP adresy
- Dnes už se příliš nepoužívá
- Třída A (0.0.0.0 – 127.255.255.255)
 - Masky /8, až 16 777 214 stanic v každé síti
- Třída B (128.0.0.0 – 191.255.255.255)
 - Masky /16, až 65 534 stanic v každé síti
- Třída C (192.0.0.0 – 223.255.255.255)
 - Masky /24, až 254 stanic v každé síti
- Třída D (224.0.0.0 – 239.255.255.255)
 - skupinové směřování - multicast
- Třída E (240.0.0.0 – 255.255.255.255)
 - Experimentální použití



zdroj: <https://http://www.tcpipguide.com>

IPv4 – CIDR

- CIDR - Classless Inter-Domain Routing, síť je daná maskou sítě, která není vázaná na IP adresu
- Dovoluje jemnější tvorbu podsítí
- Dnes již téměř kompletně nahradilo používání tříd
- Masky sítě - definuje kolik bitů zleva je pro danou síť fixních a kolik může libovolně použít
 - Spolu s IP a bránou tvoří základní konfigurační parametry IP sítě
 - Pomocí masky definuje:
 - Adresu sítě – nejnižší adresa v síti
 - 10.0.0.0/8 → 10.0.0.0
 - Adresu broadcastu – nejvyšší adresa v síti
 - 10.0.0.0/8 → 10.255.255.255
 - POZOR brána a maska spolu přímo nesouvisí !!!
 - Na základě IP a masky nejde určit bránu



IPv4 – privátní a speciální adresy



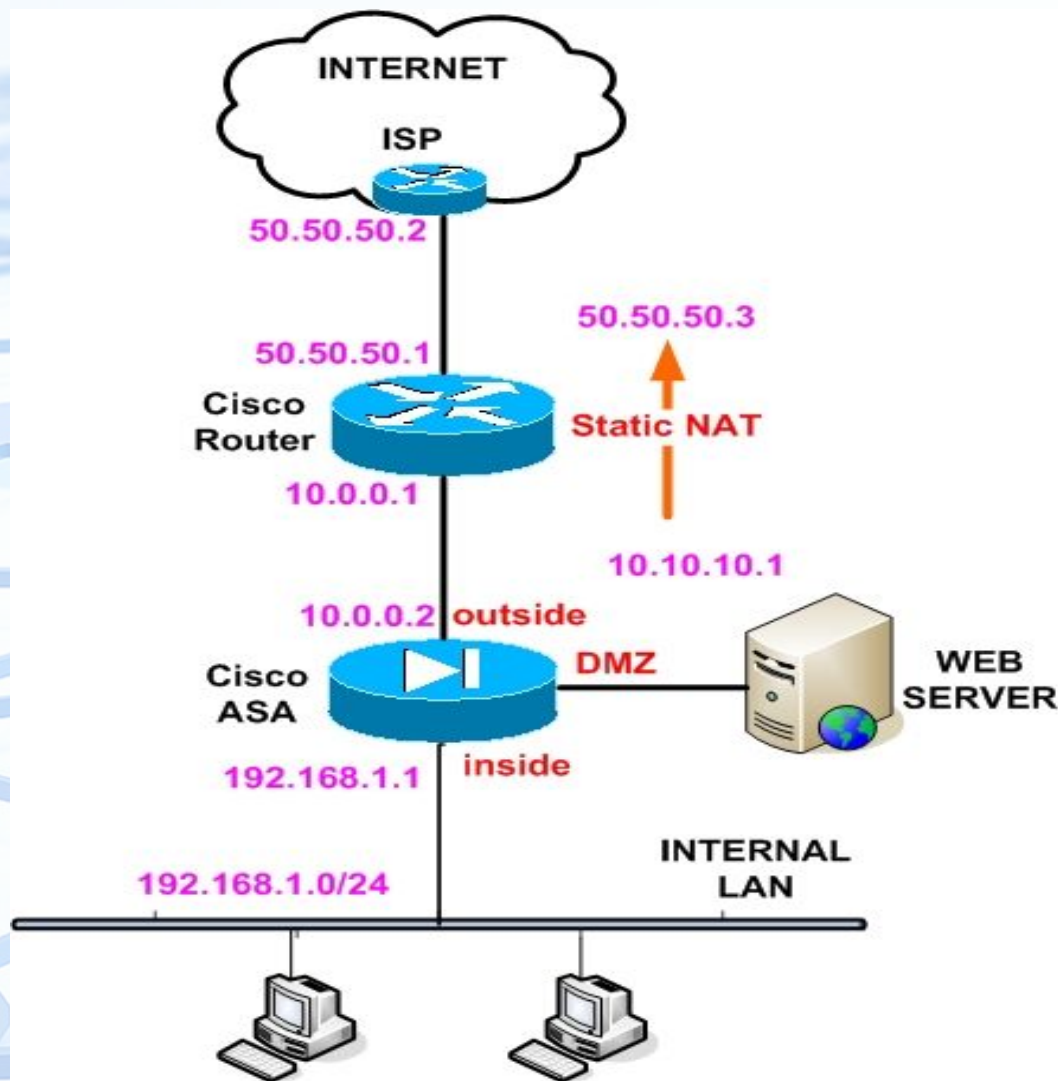
- Loopback
 - 127.0.0.1/8
 - Virtuální lokální interface
 - Je v každém zařízení a není nikdy dostupný z dalšího zařízení
- Privátní adresy
 - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
 - Adresy použité v lokálních sítích, které se následně pro provoz v Internetu překládají na veřejné pomocí NAT
 - Routery v internetu by měly blokovat provoz z veřejných IP na privátní
 - Tyto rozsahy nejsou nikde ve veřejném internetu použity
- IPv4 Prefix for Shared Address Space
 - 100.64.0.0/10
 - Adresy vyhrazené pro velké operátory a jejich interní komunikaci
 - Potřeba na interních sítích směřovat veřejné rozsahy

IPv4 - NAT



- NAT - Network address translation
- Mechanismus umožňující překlad adres při přechodu firewallem/routerem
- Typicky se používá při překladu privátních adres na veřejné
- Při přechodu NAT se zdrojová adresa nahradí veřejnou adresou routeru a zdrojový port náhodným VOLNÝM portem a toto mapování se zaznamená do NAT tabulky
- Pakety jde internetem a zpět se adresou routeru, po návratu odpovědi na router je proveden zpětný překlad na původní hodnoty na základě údajů z NAT tabulky a paket je poslán dál do LAN

IPv4 - NAT - příklad



Směrování dat v síti (L3)

- Pokud chce komunikovat s dalším zařízením, pošle do sítě paket, který obsahuje mimo jiné zdrojovou, cílovou adresu a data
- Zdrojová adresa se nastaví sama na zařízení, které zahajuje komunikaci
- Cílová adresa je nastavena aplikací a určuje s kým chceme komunikovat
- Směrování v síti se řídí cílovou adresou a o jeho směrování rozhoduje směrovací tabulka
- Směrovací tabulka může být v routeru, PC nebo serveru
- Pokud žádný záznam ve směrovací tabulce nevyhovuje, použije se výchozí brána – default gateway
- Směrovací tabulka v základu obsahuje:
 - Adresu sítě - destination
 - Masku sítě - netmask
 - Bránu – gateway
 - 0.0.0.0 – výchozí brána
 - Rozhraní – interface
- Směrování probíhá autonomně
 - Každý jeden směrovač rozhoduje sám za sebe
 - Dva pakety mezi stejným zdrojem a cílem mohou jít různými cestami

```
root@fedora10:~  
[root@fedora10 ~]# netstat -nr  
Kernel IP routing table  
Destination      Gateway          Genmask         Flags   MSS Window  irtt  Iface  
60.49.199.72     0.0.0.0         255.255.255.248 U        0 0        0 eth1  
172.16.163.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.162.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.161.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.160.0     0.0.0.0         255.255.255.0   U        0 0        0 eth0  
172.16.167.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.166.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.165.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.164.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.170.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.169.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
172.16.168.0     172.16.160.1   255.255.255.0   UG        0 0        0 eth0  
169.254.0.0      0.0.0.0         255.255.0.0     U        0 0        0 eth0  
169.254.0.0      0.0.0.0         255.255.0.0     U        0 0        0 eth1  
0.0.0.0          60.49.199.73   0.0.0.0         UG        0 0        0 eth1  
[root@fedora10 ~]#
```

„Základní/obslužné“ protokoly internetu

- Jedná se protokoly a na ně navázané služby, které často používáme „mimoděk“ a o jejich existenci často ani nevíme
- Mohou se na různých vrstvách sítě a využívat jak rámců (např ARP, DHCP), tak paketů (DNS, ICMP)
- Příklady nejběžnějších jsou
 - ARP
 - Mapování MAC na IP a obráceně
 - DHCP
 - Automatická konfigurace sítě
 - DNS
 - Mapování doménových jmen na IP a obráceně
 - ICMP
 - Diagnostika a notifikace stavu sítě

Základní protokoly: ARP

- ARP - Address Resolution Protocol
- Protokol sloužící k zjišťování a mapování IP adresy na MAC a opačně
 - Nejčastěji je ARP vázán na IP a Ethernet, ale je postaven obecněji a může fungovat i v jiných sítích
 - Plní ARP tabulku
- Záznam je do tabulky také možné vložit ručně nebo ARP protokolem
 - Ruční záznam má typicky neomezenou platnost
 - Dynamický záznam je platný je krátký čas typicky 30-60s

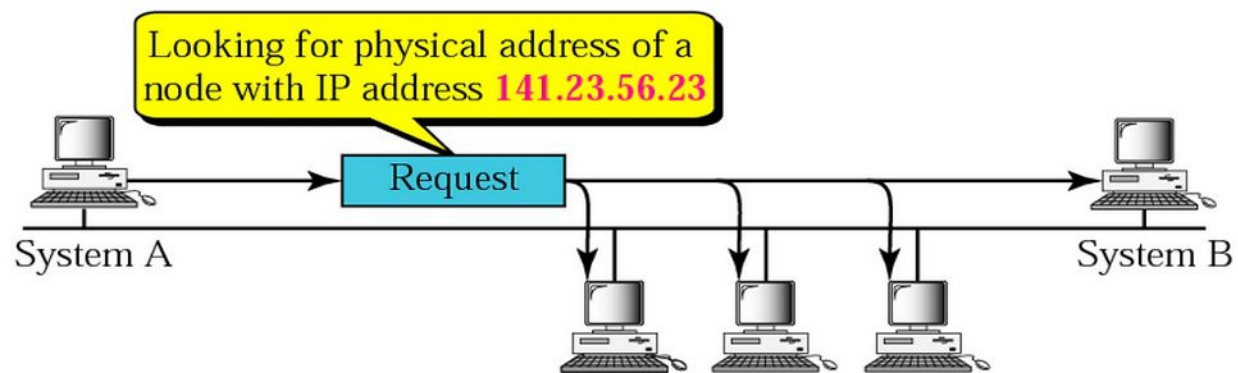
```
login as: admin
Using keyboard-interactive authentication.
Password:
Bad terminal type: "xterm". Will assume vt100.
Router>
Router>
Router>
Router> show arp-table
```

Address	HWtype	HWaddress	Flags	Mask	Iface
210.210.3.1	ether	90:6C:AC:2D:DE:9A	C		wan1
10.10.10.40	ether	00:1E:67:52:E5:B6	C		lan1
10.10.10.50		(incomplete)			lan1
10.10.10.30	ether	00:1E:67:52:E5:CE	C		lan1
10.10.10.45	ether	00:1E:67:52:E9:28	C		lan1
10.10.10.100	ether	00:1E:67:3B:1E:E0	C		lan1
10.10.10.120	ether	00:1E:67:3B:22:D2	C		lan1
210.210.3.39	*	<from_interface>	MP		wan1

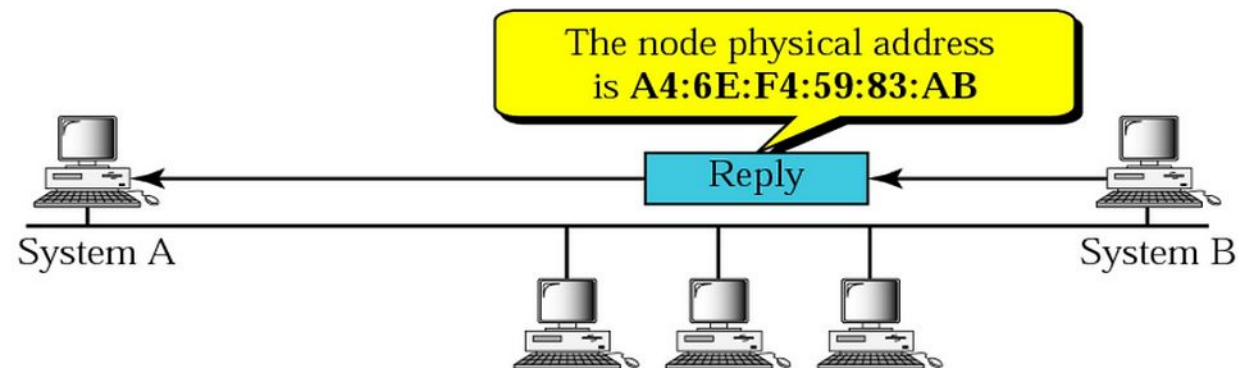
```
Router>
```

Základní protokoly: ARP - schéma

- Princip fungování
 - Pokud stanice potřebuje komunikovat s nějakou IP v LAN, pošle broadcastový rámec(FF:FF:FF:FF:FF:FF) s dotazem na MAC pro IP, se kterou chce komunikovat
- Všechny stanice v dané síti
 - limitované routerem
 - zprávu přijmou a stroj, který danou IP má odpoví tazateli dalším rámcem, kde je uvedena požadovaná MAC
- Může odpovědět i více stanic
 - to je problém a nastává pokud má více stanic stejnou IP
- Aby nebylo nutné dotazování před odesláním každého rámce ARP odpovědi se dočasně uchovávají v ARP tabulce
- Tato tabulka má dočasné záznamy a např po 30 jsou smazány a proces se opakuje



a. ARP request is broadcast

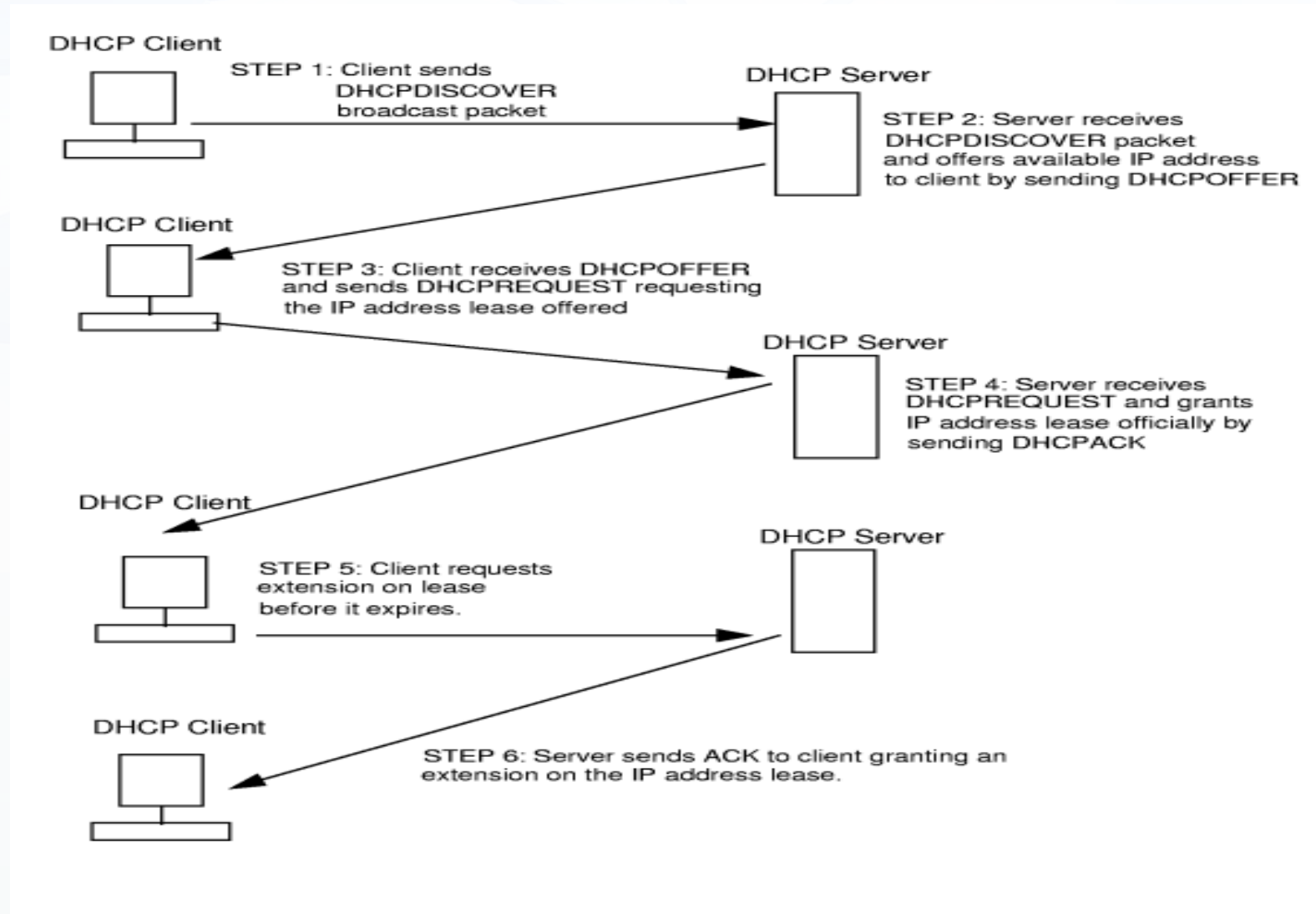


b. ARP reply is unicast

Základní protokoly: DHCP

- DHCP - Dynamic Host Configuration Protocol
 - Vychází ze staršího BOOTP protokolu, se kterým není zpětně kompatibilní a který se dne už nepoužívá
- Možnost dynamické konfigurace síťových zařízení
- IP adresy je možné přidělovat ručně
 - V malých sítích typické a není s tím problém
- Problém nastává ve velkých sítích (mnoho stanic) a při častých změnách konfigurace sítě – administrativně náročné až nemožné
- Základní myšlenka je „auto“ konfigurace zařízení po připojení k počítačové síti
- Základní princip
 - Nemám IP, ale mám MAC => mohu komunikovat v rámci LAN (broadcastem například)
 - Pošlu rámec s dotazem, zda někdo neví jak se mám na konfigurovat
 - Pokud v síti poslouchá nějaký DHCP server, dotaz přijme a v odpovědi pošle možnou konfiguraci
 - Konfigurace má omezenou platnost, po uplynutí poloviny intervalu se žádá o prodloužení
 - Ač to není běžné, odpovědět může serverů více => vyberu si první odpověď
 - Typický problém s defaultní konfigurací AP – dělají další „nepožadovaný“ DHCP server

Základní protokoly: DHCP – princip komunikace



Základní protokoly: DHCP – předávané informace

- Základní – potřebné pro fungování sítě
 - IP adresa
 - Maska
 - Brána
 - DNS server / servery
- Rozšiřující – nemusí být předávané, ale mohou zpřesňovat nastavení nebo konfigurovat další služby
 - NTP – časové servery
 - Wins, Active Directory doména – rozšířená konfigurace Windows stanic
 - NFS root / boot image – konfigurace pro boot bezdiskových stanic

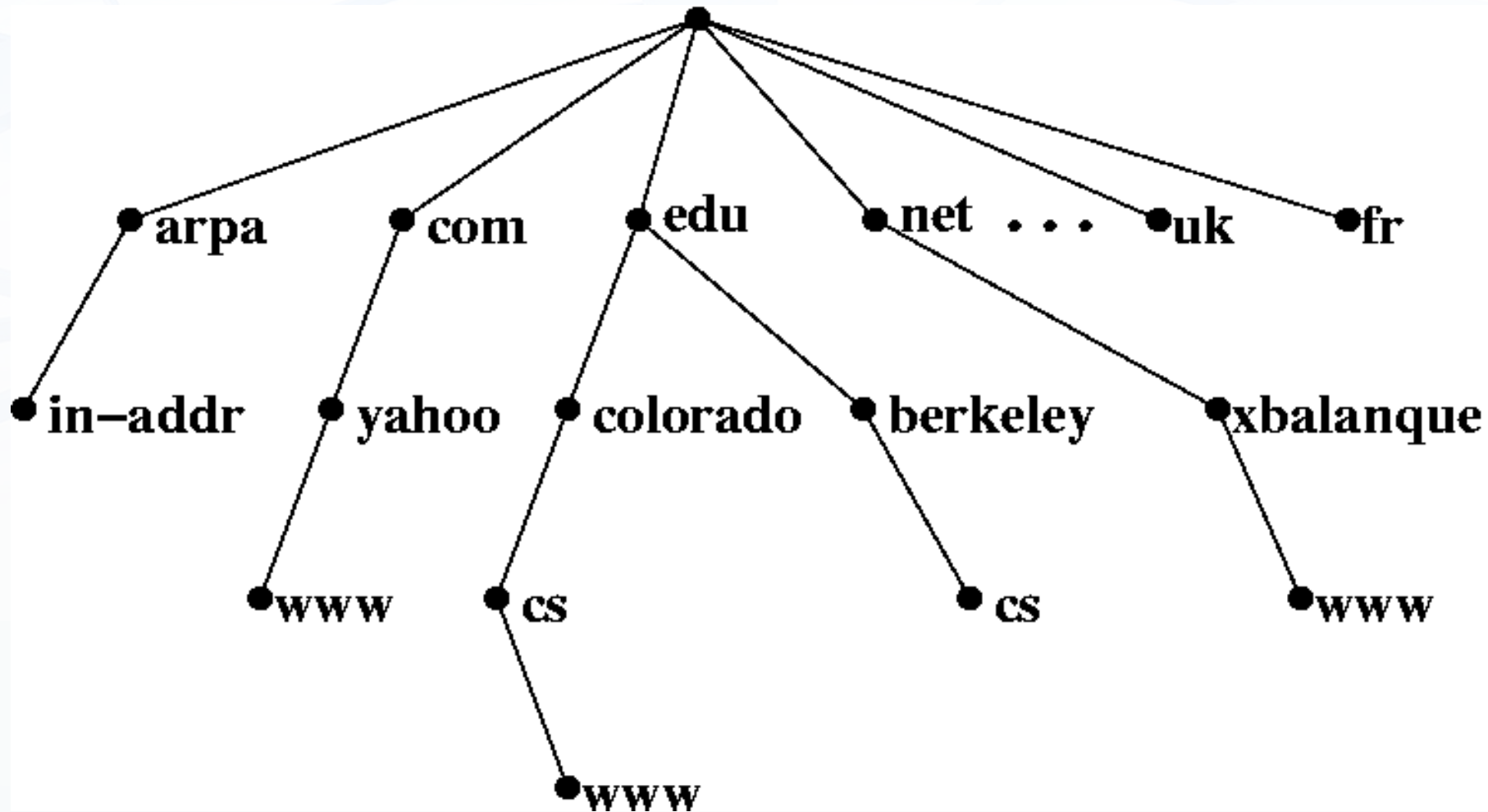
Základní protokoly: DHCP – typy přidělené adresy

- Dynamické
 - Máme pool adres – 147.228.63.10-147.228.63.100 a z nich přidělíme jednu volnou
 - Do interní databáze se zaznamená MAC požadavku a přidělená IP
 - Pokud to jde, snažíme se stejné MAC přidělovat stále stejnou IP
 - Pokud volné IP dojdou jsou dočasné rezervace rušené a recyklované
 - Šetříme nutný počet adres – firma má 90 zaměstnanců a třísměnný provoz => potřebují naráz jen 30 IP
 - Typicky pro koncové stanice zařízení ,kde potřebují IP, ale je jedno jakou
- Statická rezervace
 - Dynamické přidělování se nehodní pro zařízení poskytující obsah
 - Servery, tiskárny,
 - Do DHCP databáze provedu statickou rezervaci definicí vazby IP a MAC
 - Daná MAC VŽDY dostane stejnou IP
 - Staticky přidělené IP jsou vyjmuté z dynamického poolu

Základní protokoly: DNS

- DNS - Domain Name System
- Slouží k převodu jména na IP a opačně
 - `www.kiv.zcu.cz` => `147.228.63.11`
 - `147.228.63.11` => `proteus.fav.zcu.cz` (reverzní záznam)
- Jeden z „nejdůležitějších“ aplikačních protokolů Internetu
 - Pro většinu lidí platí, že pokud nejde DNS nejde Internet
- Ovlivňuje chování dalších protokolů a služeb (např WWW nebo email)
- Některé služby se přes DNS i konfiguruji (DKIM, SPF, Windows Active Directory, ...)
- Jedná se o decentralizovaný systém
 - Výrazně se tím zvyšuje odolnost systému jako celku
- Hierarchický model oddělovaný „tečkami“ a začínající „neviditelnou“ tečkou vpravo
 - www.kiv.zcu.cz.
 - MAX 63 znaků na 1 úrovni, max. délka 255 znaků celkem, MAX 127 úrovní stromu

Základní protokoly: DNS - schéma



Základní protokoly: DNS – kořenové servery

- 13 kořenových jmenných(name) serverů rozmístěných po celém světě
- Obsahují informace o kořenových doménách (.cz .de .org)
- Kritické a velmi hlídané stoje
- Serverů není fyzicky 13, ale jsou spuštěny násobně v X instancích
 - Důvodem je redundance, stabilita a rychlost odezvy v dané lokalitě
- Kompletní seznam a info na <https://www.root-servers.org>
- Delegují odpovědi na jednotlivé správce národních a dalších domén
 - Například CZ.NIC pro .cz
- Sice se můžeme vždy ptát kořenových name-serverů, ale výhodnější je dotaz na nejbližší DNS – DNS ISP – který může odpovědět výrazně rychleji

Základní protokoly: DNS – kořenové servery - mapa



zdroj: <https://coednssecurity.in>

Základní protokoly: DNS – role serverů

- Primární
 - Obsahuje primární info o doméně
 - Slouží jako zdroj pro sekundární server
 - Je autoritativní pro své domény
- Sekundární
 - Přebírá info od domény od primárního
 - Cyklicky nebo na vyzvání
 - Je autoritativní pro své domény
 - Neprovádí se zde změny záznamů
 - Aby nevznikal problém s konzistencí mezi primárním a sekundárním serverem
- Pomocný / cachovací
 - Nemá vlastní doménu
 - Slouží jako cache – snižuje datový trafik a zrychluje odpověď klientovi
 - Zná kořenové servery nebo referery, kterých se ptá pokud odpověď nezná
- Jedna instance může kombinovat všechny role / typy serverů

Základní protokoly: DNS – typy záznamů

- DNS je vlastně databáze a má několik základních „datových“ typů
 - A
 - Obsahuje IP adresu, proteus.fav.zcu.cz => 147.228.63.11
 - Jedna IP by měla mít jen jeden A záznam
 - CNAME (alias / přezdívka)
 - Odkazuje na jiný A nebo CNAME, www.kiv.zcu.cz => proteus.fav.zcu.cz.
 - MX (mail exchange)
 - Slouží ke směrování pošty zcu.cz => 10 fred.zcu.cz.
 - Nesmí ukazovat přímo na IP, obsahuje prioritu => záznamů může být více, nižší číslo má přednost
 - NS (name server)
 - Autoritativní nameserver, zcu.cz => erebos.zcu.cz.
 - PTR (reverzní záznam)
 - Slouží k reverznímu mapování IP na jméno, 147.228.63.11 => proteus.fav.zcu.cz.
 - AAAA
 - Stejně jako A, ale pro IPv6, zcu.cz => 2001:718:1801:1058::1:100

Základní protokoly: DNS – registrace domény

- Je třeba si zvolit registrátora – pro .CZ na <https://www.nic.cz/whois/registrars/>
 - Aktuálně jejich přes 40
 - Různé rozhraní, ceny, podmínky i nabízené domény
- Proveďte se ověření zda je doména volná v WHOIS databázi
- Potřebuje 2 „různé“ DNS servery
 - Dva kvůli redundanci – nemá smysl uvést jeden 2x, či dva ve stejné síti ...
 - Pokud vlastní DNS nemáte, většina registrátorů vám nabídne zdarma svůj
- Zvolíme platnost od 1 do 10 let – podle domény
- Vytvoří se žádost a přijde výzva k platbě
- Provedou se technické testy – ověření správného nastavení autoritativních serverů
- Ověří se platba a doména se zveřejní
- Před expirací přijde typicky výzva k prodloužení – NATO POZOR, o doménu můžete při neuhrazení přijít
 - Aktivní => Expirovaná => V ochranné lhůtě => Volná

Základní protokoly: DNS – běžné komplikace

- Neaktuální záznamy na pomocných serverech
 - Typicky u velkých proviadrů s cílem šetřit přenosy
- Expirovaná doména v ochranné lhůtě
 - Doména je ještě vaše, ale už nefunguje
- Expirovaná doména po ochranné lhůtě
 - Obecně je doména volná a může si jí kdokoliv koupit
 - Může dojít ke spekulativnímu nákupu s cílem přeprodeje
- Podvržené nebo kompromitované DNS servery
 - Jeden z typu útoků v rámci Internetu
 - Oběť netuší, že nekomunikuje s pravým partnerem - například bankou
 - Může řešit DNSSec nebo SSL
 - Více na poslední přednášce o základech zabezpečení počítačových sítí

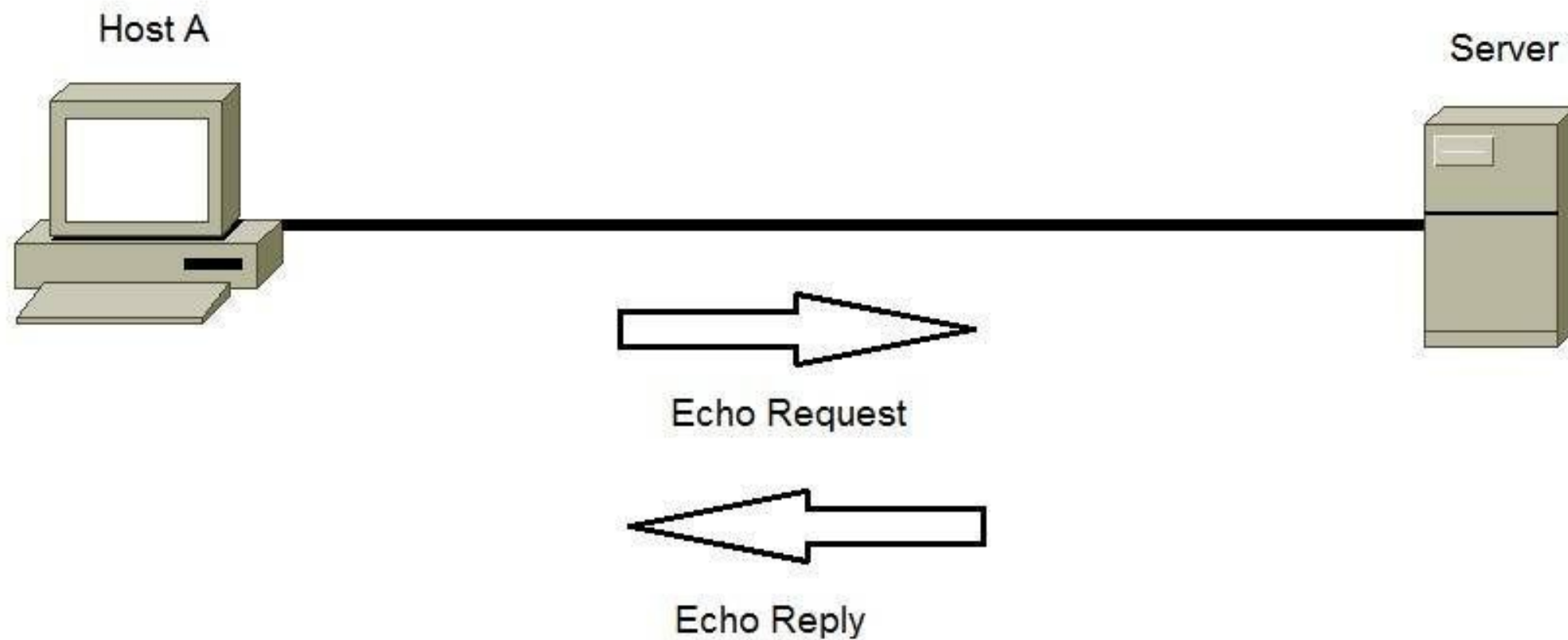
Základní protokoly: ICMP

- ICMP Internet Control Message Protocol
- Pomocný / servisní protokol pro možnost informovat o chybových nebo nestandardních situacích
- Dnes použitelný ve dvou kontextech
 - Informace o chybách – např. Router zjistil, že nemůže data poslat na cílovou stanici, protože ta je nedostupná, tak pošle odesilateli zprávu o nedostupnosti cíle – aby se nečekalo
 - Diagnostika stavu sítě – cíleně posíláme zprávy s cílem zjistit dostupnost stroje nebo např uzly přes které v síti prochází
- Vyžívají jej programy jako ping nebo traceroute
- Na některých zařízeních se dle bezpečnostních pravidel zakazuje
 - Může zvýšit bezpečnost, protože útočník neví zda zařízení nežije či filtruje provoz
 - Podstatně hůře se diagnostikují závady
 - V případě problémů může systém mít výrazně delší odezvu, protože pokud nedostane info o chybě přes ICMP musí čekat na timeout

Základní protokoly: ICMP – typy zpráv

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

Základní protokoly: ICMP – ping



Základní protokoly: ICMP - ping -výstup

Command Prompt

```
C:\Users\LxsoftWin>ping google.com
```

```
Pinging google.com [172.217.24.238] with 32 bytes of data:
```

```
Reply from 172.217.24.238: bytes=32 time=1451ms TTL=53
```

```
Reply from 172.217.24.238: bytes=32 time=599ms TTL=53
```

```
Reply from 172.217.24.238: bytes=32 time=1438ms TTL=53
```

```
Reply from 172.217.24.238: bytes=32 time=1656ms TTL=53
```

```
Ping statistics for 172.217.24.238:
```

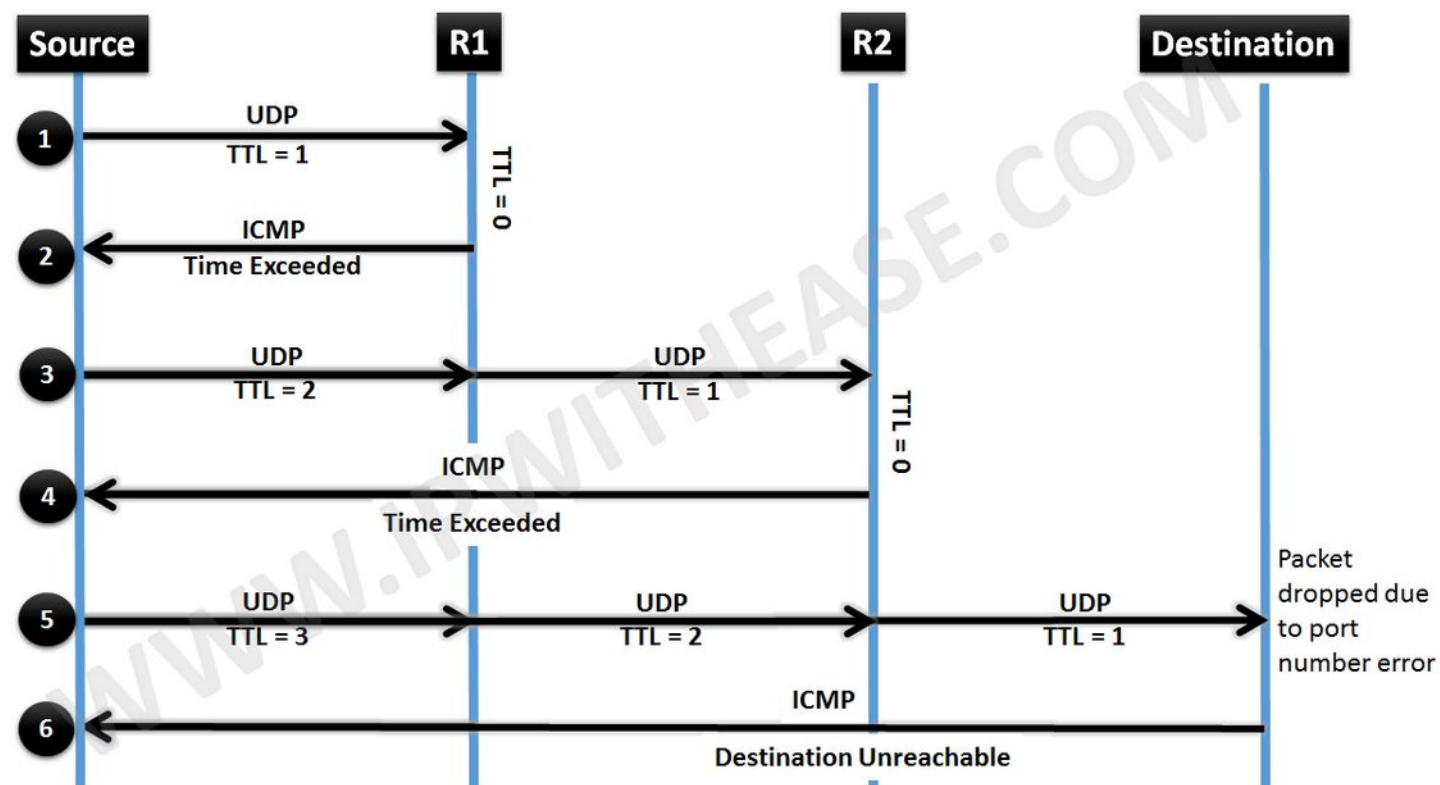
```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
    Approximate round trip times in milli-seconds:
```

```
        Minimum = 599ms, Maximum = 1656ms, Average = 1286ms
```

```
C:\Users\LxsoftWin>
```

Základní protokoly: ICMP -traceroute



*** Each set of communication happens 3 times i.e. Set 1&2 , Set 3 &4 and Set 5&6

zdroj: <https://taylor.git-pages.mst.edu>

Základní protokoly: ICMP -traceroute - výstup

```
Command Prompt
C:\>tracert mediacollege.com

Tracing route to mediacollege.com [66.246.3.197]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  192.168.1.1
  2  240 ms  421 ms  70 ms  219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
  3  20 ms   30 ms   30 ms  210.55.205.123
  4  *       *       *       Request timed out.
  5  30 ms   30 ms   40 ms  202.50.245.197
  6  30 ms   40 ms   40 ms  g2-0-3.tkbr3.global-gateway.net.nz [202.37.245.140]
  7  30 ms   30 ms   40 ms  so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
  8  160 ms  161 ms  160 ms  pi-3.sjbr1.global-gateway.net.nz [202.50.116.178]
  9  160 ms  171 ms  160 ms  so-1-3-0-0.pabr3.global-gateway.net.nz [202.37.245.230]
 10  160 ms  161 ms  170 ms  pao1-br1-g2-1-101.gnaps.net [198.32.176.165]
 11  180 ms  181 ms  180 ms  lax1-br1-p2-1.gnaps.net [199.232.44.5]
 12  170 ms  170 ms  171 ms  lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
 13  240 ms  241 ms  240 ms  nyc-m20-ge2-2-0.gnaps.net [199.232.44.21]
 14  240 ms  251 ms  250 ms  ash-m20-ge1-0-0.gnaps.net [199.232.131.36]
 15  241 ms  240 ms  250 ms  0503.ge-0-0-0.gbr1.ash.nac.net [207.99.39.157]
 16  251 ms  260 ms  250 ms  0.so-2-2-0.gbr2.nwr.nac.net [209.123.11.29]
 17  250 ms  260 ms  261 ms  0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
 18  250 ms  260 ms  261 ms  209.123.182.243
 19  250 ms  260 ms  261 ms  sol.yourhost.co.nz [66.246.3.197]

Trace complete.
C:\>
```

zdroj: <https://www.tech-faq.com/>

Základní diagnostika sítě

- `ipconfig / ifconfig / ip`
 - Výpis nastavení síťového interfaceu
- `route print / route / ip route`
 - Výpis routovací tabulky
- `arp`
 - Výpis ARP tabulky
- `ping`
 - Ověření dostupnosti cíle pomocí ICMP
- `tracert / traceroute`
 - Zjištění trasy k cíli pomocí ICMP
- `nslookup / dig`
 - Zjištění hodnot z DNS
- `netstat / ss`
 - Výpis otevřených spojení
- `wireshark / tcpdump`
 - Sniffer síťové komunikace