



Přednáška 9

Síťové rozhraní.

Katedra číslicových systémů FIT, České vysoké učení technické v Praze

©Jan Trdlička, 2011

Příprava studijního programu Informatika je podporována projektem financovaným z Evropského sociálního fondu a rozpočtu hlavního města Prahy.

Praha & EU: Investujeme do vaší budoucnosti

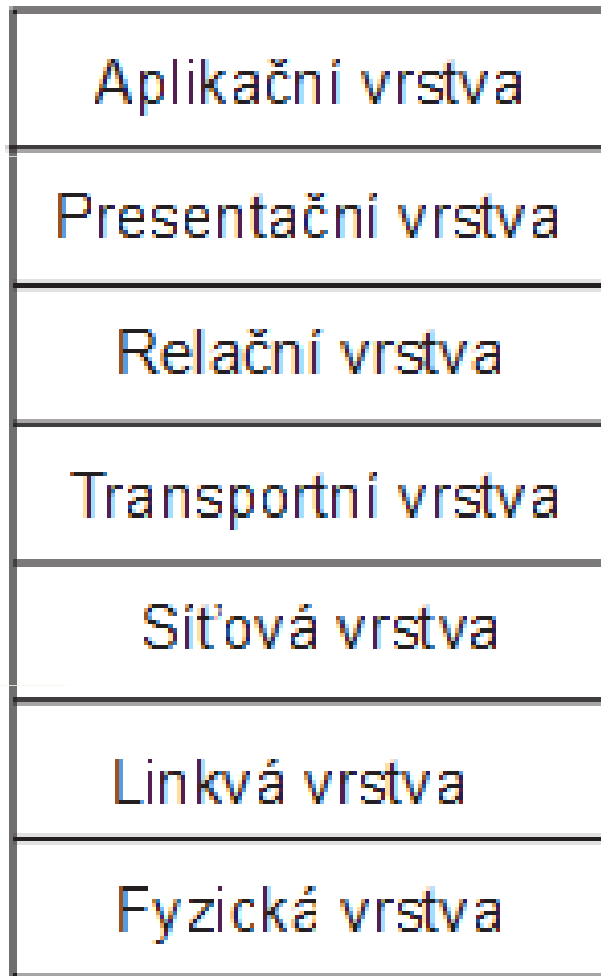


- Sítě jsou složité \Rightarrow pro zjednodušení jsou řešeny po vrstvách
- **ISO/OSI model**
 - od teorie k praxi
 - příliš se neujal
 - 7 vrstev
- **TCP/IP model**
 - od praxe k teorii
 - sada protokolů implementovaných na internetu
 - 4 resp. 5 vrstev
 - specifikován RFC
- **Protokol**
 - sada pravidel popisujících výměnu dat
 - pro TCP/IP jsou nejčastěji definovány v tzv. RFC (Request For Comments)

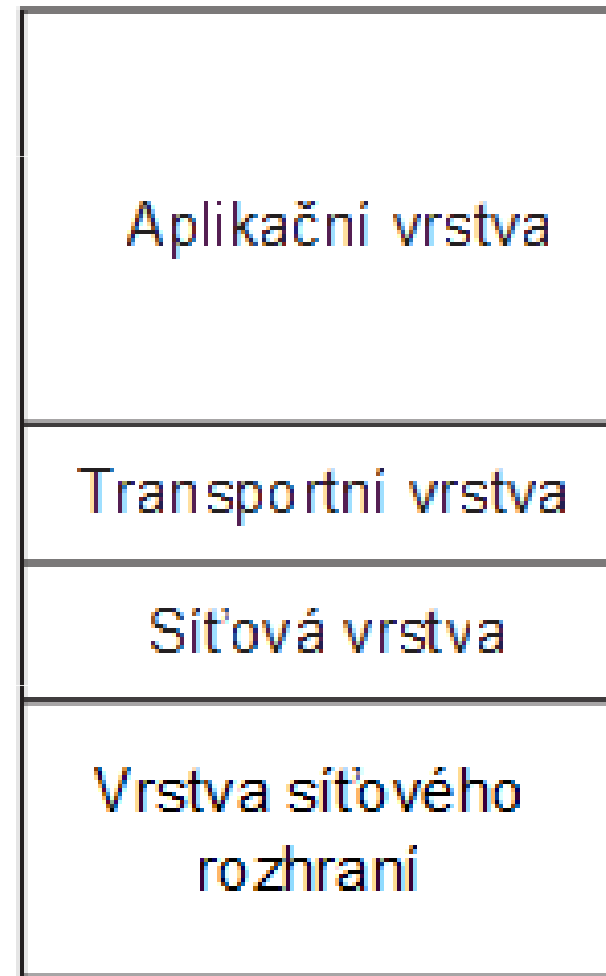


Sít'ové modely

Model ISO/OSI



Model TCP/IP



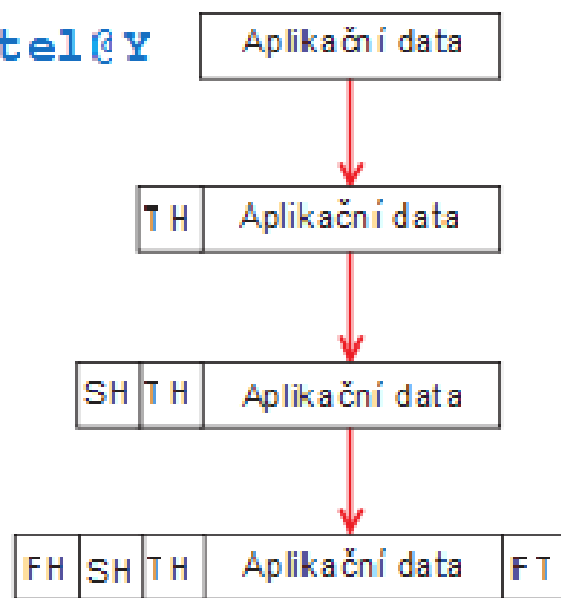


Zapouzdření

Lokální systém X

Vzdálený systém Y

`ssh uživatel@Y`



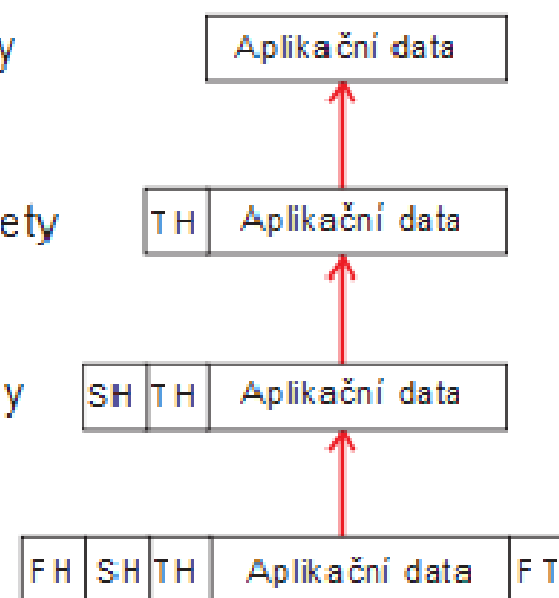
Aplikační vrstva - zprávy
(ssh protokol)

Transportní vrstva - pakety
(TCP)

Síťová vrstva - datagramy
(IP)

Vrstva síť. rozhraní - rámce
(Ethernet)

`sshd`





Vrstva síťového rozhraní

- **Topologie**

- **sběrnice (bus)** – např. Ethernet na koaxiálním kabelu
- **hvězda (star)** – např. Ethernet na kroucené dvoulince, FDDI,...
- **kruh (ring)** – např. Token ring

- **Charakter komunikace**

- **spojové**

- před zahájením přenosu nutné navázat spojení, tzv. virtuální kanál
- prostřednictvím virtuálního kanálu jsou potom přenášena data
- např. ATM

- **nespojové**

- např. technologie založené na broadcastu, tzn. všesměrovém vysílání
- např. Ethernet, Token Ring, FDDI



Vrstva síťového rozhraní

- **Princip komunikace**

- **stochastický**

- založený na náhodném přístupu k médiu
 - např. CSMA-CD u Ethernetu

- **deterministický**

- založený na řízení přístupu k médiu, k řízení je používána metoda předávání speciálního paketu - peška (token)
 - např. Token Ring

- **Rozsah sítí**

- **LAN (Local Area Network)**

- běžně síť v jedné nebo několika sousedních budovách

- **MAN (Metropolitan Area Network)**

- síť většího rozsahu pokrývající např. území velkého podniku nebo města

- **WAN (Wide Area Network)**

- síť tvořená větším či menším počtem vzájemně vzdálených LAN



Vrstva síťového rozhraní

- **Zajišťuje přístup ke sdílenému médiu a adresaci** na fyzickém spojení v jednom síťovém segmentu.
- K adresaci jsou používány fyzické neboli **MAC (Media Access Control)** adresy.
- Obvyklý **formát hlavičky** síťové vrstvy:

úvodní sekvence	cílová adresa	zdrojová adresa	...
-----------------	---------------	-----------------	-----

- Datové jednotky přenášené síťovou vrstvou jsou **rámce** (frame).



- **Protokoly**
 - **Ethernet, Token Ring, ATM**
 - fyzické přenosové protokoly
 - **SLIP (Serial Line IP)**
 - přenos po sériové lince
 - **PPP (Point to Point Protocol)**
 - novější způsob přenosu IP po sériové lince
 - **ARP (Address Resolution Protocol)**
 - mapování IP adres na MAC adresy
 - **RARP (Reverse Address Resolution Protocol)**
 - zjištění IP adresy na základě MAC adresy



- Výpis informací o síťových rozhraních**

```
$ ifconfig -a
```

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL>
```

```
mtu 8232 index 1 inet 127.0.0.1 netmask ff000000
```

```
bge0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
```

```
mtu 1500 index 2 inet 147.32.192.154 netmask ffff0000
```

```
broadcast 147.32.207.255 ether 00:04:76:A4:DF:9B
```

```
bge3: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
```

```
mtu 1500 index 3 inet 172.16.16.17 netmask ffff0000
```

```
broadcast 172.16.255.255 ether 00:04:76:A4:AF:02
```



Vrstva síťového rozhraní

- Výpis nakonfigurovaných rozhraní a informace o přenesených paketech**

\$ netstat -i

Name	Mtu	Net/Dest	Address	Ipkts	Ierrs	Opkts	Oerrs	Collis	Queue
lo0	8232	loopback	localhost	1981597	0	1981597	0	0	0
e1000g0	1500	fray1	fray1	7308678	0	7711202	0	0	0
e1000g3	1500	fray1-e1000g3	fray1-e1000g3	7320842	0	5915331	0	0	0

Chyby

- nesmí být, pokud existují pravidelně, znemožňují provoz



- **Segment sítě**
 - jeden fyzický úsek sítě (např. jeden kroucený kabel)
- **Opakovač (repeater, hub)**
 - spojuje segmenty sítě do tzv. kolizní domény
 - šíří všechny pakety včetně kolizí a chyb (může chybový port odpojit)
- **Přepínač (switch, bridge)**
 - přepíná rámce na vrstvě síťového rozhraní na základě fyzických adres
 - spojuje kolizní domény a přenáší mezi nimi jen potřebná data
 - zvyšuje bezpečnost a zmenšuje zátěž sítě
 - je dražší a hlučnější než hub
- **Směrovač (router)**
 - pracuje na podobném principu jako bridge
 - rozdíl je v tom, že směrovač pracuje s logickými adresami



- Zajišťuje **adresaci v rámci sít'ového prostředí s více fyzickými segmenty**.
- Používá **logické adresy** a prostřednictvím nich zajišťuje přenos dat z jednoho zařízení na druhé i z jedné sítě do jiné.
- **Logická adresa** (dvě verze IPv4 a IPv6):
 - část definující **adresu sítě**
 - část definující **adresu uzlu**
- **Protokoly**
 - **IP (Internet Protocol)**
 - přenos datagramů mezi dvěma uzly sítě
 - **ICMP (Internet Control Message Protocol)**
 - testování a přenos chybových zpráv



- **Výpis nastavení sít'ového rozhraní:** `ifconfig -a`

- **Ověření průchodnosti cesty:** `ping`

```
$ ping www.google.com
```

```
www.google.com is alive
```

```
$ ping -s www.google.com
```

```
PING www.google.com: 56 data bytes
```

```
64 bytes from nf-in-f103.google.com (64.233.183.103): icmp_seq=0. time=24.8 ms
```

```
64 bytes from nf-in-f103.google.com (64.233.183.103): icmp_seq=1. time=24.7 ms
```

```
^C
```

```
----www.google.com PING Statistics----
```

```
2 packets transmitted, 2 packets received, 0% packet loss
```

```
round-trip (ms) min/avg/max/stddev = 24.7/24.7/24.8/0.045
```



- **Náhrada logických adres jménem**
 - pomůcka pro uživatele
 - překlad jmen na adresy (a naopak) se nazývá „resolvování“
 - jméno může být jednoduché nebo doménové
 - překlad je pomocí:
 - souboru **/etc/hosts**
 - pomocí jmenných služeb: **DNS, NIS, NIS+, LDAP**
 - soubor **/etc/nsswitch.conf** určuje, která databáze se použije pro překlad



- **Směrování (routing)**

- přepínání datagramů v mezilehlých uzlech (routerech)
- je ovlivněna adresou sítě, nikoliv uzlu
- v Unixu je implementováno v jádře
- je řízeno tabulkou, kterou lze nastavit
 - ručně příkazem **route**
 - dynamicky pomocí protokolů: **RIP, OSPF, BGP,...**

- **Maska sítě**

- explicitně definuje rozdělení adresy sítě a adresu uzlu

- **Podsítě**

- pomocí masky sítě delší než je standardní se jedna síť rozdělí na více podsítí



- **Výpis směrovací tabulky:** `netstat -r`

```
$ netstat -r
```

```
Routing Table: IPv4
```

Destination	Gateway	Flags	Ref	Use	Interface
-----	-----	-----	-----	-----	-----
default	gw129.fit.cvut.cz	UG	1	2082	
147.32.232.128	fray1	U	1	319	e1000g0
172.16.0.0	fray1-e1000g3	U	1	1129	e1000g3
localhost	localhost	UH	10	36269	lo0

- **Ověření cesty k cíli:** `traceroute`

```
$ traceroute sunray1.felk.cvut.cz
```

```
traceroute: Warning: Multiple interfaces found; using 147.32.192.154 @ bge0
```

```
traceroute to sunray1.felk.cvut.cz (147.32.80.36), 30 hops max, 40 byte packets
```

```
1  147.32.192.1 (147.32.192.1)  0.946 ms  0.650 ms  0.696 ms
```

```
2  rlde-fel.net.cvut.cz (147.32.252.29)  0.557 ms  0.726 ms  0.711 ms
```

```
...
```




- Doplňuje adresaci uzlů o adresaci aplikací (služeb) běžících na uzlech (o tzv. porty)
- **Protokoly**
 - přiřazení čísel protokolům je v souboru `/etc/protocols`
 - **TCP (Transmission Control Protocol)**
 - obousměrný spojovaný spolehlivý proud dat
 - **UDP (User Datagram Protocol)**
 - nespojovaný, nespolehlivý přenos datagramů mezi aplikacemi
- **Porty**
 - 64k portů TCP, 64k portů UDP
 - porty 0-1023 jsou privilegované (mohou být použity pouze aplikacemi s EUID=0)
 - v souboru `/etc/services` jsou uvedeny porty přidělené standardním službám (IANA = Internet Assigned Numbers Authority)



- **Model klient server**

- Aplikace je obvykle tvořena klientem (volaným přímo uživatelem) a serverem (běžícím nebo podle potřeby odstartovaným démonem).
- Aplikace se píší metodou socketů (BSD) nebo RPC.

- **Sockety**

- obdoba souborů
- většina portů z `/etc/services` je používána pomocí socketů
- např. `telnet`, `ftp`, `rlogin`, ...

- **RPC (Remote Procedure Call)**

- síťové operace jsou zamaskovány pomocí volání procedur, které se provádějí na vzdáleném uzlu
- přidělování portů může být dynamické pomocí démona `rpcbind/portmapper`



- **Start serverů aplikací**

- ručně
- při spuštění systému pomocí startovacích skriptů
- v případě potřeby pomocí programu `inetd`

- **Program `inetd`**

- je spuštěn při spuštění systému
- poslouchá na požadovaných portech a při požadavku dané služby statuje příslušného démona
- podporované služby jsou definované v souboru `/etc/inetd.conf`
- běží s EUID=0 a proto může být použit k útokům na systém
- pro zvýšení bezpečnosti lze použít tzv. wrappery



- **Výpis aktivních spojení:** `netstat -a`

