Úvod do analýzy

počítačových sítí

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 8. prosince 2013

Základní pojmy

Protokol

- popisuje způsob komunikace na určité úrovni – formát datových jednotek a pravidla pro jejich zasílání a přijímání
- lidé se domlouvají pomocí určitého jazyka, počítače (procesy) pomocí určitého protokolu

Aby protokol fungoval:

- musí ho znát obě komunikující strany (tj. implementovat)
- nesmí být moc složitý, nesmí být výpočetně náročný

$\Rightarrow$ každý protokol slouží svému (jednoduchému) účelu, v komunikaci kombinujeme několik protokolů

$\Rightarrow$ aby mohly spolupracovat, musí mít přesně dané komunikační rozhraní, unifikované

Základní pojmy

Protokolový zásobník

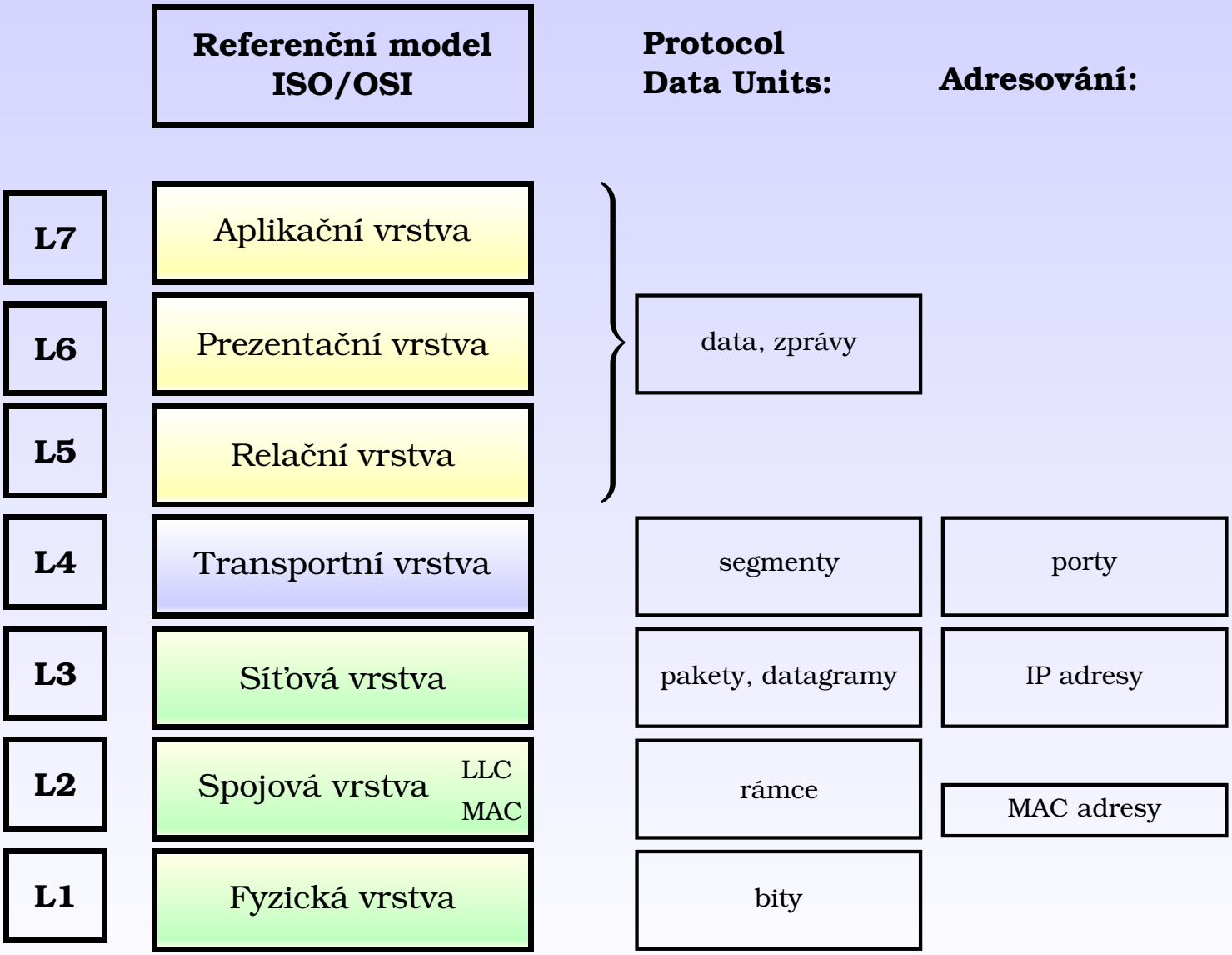
= sada protokolů, které navzájem za určitým účelem spolupracují

- podřízený protokol (v nižší vrstvě) poskytuje služby nadřízenému protokolu
- aby si „rozuměla“ síťová zařízení od různých výrobců, musí být protokolový zásobník standardizován
  - Referenční model ISO/OSI
  - Referenční model TCP/IP
- přesněji:
  - sada protokolů = množina protokolů v konkrétním referenčním modelu
  - protokolový zásobník = podmnožina určité sady protokolů, která je implementována na konkrétním síťovém zařízení

Referenční model ISO/OSI

ISO/OSI (Open Systems Interconnection)

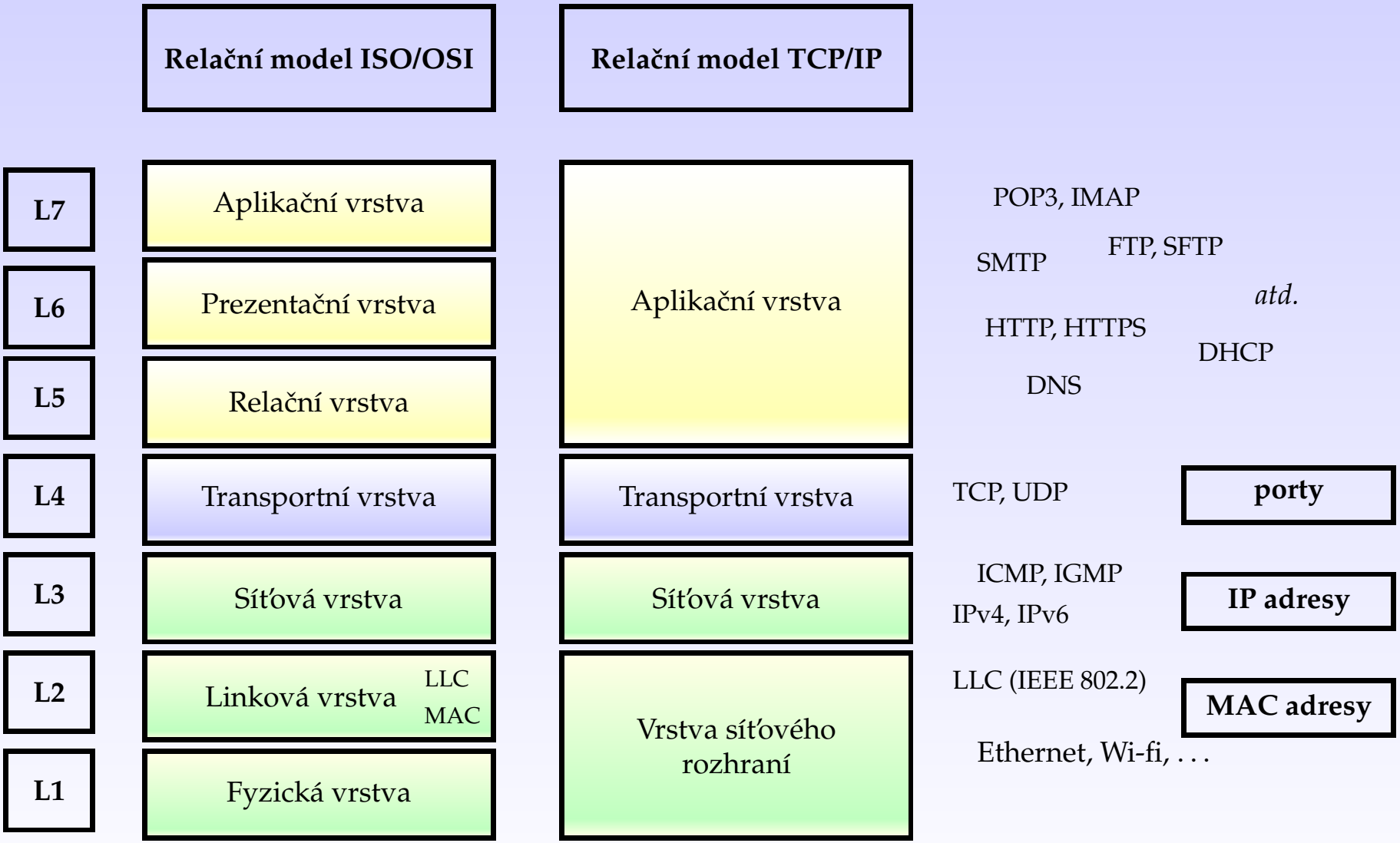
- model spíše teoretický, příliš komplexní, úplný
- u každé vrstvy je jednoznačně určeno, k čemu slouží


Referenční model ISO/OSI
Protocol Data Units:
Adresování:
L7
Aplikační vrstva
L6
Prezentační vrstva
L5
Relační vrstva
data, zprávy
L4
Transportní vrstva
segmenty
porty
L3
Síťová vrstva
pakety, datagramy
IP adresy
L2
Spojová vrstva
LLC
MAC
rámce
MAC adresy
L1
Fyzická vrstva
bity

Referenční model TCP/IP

TCP/IP

- jednodušší, orientován na praktické využití
- když hovoříme o protokolech, obvykle je zařazujeme právě do vrstev TCP/IP


Relační model ISO/OSI
Relační model TCP/IP
L7
L6
L5
L4
L3
L2
L1
Aplikační vrstva
Prezentační vrstva
Relační vrstva
Transportní vrstva
Síťová vrstva
Linková vrstva
LLC
MAC
Fyzická vrstva
Aplikační vrstva
Transportní vrstva
Síťová vrstva
Vrstva síťového rozhraní
POP3, IMAP
SMTP
FTP, SFTP
atd.
HTTP, HTTPS
DHCP
DNS
TCP, UDP
porty
ICMP, IGMP
IPv4, IPv6
IP adresy
LLC (IEEE 802.2)
MAC adresy
Ethernet, Wi-fi, . . .

Komunikace mezi protokoly – zapouzdřování

- při odesílání se postupně přidávají záhlaví (příp. zápatí) jednotlivých vrstev, při přijímání probíhá opačný proces

Komunikace mezi protokoly – zapouzdřování

- při odesílání se postupně přidávají záhlaví (příp. zápatí) jednotlivých vrstev, při přijímání probíhá opačný proces

Postup:

1. některý protokol na aplikační vrstvě odesílá data
2. na transportní vrstvě je převezme např. protokol TCP, opatří záhlavím
3. na síťové vrstvě je převezme protokol IP, opatří záhlavím
4. na vrstvě síťového rozhraní je převezme některý protokol IEEE 802.3, opatří záhlavím a zápatím

Data aplikačního protokolu

Komunikace mezi protokoly – zapouzdřování

- při odesílání se postupně přidávají záhlaví (příp. zápatí) jednotlivých vrstev, při přijímání probíhá opačný proces

Postup:

1. některý protokol na aplikační vrstvě odesílá data
2. na transportní vrstvě je převezme např. protokol TCP, opatří záhlavím
3. na síťové vrstvě je převezme protokol IP, opatří záhlavím
4. na vrstvě síťového rozhraní je převezme některý protokol IEEE 802.3, opatří záhlavím a zápatím

Záhlaví TCP	Data aplikačního protokolu

Komunikace mezi protokoly – zapouzdřování

- při odesílání se postupně přidávají záhlaví (příp. zápatí) jednotlivých vrstev, při přijímání probíhá opačný proces

Postup:

1. některý protokol na aplikační vrstvě odesílá data
2. na transportní vrstvě je převezme např. protokol TCP, opatří záhlavím
3. na síťové vrstvě je převezme protokol IP, opatří záhlavím
4. na vrstvě síťového rozhraní je převezme některý protokol IEEE 802.3, opatří záhlavím a zápatím

Záhlaví IP	Záhlaví TCP	Data aplikačního protokolu

Komunikace mezi protokoly – zapouzdřování

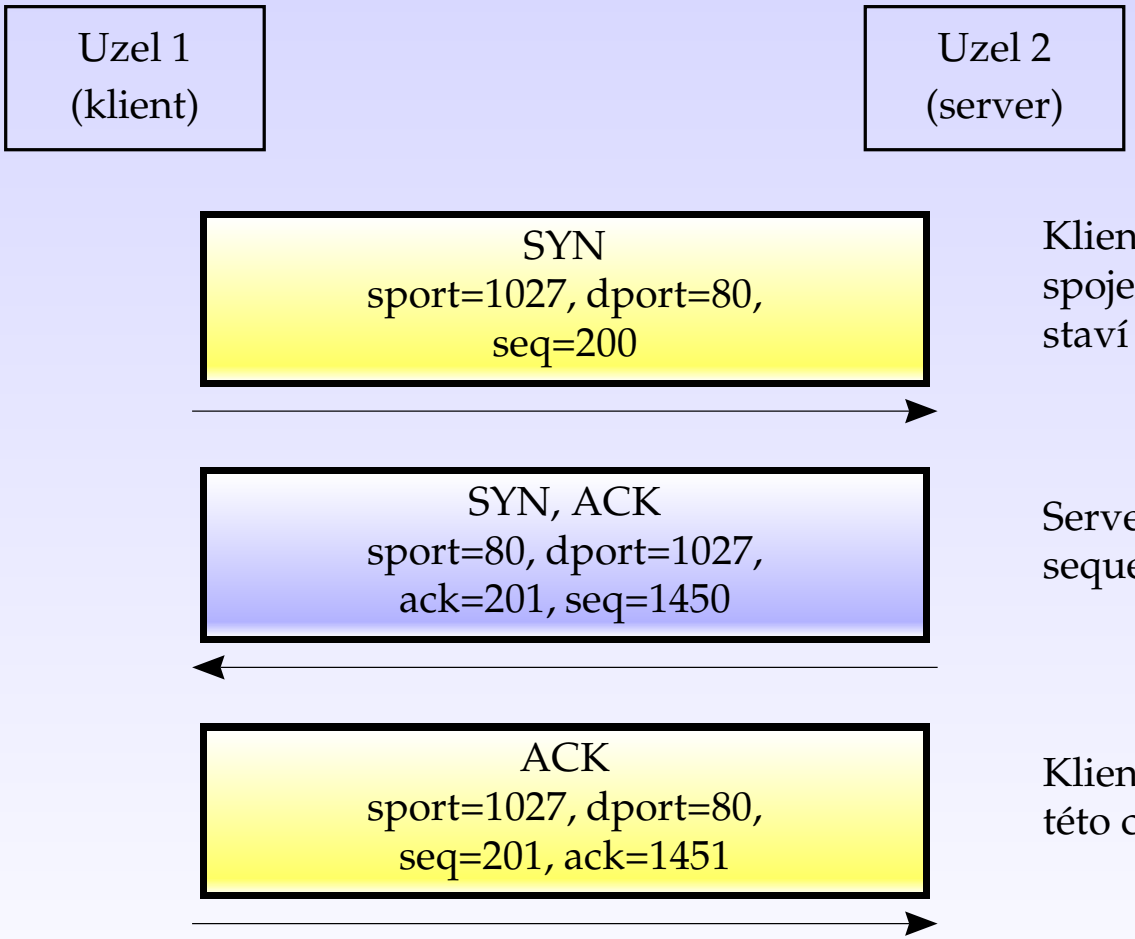
- při odesílání se postupně přidávají záhlaví (příp. zápatí) jednotlivých vrstev, při přijímání probíhá opačný proces

Postup:

1. některý protokol na aplikační vrstvě odesílá data
2. na transportní vrstvě je převezme např. protokol TCP, opatří záhlavím
3. na síťové vrstvě je převezme protokol IP, opatří záhlavím
4. na vrstvě síťového rozhraní je převezme některý protokol IEEE 802.3, opatří záhlavím a zápatím

Záhlaví Ethernet	Záhlaví IP	Záhlaví TCP	Data aplikačního protokolu	Zápatí Ethernet

Komunikace v TCP – handshake



Klient začíná handshake – navázání spojení („chci komunikovat“), nastaví svoje sequence number

Server souhlasí, nastavuje svoje sequence number

Klient potvrdí údaje od serveru, od této chvíle existuje spojení

Port

Významy slova

- číslo označující komunikační kanál z aplikační vrstvy k TCP nebo UDP portu na transportní vrstvě, například:
  - 80 – HTTP (přes TCP), 443 – HTTPS (přes TCP)
  - 21 – FTP (řízení přenosu, TCP), 20 – FTP (data, TCP)
  - 23 – Telnet, 22 – SSH (oba TCP)
  - 25 – SMTP, 143 a 220 – IMAP (TCP), 110 – POP3 (TCP)
  - 53 – DNS (TCP a UDP)
  - 67, 68 – DHCP (UDP)
- fyzické rozhraní, přes které zařízení komunikuje s některým svým sousedem (například RJ-45 port)

Hub (rozbočovač)

Vlastnosti

- pracuje na vrstvě L1 (fyzické), má nejméně 2 porty

$\Rightarrow$ vidí jen sled bitů, pozná, kde začíná a kde končí

- moc toho neumí, ale zato je rychlý
- přijme data na jednom portu, odešle na všechny ostatní

Switch (přepínač)

Vlastnosti

- pracuje obvykle na vrstvě L2 (spojové), ale existují i switche pracující na vyšších vrstvách

$\Rightarrow$ vidí záhlaví a zápatí vrstvy L2 (například ethernetové nebo wi-fi rámce)

- vcelku rychlý, dokáže rozhodovat podle L2 informací
- přijme data na jednom portu, v záhlaví L2 zjistí, pro koho je PDU určen, přeloží podle ARP, odešle na 1 port
- broadcast pakety nebo pakety pro neznámý cíl odesílá na všechny porty kromě přijímajícího
- možnost konfigurace – buď přes webové rozhraní nebo přes konzolu

Switch (přepínač)

CAM (MAC) tabulka

- tabulka známých MAC adres
- záznam = dvojice [MAC adresa, port]
- když mám odeslat paket na danou MAC adresu, pošlu ji na uvedený port
- jak se záznam v tabulce objeví: switch se učí „za provozu“
- v záhlaví L2 jsou uvedeny nejméně 2 MAC adresy – adresa zdroje a adresa cíle
- přijde paket přes port X, zdrojová adresa je mi neznámá $\Rightarrow$ dotyčný zdroj je dosažitelný přes port X, přidám info do CAM

Router (směrovač)

Vlastnosti

- pracuje na vrstvě L3 (síťové)

$\Rightarrow$ vidí záhlaví vrstvy L3, včetně IP adresy cíle

- pomalejší, dokáže rozhodovat podle L3 informací
- přijme data na jednom portu, v záhlaví L3 zjistí, pro koho je PDU určen, přeloží podle směrovací tabulky (CAM), pak podle ARP, odešle na 1 port
- broadcasty a neznámé buď zahazuje, nebo neznámé odešle na bránu
- možnost konfigurace – buď přes webové rozhraní nebo přes konzolu
- propojuje spíše sítě než koncové stanice (až na wi-fi routery)

Zjišťování základních informací

- `ipconfig /all`
  - zjistím svou IP adresu, MAC adresu a další informace
- `route print`
  - zjistím, přes kterou IP adresu jdu, když komunikuji s určitým cílem
  - vypisuje směrovací tabulku – přes kterého souseda se dostanu k cíli
- `arp -a`
  - zjistím MAC adresy svých sousedů
  - vypisuje ARP tabulku, podle které se překládá IP adresa na MAC adresu

DNS (Domain Name System)

- slouží k překladu jmenných („slovních“) adres na IP adresy
- distribuovaná služba
- každé zařízení má IP adresu, kanonické jméno (CNAME) a případně aliasy
- typy záznamů:
  - A, AAAA – známe kanovnické jméno, hledáme IPv4 nebo IPv6 adresu
  - CNAME – známe alias, hledáme kanovnické jméno
  - PTR – reverzní překlad, známe IP adresu, hledáme kanovnické jméno
  - NS – hledáme DNS server (name server)
  - MX – hledáme poštovní server (mail exchange)
  - další

Základní práce s DNS

- `ipconfig /displaydns`
  - zobrazí DNS cache na našem zařízení vč. TTL
- `ipconfig /flushdns`
  - vyčistí DNS cache
- `nslookup`
  - komplexní program pro práci s DNS, především překlad
  - pracuje buď klasicky (parametr = IP nebo jmenná adresa), nebo interaktivně
  - přechod do interaktivního režimu: `nslookup`

`nslookup` v interaktivním módu

- `set all`
- `ls fpf.slu.cz`
- `ls -t ns fpf.slu.cz`
- `ls -t aaaa fpf.slu.cz`

Linux: taky existuje `nslookup`, ale ještě lepší nástroj je `dig`

Základní práce s IP

- `ping adresa`
  - zjišťuje propustnost a dostupnost
- `tracert adresa`
  - zjišťuje stav cesty k cíli
- `pathping adresa`
  - zjišťuje stav cesty k cíli včetně statistických informací

`netstat` (Network Statistics)

- `netstat -ao`
  - celková statistika (all) včetně PID komunikujících procesů
  - jak získat k PID název procesu: `tasklist`
- `netstat -ano`
  - totéž, navíc místo jmenných adres vypisuje IP adresy
- `netstat -es`
  - podrobná statistika všech protokolů z rodiny TCP/IP
- `netstat -sp tcp`
  - pouze statistika protokolu TCP (podobně ip, udp, icmp, atd.)
- `netstat -ab`
  - vypisuje i spustitelné soubory, které do komunikace vstupují

Činnost na stanicích v síti

Máme tyto možnosti:

- Linux – přihlášení přes Telnet (obvykle zakázáno) nebo SSH
- Windows – přihlášení přes Telnet (obvykle zakázáno), práce přes WMI nebo Vzdálená plocha apod.

Mechanismus WMI

- pokud máme dostatečná oprávnění, dokážeme v lokální síti získat informace o počítačích s Windows
- ve Windows běží služba WMI, která udržuje databázi veškerých informací o daném počítači
- k této službě lze přistupovat i z jiného počítače v rámci sítě
- program `wmic` na příkazovém řádku (zadáním bez parametrů se dostaneme do interaktivního režimu)
- nápověda v interaktivním režimu: `/?`
- je třeba mít vyšší přístupová oprávnění

Mechanismus WMI

Příklady (jsme v interaktivním režimu)

- `os list`
  - úplná informace o operačním systému našeho počítače
- `/node:ucetni os list`
  - totéž, ale ptáme se počítače s názvem `ucetni`
- `memorychip get capacity,devicelocator,name`
  - ptáme se na čipy operační paměti, nezajímá nás vše, ale jen vybrané informace
- `service where state="running" get caption,name`
  - chceme informace o všech službách, které na počítači právě běží

Mechanismus WMI

Příklady

- `wmic service "spooler" call startservice`
  - na našem počítači jsme spustili zadanou službu
- `wmic os call reboot`
  - restartovali jsme náš počítač
- `wmic /node:ucetni os call reboot`
  - restartovali jsme cizí počítač
- `wmic /node:ucetni /user:dadmin process where name=explorer.exe call terminate`
  - ukončili jsme zadaný proces na cizím počítači, pod přihlašovacím jménem `dadmin`