

# Siete, TCP/IP, smerovanie a adresácia I.

Mgr. Dan Keder [keder@fi.muni.cz](mailto:keder@fi.muni.cz)

Centrum výpočetní techniky  
Fakulta informatiky  
Masarykova univerzita

23. september 2009

## 1 ISO/OSI model

- Fyzická vrstva a vrstva dátového spoja
- Sieťová vrstva
- Transportná vrstva
- Relačná vrstva
- Prezentačná vrstva
- Aplikačná vrstva

## 2 Protokoly a služby

- Automatická konfigurácia siete
- DNS
- Vzdialený prístup

- Prehľad rôznych sieťových protokolov a služieb v kontexte počítačovej siete FI
- Internet nie je modrá ikonka v tvare písmena e, ktorú možno máte na ploche
- Väčšinu prezentovaných vecí si môžete vyskúšať v Linuxe či v inom podobnom systéme



- ARPANET (Advanced Research Project Agency Network)
  - Projekt financovaný Ministerstvom obrany USA, 1969
  - Nový koncept – zasielanie dátových paketov
  - Distribuovaná architektúra – pri výpadku niektorých uzlov zbytok siete stále funguje
- Internet – "Network of networks"

# ISO/OSI model

## Open System Interconnection Reference Model

### 1 ISO/OSI model

- Fyzická vrstva a vrstva dátového spoja
- Sieťová vrstva
- Transportná vrstva
- Relačná vrstva
- Prezentačná vrstva
- Aplikačná vrstva

### 2 Protokoly a služby

# ISO/OSI model

## Open System Interconnection Reference Model

- Teoretický model popisujúci spôsob návrhu sieťových protokolov
- Teoretický model, vrstevnatá architektúra (protocol stack)
- ISO štandard
- Nižšie vrstvy poskytujú služby vyšším vrstvám
- V skutočnosti sa protokoly môžu prekrývať s viacerými vrstvami



# Fyzická vrstva a vrstva dátového spoja

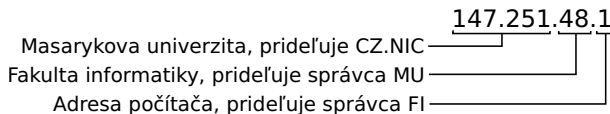
## Physical Layer & Data Link Layer

- Fyzická vrstva – fyzické prepojenie HW zariadení
- Vrstva dátového spoja – prenos dát v rámci jedného sieťového segmentu
- 802.3 – Ethernet, 802.11abgn – Wifi, ...
- Každé zariadenie má priradenú MAC adresu (Media access control)
  - 6 bajtov: 01:00:0a:13:0b:05
  - v Linuxe: `ifconfig -a`
- ARP (Address resolution protocol)
  - preklad IP adresy na MAC adresu
  - v Linuxe: `arp -a`
- Preposielanie paketov na základe MAC adresy – **switching**

# Sieťová vrstva

## Network Layer

- Umožňuje komunikáciu medzi viacerými sieťovými segmentami
- IP – Internet Protocol, ICMP
- Prenášané informácie sú delené na **pakety** (datagramy)
  - hlavička paketu, prenášané dáta
- Pakety sa môžu strácať, doručovať v rôznom poradí...
  - Ošetrujú protokoly na vyšších vrstvách
  - Niekedy výpadky nevadia (napr. počítačové hry)
- Adresovanie pomocou IP adries
  - 32bitové číslo (4 bajty)
  - IP adresy prideluje NIC (Network Information Center)
  - Už dlho hrozí vyčerpanie IP adries ⇒ NAT, IPv6





# Sieťová vrstva – IP adresa

## Network Layer

- IP adresa má 2 časti: adresa siete, adresa počítača
- Triedy IP adries:
  - Formát adresy: N – adresa siete, h – adresa počítača

Trieda	Prvý bajt adresy	Formát adresy
A	0 - 127	N.h.h.h
B	128 - 191	N.N.h.h
C	192 - 223	N.N.N.h

- Triedy nestačia  $\Rightarrow$  CIDR (Classless Inter-domain Routing)
  - dĺžka sieťového prefixu ľubovoľná
  - napr. 10.0.0.0/14
- Privátne adresy – nesmú sa smerovať do Internetu
  - 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/24
  - V každej triede adries jeden rozsah privátnych adries

# Sieťová vrstva – Smerovanie

## Network Layer

- Smerovanie – hľadanie cesty v sieti
- IP adresa, maska siete, router
- Smerovacia tabuľka:

Sieť	Router	Maska siete	Rozhranie
147.251.48.0	0.0.0.0	255.255.255.0	eth0
0.0.0.0	147.251.48.14	0.0.0.0	eth0

- v Linuxe: `route`
- Smerovanie: statické, dynamické (BGP, OSPF...)
- Problémy: existencia viacerých ciest, zacyklenie paketov, straty paketov, ...

# Transportná vrstva

## Transport layer

- Protokoly: TCP (Transmission Control Protocol), UDP (User Datagram Protocol)
- Fungujú nad IP, zavádzajú **porty**
  - well-known porty (80: http, 443: https, ...)
  - v Linuxe: /etc/services
- Zaisťujú integritu dát
- UDP jednoduchšie, nezaručuje spoľahlivý prenos dát – pakety sa môžu cestou stratiť
- TCP zaisťuje spoľahlivý prenos dát
  - retransmisia stratených paketov
  - zahodenie duplicitných paketov
  - kontrola zahltenia siete
- v TCP sa uzatvára 2-bodové **spojenie** (three-way handshake)

- Správa relácie (session) medzi koncovými procesmi
- SIP – Session Initiation Protocol, používa sa u VoIP
  - Signalizačný protokol, RFC 3261
  - Stará sa o registráciu klientov, nadväzovanie, správu a ukončenie telefonického (VoIP) hovoru
  - Cestujúci užívateľ môže mať každú chvíľu inú IP adresu, ale musí byť dostupný pod jedným telefónnym číslom
  - Na vlastný prenos hlasových dát sa používa iný protokol (RTP)

- Spracovanie dát, kódovanie, šifrovanie, ...
- Protokoly: SSL, TLS, MIME
- Zasahujú sem i niektoré aplikačné protokoly (HTTP)

- Kryptografické protokoly, ktoré zabezpečujú prenos dát sieťou
- TLS (RFC 5246) je nástupcom SSL
- Zabraňujú odpočúvaniu a podvrhovaniu prenášaných dát
- Založené na asymetrickej kryptografii
  - PKI (Public Key Infrastructure), certifikáty
  - Klient musí dôverovať certifikačnej autorite, ktorá podpisuje certifikáty
- Bežne sa používa napr. v spojení s HTTP, POP3, IMAP
- Kontrolujte certifikáty – ak server poslal podvrhnutý certifikát, dáta posielate niekomu inému, než si myslíte

- Veľké množstvo protokolov a služieb
- Protokoly konkrétnych aplikácií
- Web: HTTP
- Pošta: SMTP, POP3, IMAP
- Prenos súborov: FTP, rsync
- Vzdialený prístup: telnet, SSH
- Adresárové služby: LDAP
- ...

## 1 ISO/OSI model

## 2 Protokoly a služby

- Automatická konfigurácia siete
- DNS
- Vzdialený prístup



# BOOTP

## Bootstrap protocol

- RFC 951, 1533, 1542
- Jednoduchý protokol pre pridelenie IP adresy klientovi
- Bezdiskové stanice, automatické inštalácie OS
- Nutná podpora vo firmware sieťovej karty
- UDP, porty 67 (server) a 68 (klient), správy BOOTREQUEST a BOOTREPLY

- RFC 2131, 3132
- Rozširuje možnosti BOOTP, spätná kompatibilita s BOOTP
- Klientovi umožňuje nastaviť sieťové rozhranie
- Adresy sa pridávajú na základe MAC adresy alebo dynamicky z určitého rozsahu; klientom sa po určitý čas rezervuje naposledy pridelená adresa
- Správy DHCP Discover, Offer, Request, Acknowledge, Release

- Problém: Ako si zapamätať zložité IP adresy?
  - Zaviest "názvy IP adries"
- Problém 2: Ako udržovať mapovanie *názov* – *IP adresa* aktuálne?
  - /etc/hosts nestačí (veľké množstvo dát)
  - DNS
- DNS zavádza do doménových názvov hierarchiu, zmena na jednom stupni nevynucuje zmenu na ostatných stupňoch
  - `www.fi.muni.cz`
  - TLD (Top Level Domain) – názvy domén najvyššieho rádu (cz, sk, com, ...), požiadavky na ne obsluhujú tzv. koreňové name servery
  - domény nižších rádov majú svojich vlastných správcov

- Typy name serverov
  - primárny name server
  - sekundárny name server – záloha primárneho serveru, synchronizuje sa s primárnym name serverom
  - cache-only name server – neautoritatívny server, slúži na zníženie záťaže
- BIND (Berkeley Internet Name Domain Service)
  - named - proces v UNIXu zaisťujúci transformáciu adries v doménovom tvare na IP adresy
- Na strane klienta – resolver, pre aplikácie je komunikácia s DNS serverom transparentná
  - v Linuxe: `/etc/resolv.conf`

- Telnet sa pôvodne používal na vzdialené prihlasovanie k príkazovému riadku počítača (shellu)
- Všetky dáta sa posielajú po sieti nezabezpečené (i heslá), preto sa na to dnes už nepoužíva
- Port 21, ale je možné špecifikovať ľubovoľný port, na ktorý sa má pripojiť
- Telnet je užitočný na skúšanie alebo ladenie sieťových služieb a protokolov, ktoré majú človekom čitateľný formát (t.j. text)

# Telnet – príklad

Teletype network

```
$ telnet www.fi.muni.cz 80
Trying 147.251.48.1...
Connected to www.fi.muni.cz.
Escape character is '^]'.
HEAD / HTTP-1.1

HTTP/1.1 200 OK
Date: Tue, 22 Sep 2009 10:43:00 GMT
Server: Apache
Content-Location: index.xhtml.cs
Vary: negotiate,accept-language
TCN: choice
Last-Modified: Tue, 22 Sep 2009 08:47:46 GMT
ETag: "2d77a05-32f7-a6fcb080"
Accept-Ranges: bytes
Content-Length: 13047
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Language: cs

Connection closed by foreign host.
```

- RFC 4250 až 4256
- SSH je protokol, ktorý umožňuje bezpečnú komunikáciu v sieti medzi dvoma počítačmi
  - Zabezpečuje **dôvernosť** a **integritu** dát
- Hybridný kryptosystém
  - používa asymetrickú kryptografiu k overeniu totožnosti oboch účastníkov
  - používa symetrickú kryptografiu na šifrovanie prenášaných dát
- Dve verzie:
  - v1: moc sa nepoužíva, známe bezpečnostné chyby
  - v2: používa sa dnes, má čistejšiu architektúru než v1 (spojová, autentizačná a transportná vrstva), podpora silnejších šifri
- Najpoužívanejšia implementácia: OpenSSH

- Server počúva na TCP porte 22
- Metódy autentizácie:
  - "password" – jednoduché overenie hesla
  - "publickey" – privátny + verejný kľúč
  - "keyboard-interactive" – server posiela klientovi výzvy na zadanie autentizačných údajov
  - GSSAPI – autentizácia pomocou Kerbera
- Šifrovacie algoritmy:
  - 3DES, RC4, AES, Blowfish, CAST
- Vzájomná dohoda na metóde autentizácie a šifrovacom algoritme



- Umožňujú prihlasovanie na vzdialené počítače "bez hesla"
- Asymetrická kryptografia – privátny a verejný kľúč
- Vytvorenie kľúča:

```
$ ssh-keygen -t dsa
```

- Privátny kľúč uložený väčšinou ako `~/.ssh/id_dsa`, verejný `~/.ssh/id_dsa.pub`
- Zoznam **verejných** kľúčov oprávnených prihlásiť sa v súbore `~/.ssh/authorized_keys`
- Možnosť použiť `ssh-agent(1)` a `ssh-add(1)` k zapamätaniu hesiel SSH kľúčov

- Primárne navrhnuté ako náhrada za telnet a rsh
  - spúšťanie procesov na vzdialenom počítači
- Široké možnosti použitia
  - synchronizácia súborov a adresárov (v spolupráci s rsync)
  - tunelovanie TCP/IP spojení
  - bezpečný X11-forwarding
  - bezpečné pripojenie vzdialeného adresára na lokálny stroj (sshfs)
  - ...

- Triviálny príklad

```
$ ssh user@server.example.com
```

- X11 Forwarding

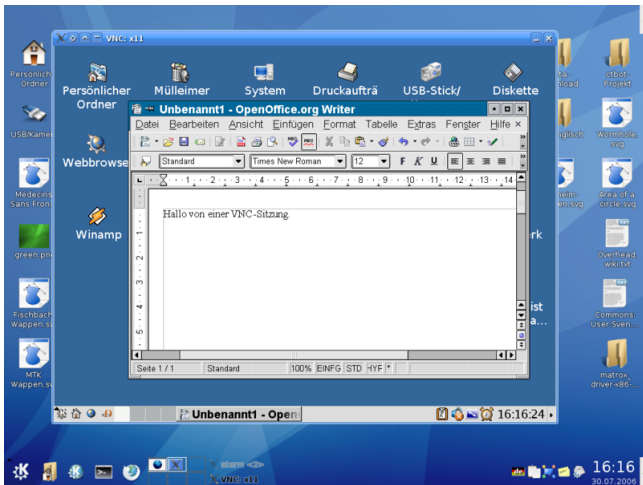
```
$ ssh -X -f user@server.example.com xclock
```

- Tunelovanie TCP spojení

```
$ ssh -f -L 1234:localhost:6667 \  
    server.example.com -N  
$ irc -c '#users' -p 1234 pinky localhost
```

# VNC

## Virtual Network Computing I.



- Umožňuje vzdialené ovládanie počítača v grafickom móde
  - "Vzdialená pracovná plocha"
- Nezávislé na platforme
- Dve súčasti
  - server – periodicky posiela klientovi časti obrazovky, ktoré sa zmenili (ako bitmapu)
  - klient (viewer) – zobrazuje u užívateľa pracovnú plochu vzdialeného počítača, zasiela serveru udalosti (myš, klávesnica)
- Efektívny prenos prenášaných dát – podpora rôznych kódovaní

- TCP porty 5900 – 5906
- Nezabezpečený protokol, tunelovanie cez SSH
- Použitie
  - náhrada X11 forwardingu – lepší výkon v pomalej sieti
  - virtualizácia – prístup na bežiaci virtuálny stroj
  - možnosť pripojiť sa k existujúcemu X11 sedeniu (x11vnc)
  - ...
- Implementácie: x11vnc, tightvnc, Apple Remote Desktop

## Kde hľadať ďalšie informácie

- Warriors of the Net
  - <http://www.warriorsofthe.net/movie.html>
- Repozitár RFC dokumentov
  - <http://tools.ietf.org/html/>
- Manuálové stránky a dokumentácia k programom
- Google, Wikipedia

