S IPv6 na věčné časy a n~~i~~ěkdy jinak

síťové architektury a jejich budoucnost

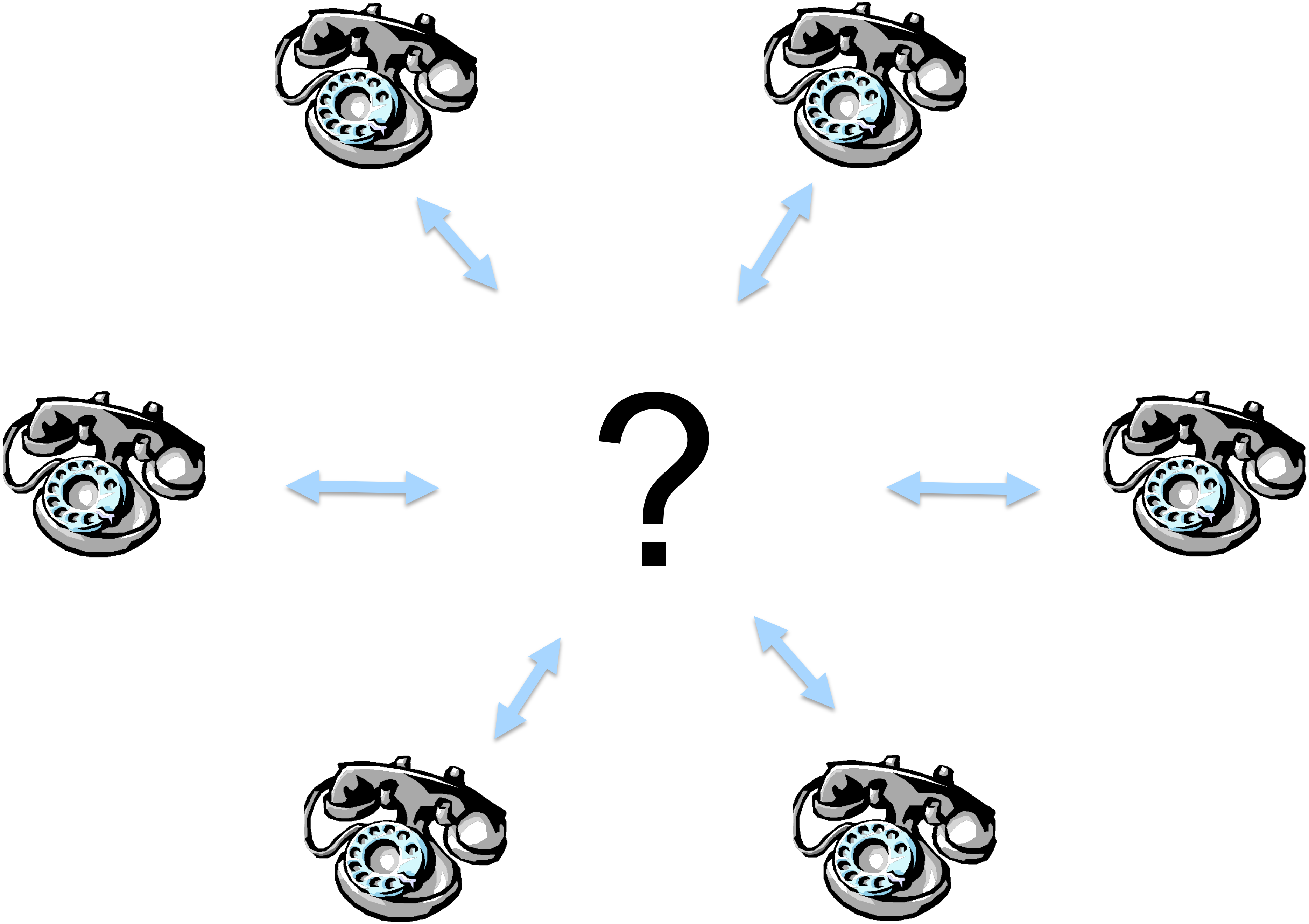
CVIS
CENTRUM VÝPOČETNÍCH A INFORMAČNÍCH SLUŽEB

Konference Internet a Technologie 13, Praha 2013

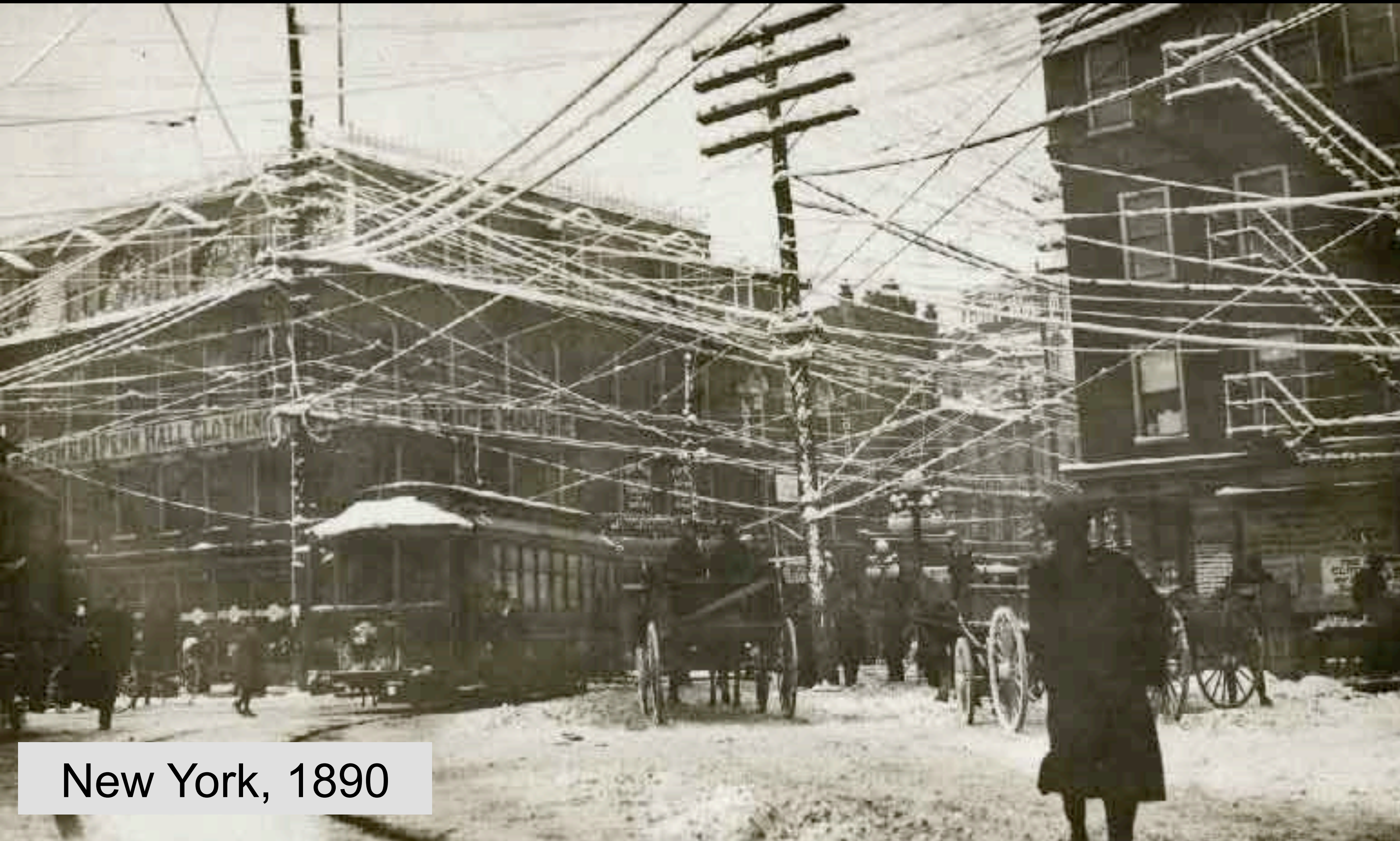
Tomáš Podermanski, tpoder@cis.vutbr.cz
Vysoké učení technické v Brně

FIT
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

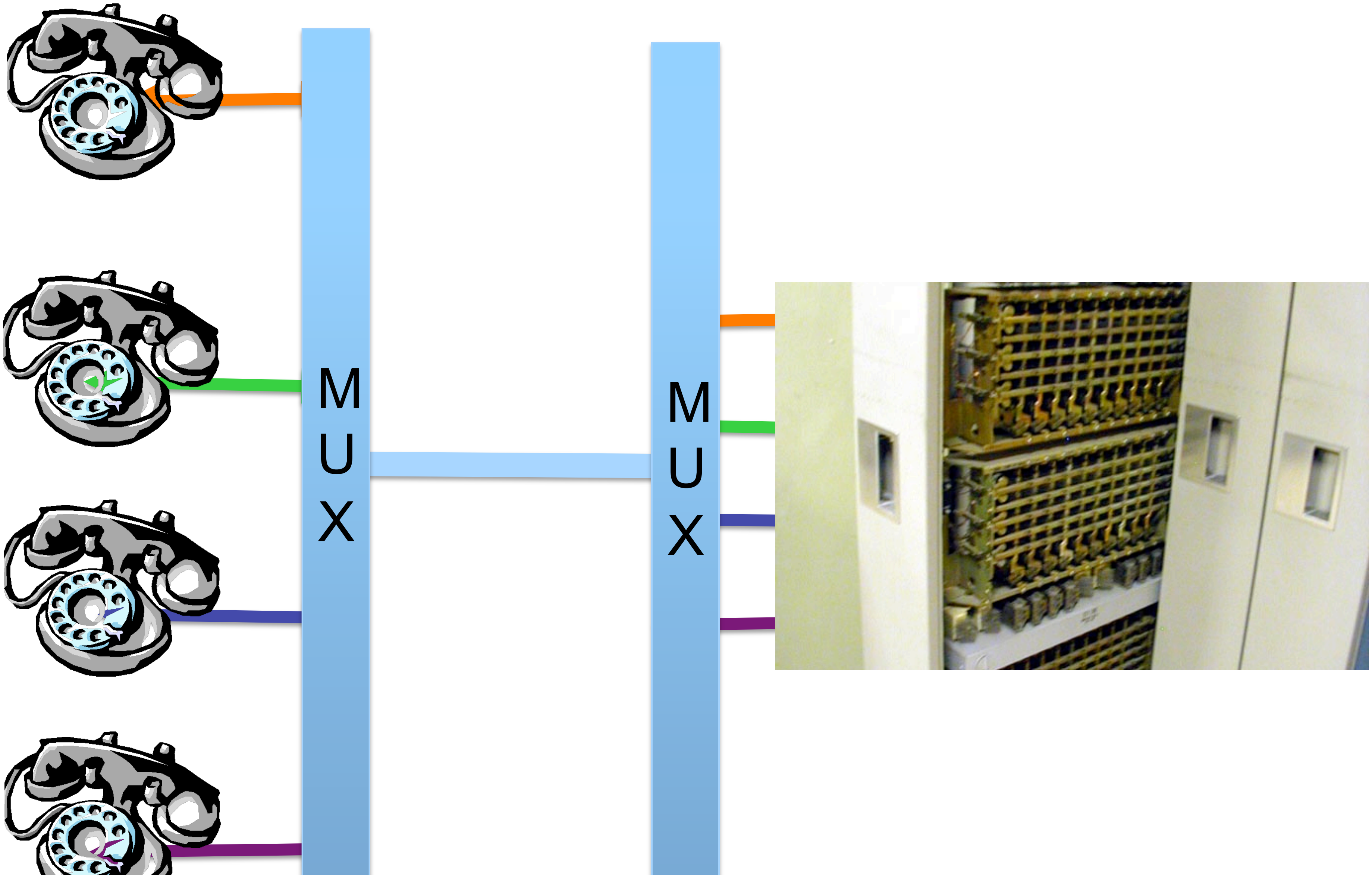
1876



Ústředna Siemens, 1937

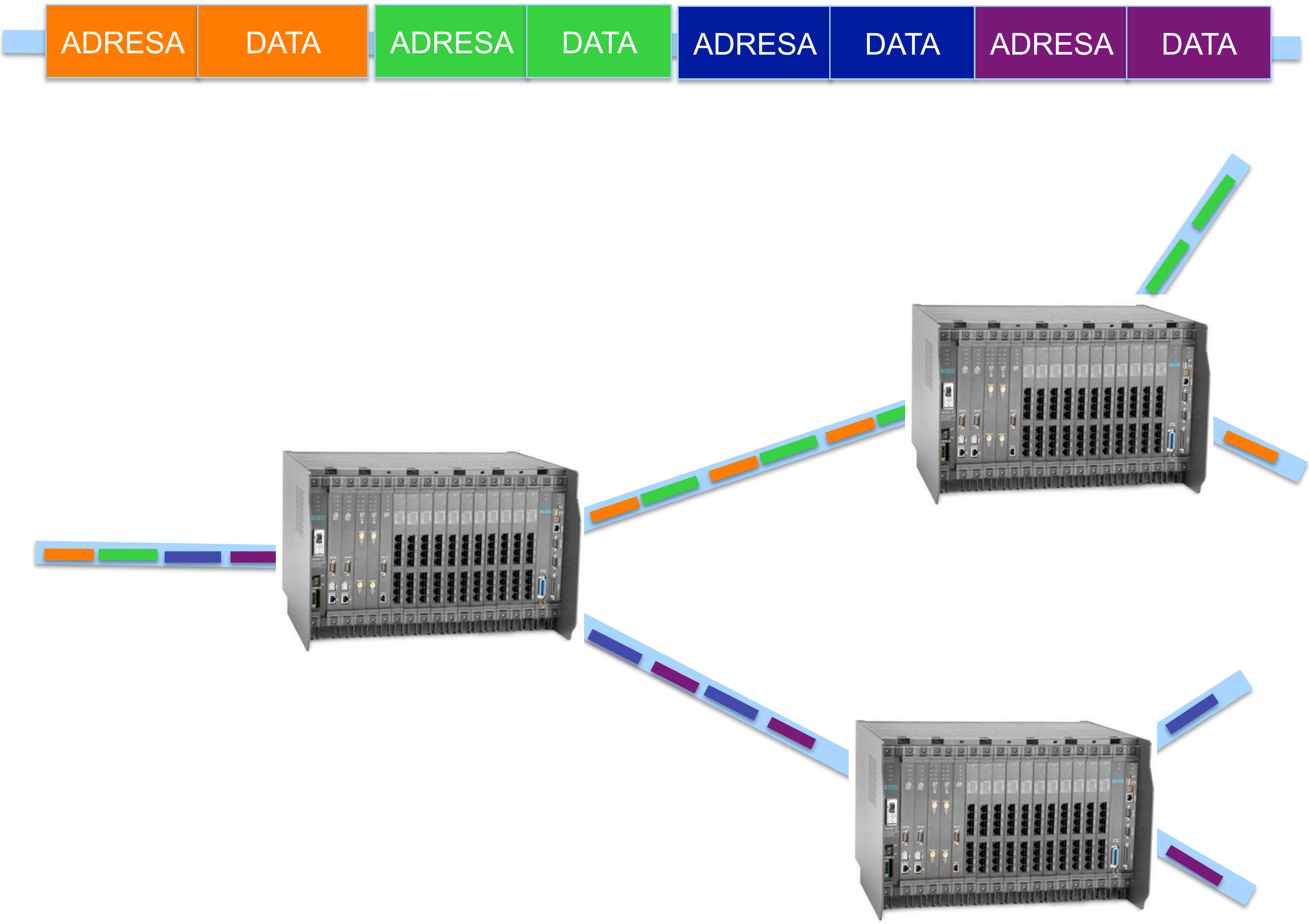


New York, 1890

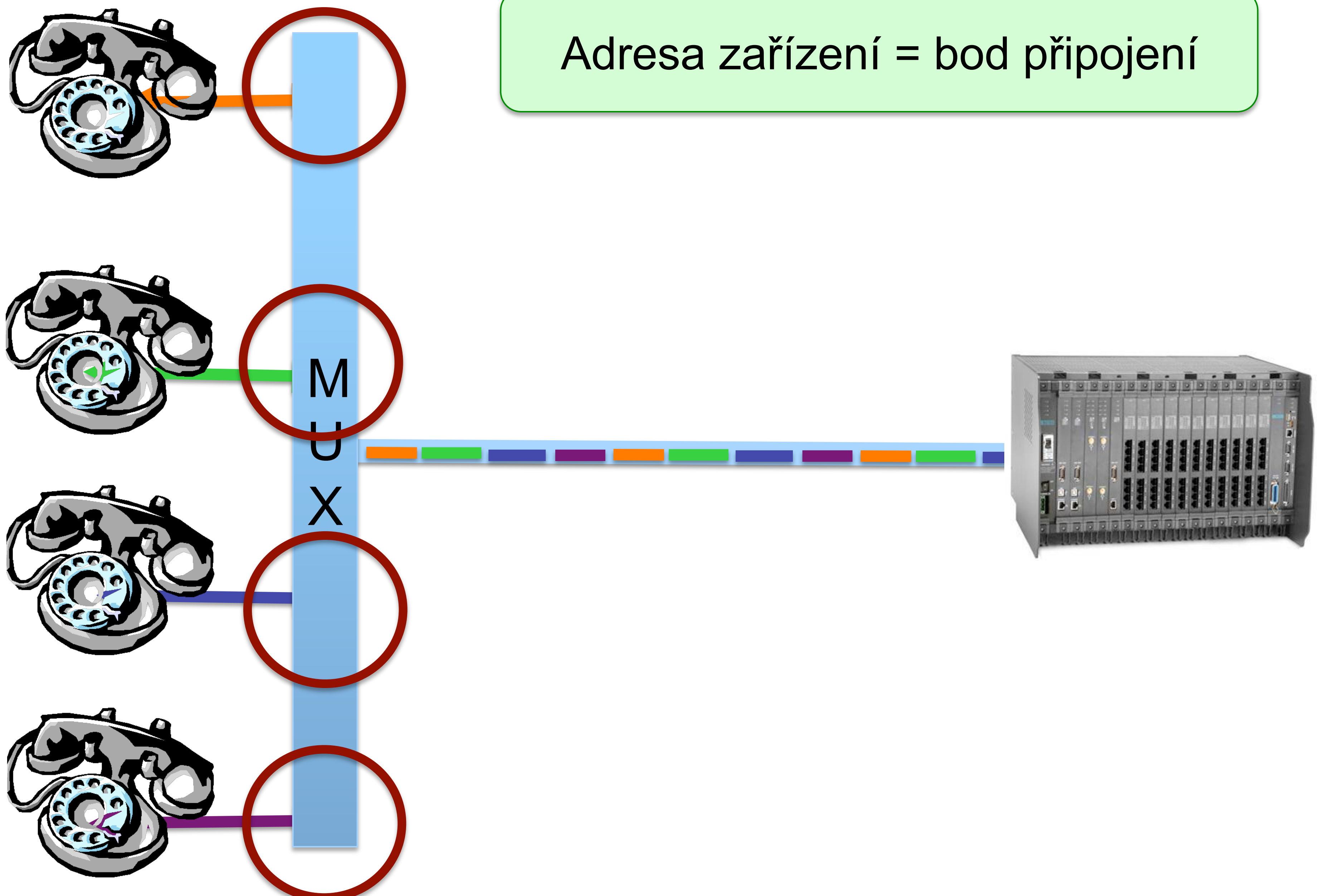


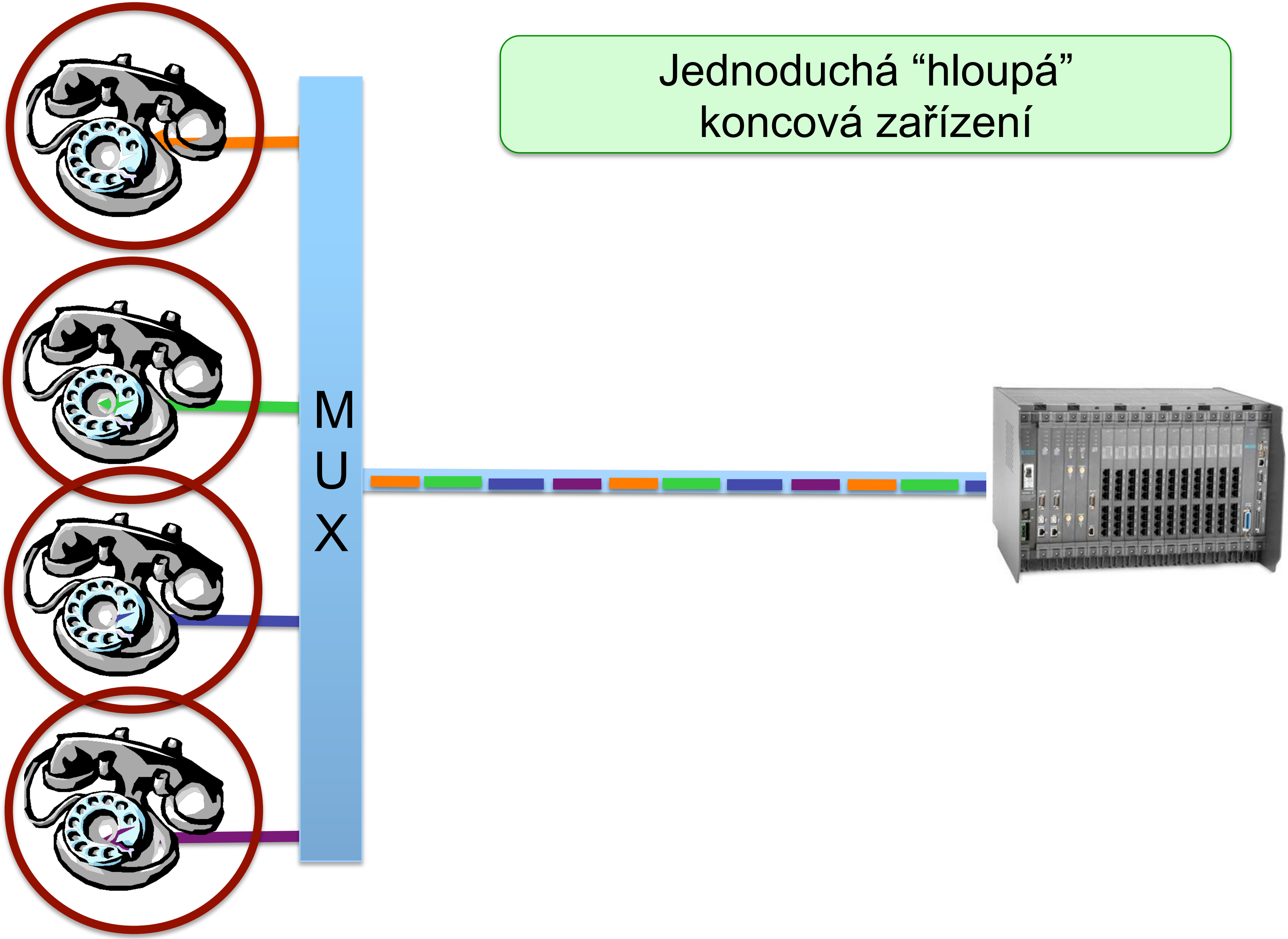
1938, automatická ústředna - 20 linek


Fisher-Price®


ADRESA
DATA
ADRESA
DATA
ADRESA
DATA
ADRESA
DATA

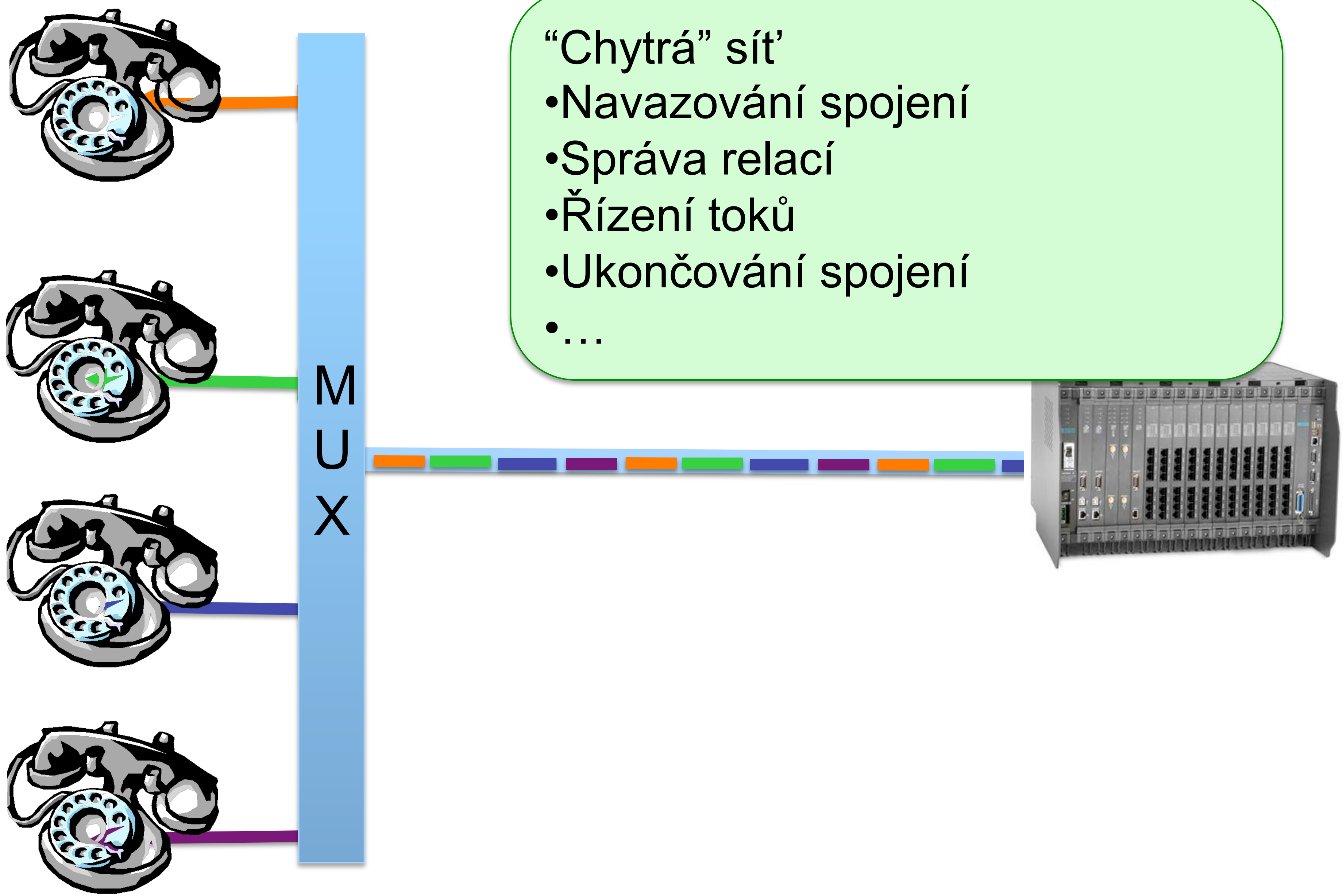
Adresa zařízení = bod připojení

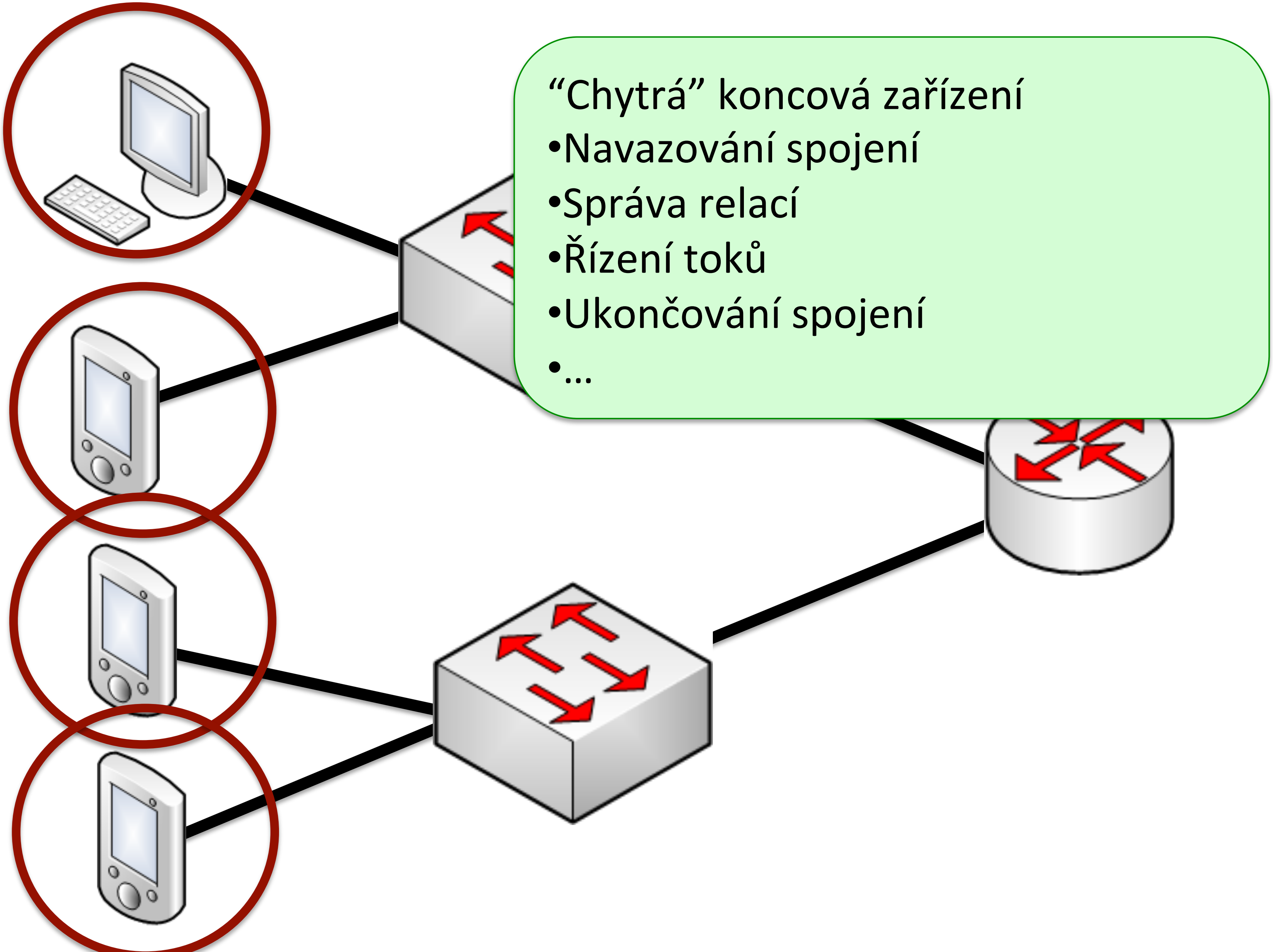



Jednoduchá “hloupá”
koncová zařízení
MUX

“Chytrá” sít’

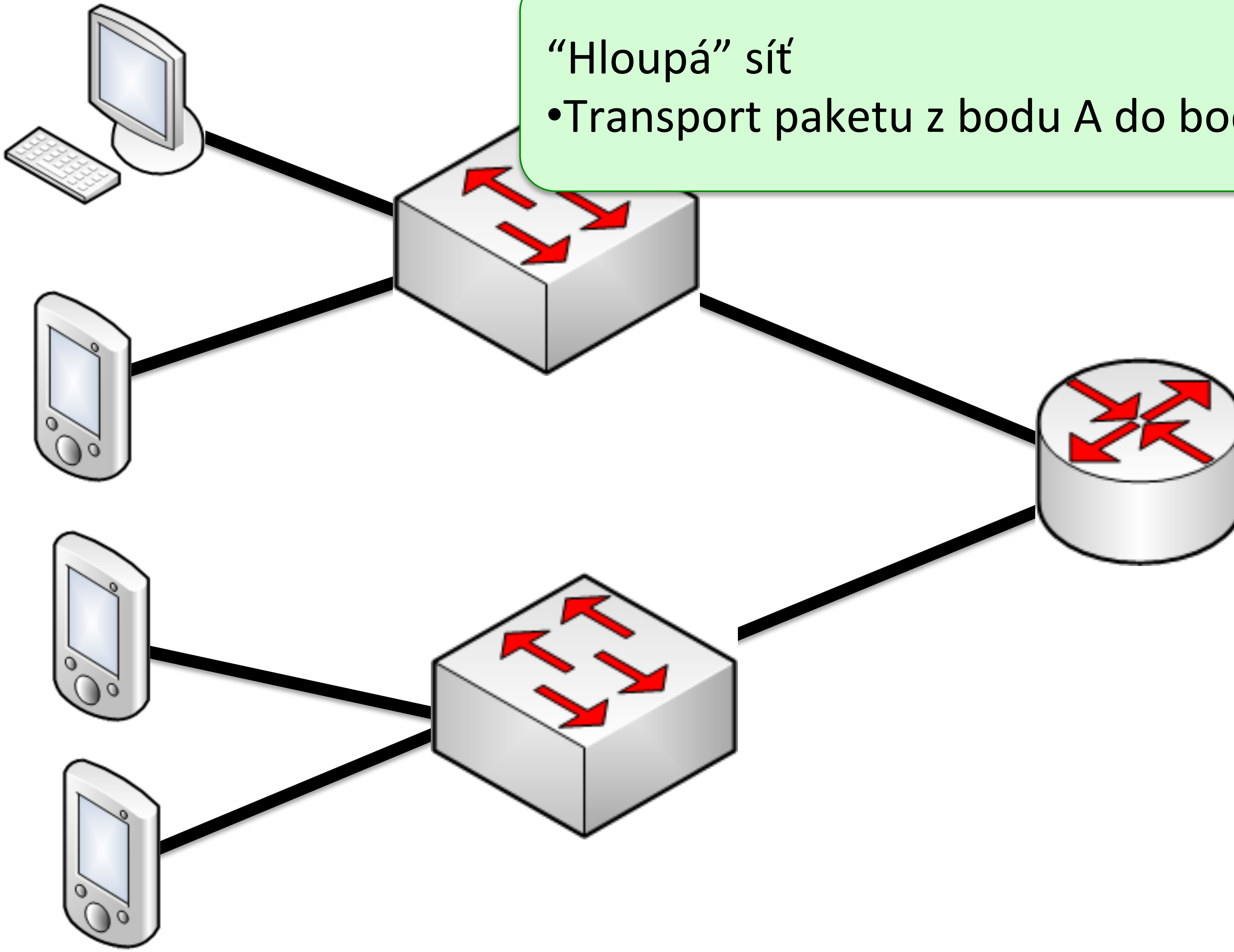
- Navazování spojení
- Správa relací
- Řízení toků
- Ukončování spojení
- …




“Chytrá” koncová zařízení
•Navazování spojení
•Správa relací
•Řízení toků
•Ukončování spojení
•…

“Hloupá” síť

•Transport paketu z bodu A do bodu B



End-to-end principle (argument)

- Publikováno v roce 1981

Saltzer, J. H., D. P. Reed, and D. D. Clark, 1981

Maximum funkcionality by mělo být implementováno v **koncových** zařízeních. **Mezilehlá** zařízení by měla realizovat pouze naprosto **nezbytné** funkce.

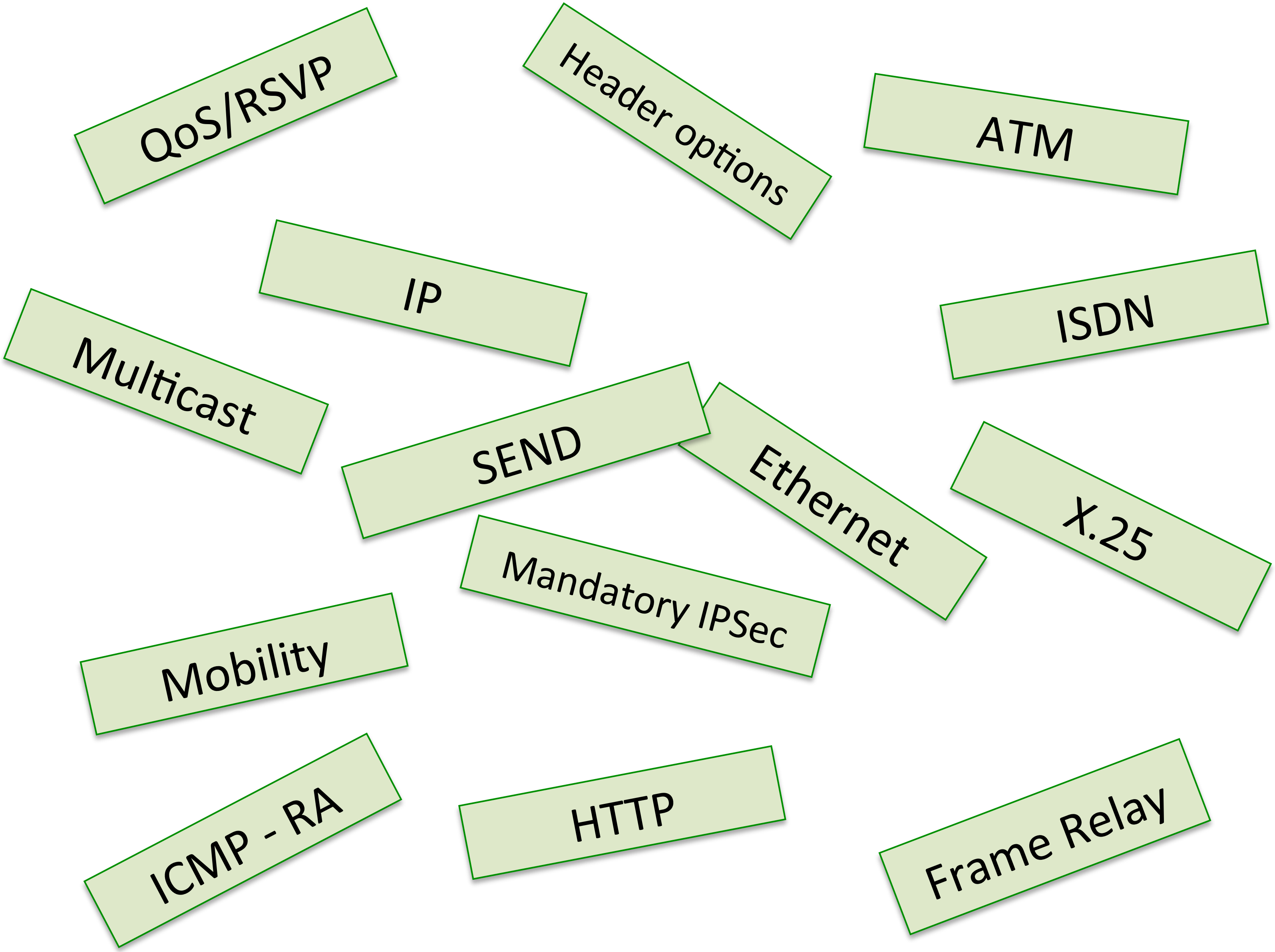
Architektura umožňuje rozvoj nových technologií bez zasahování do síťové infrastruktury.

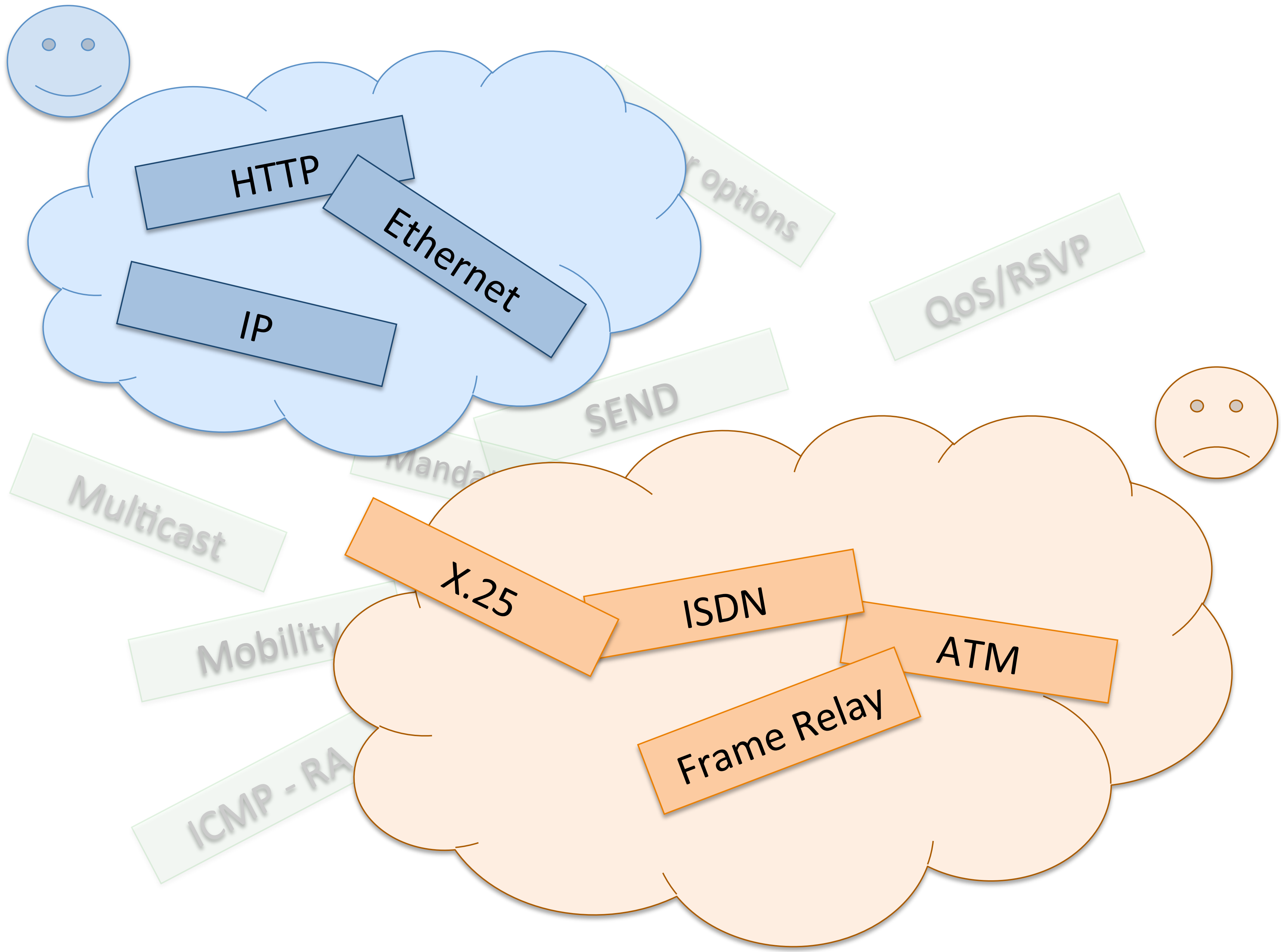
Ford
PIAA
SUPER RACING
PIAA
SUPER RACING

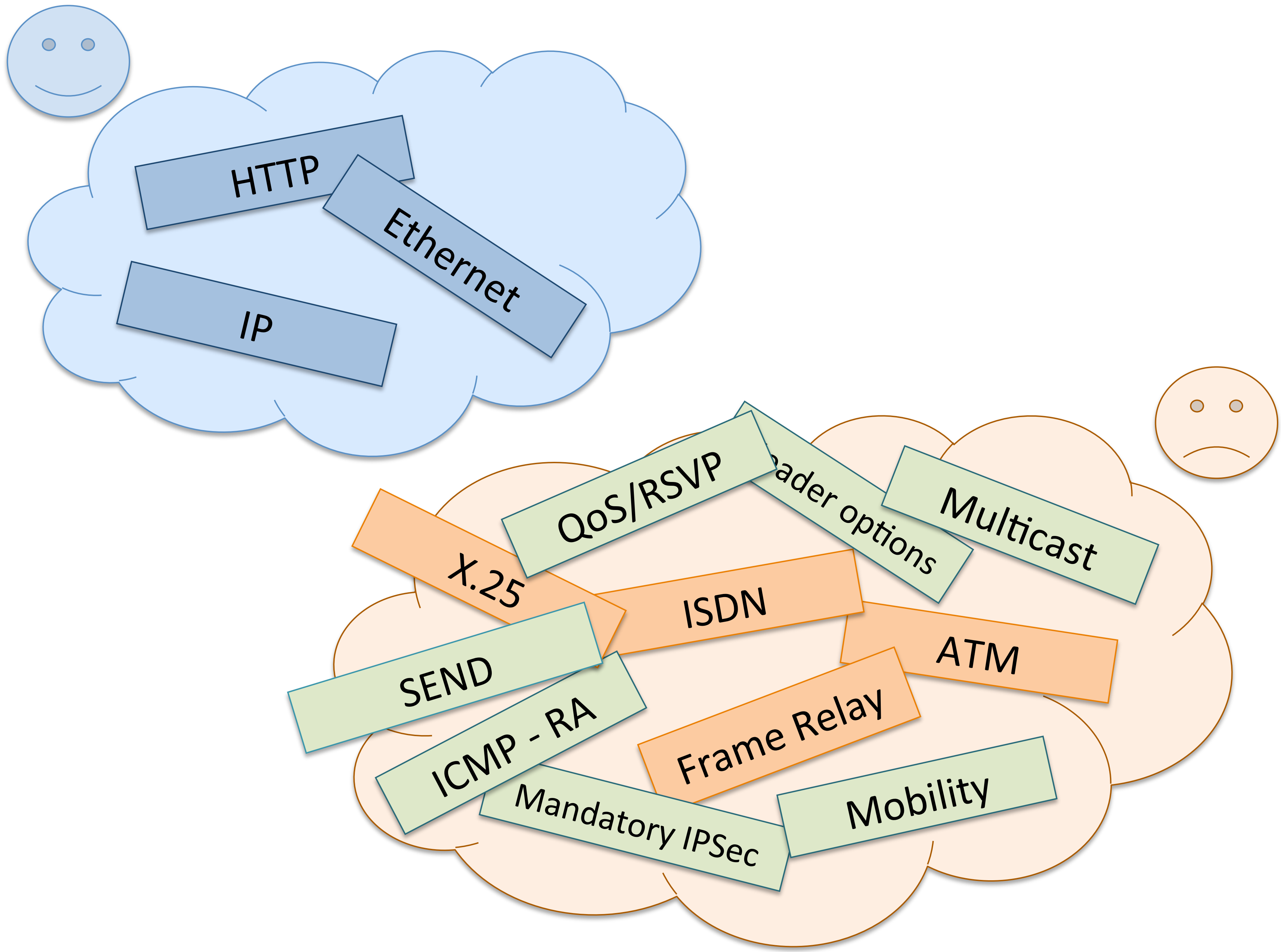
Dva pohledy na návrh protokolu

- Dáme tam vše -> určitě se nám to bude hodit
  - Je mnohem složitější eliminovat neužitečnou funkcionalitu
  - Pokud se něco masově nepoužívá neznamená to, že to nikdy nikdo nepoužil
  - Jednou špatně/nevhodně navržené části protokoku je prakticky nemožné změnit : rozšířené hlavičky, SLAAC, DHCPv6, 6to4

- Začneme s minimem a pak se uvidí
  - Přidání nové funkcionality je přirozený proces
    - First hop security, Rozšíření TCP, IPSEC-IPv4, NAT
  - Standardizace: stačí prokázat, že věc je používaná
  - Musím řešit kompatibilitu
  - Snadná implementace a tedy progres síťových technologií (b/s: 10M -> 100M –> 1G -> 10G -> 100G)


QoS/RSVP
Header options
ATM
IP
ISDN
Multicast
SEND
Ethernet
X.25
Mandatory IPSec
Mobility
ICMP - RA
HTTP
Frame Relay


HTTP
Ethernet
IP
options
QoS/RSVP
SEND
Multicast
Mobility
ICMP - RA
X.25
ISDN
ATM
Frame Relay


HTTP
Ethernet
IP
QoS/RSVP
ader options
Multicast
X.25
ISDN
ATM
SEND
ICMP - RA
Frame Relay
Mandatory IPSec
Mobility

Vrstvy

Ale vždyť to už přece známe

Application

Presentation

Session

Transport

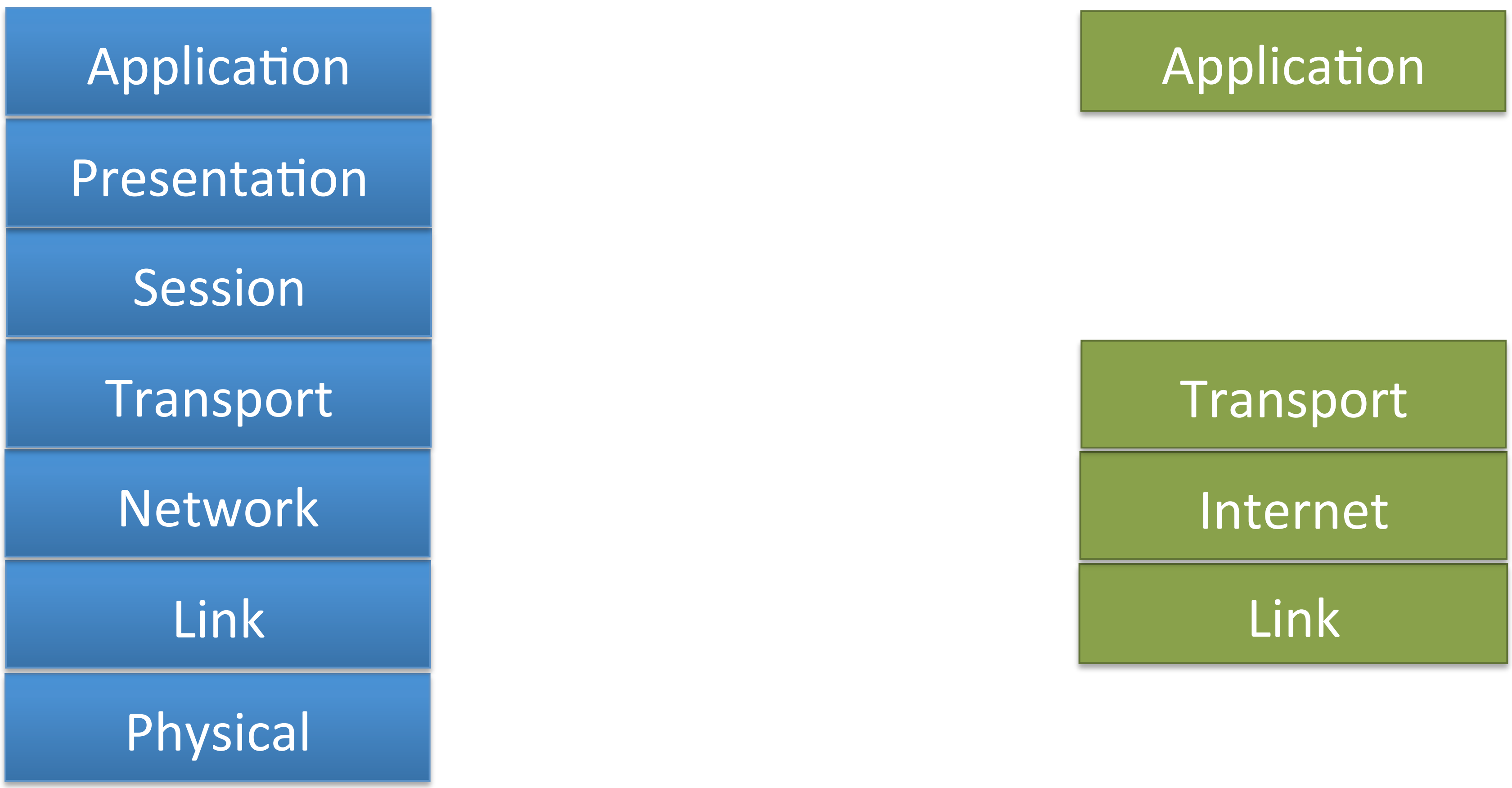
Network

Link

Physical

ISO/OSI

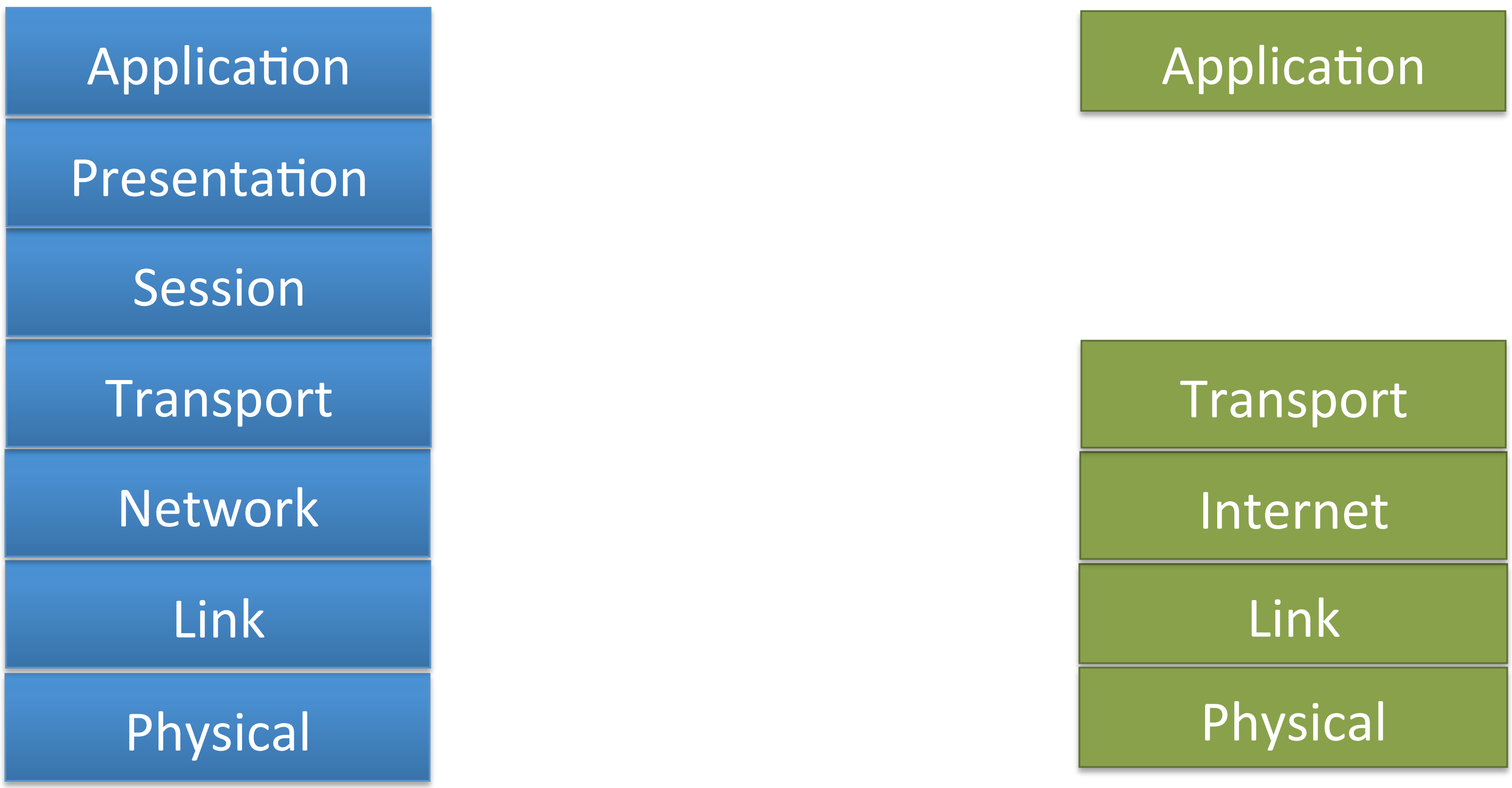
Ale vždyť to už přece známe



ISO/OSI

TCP/IP

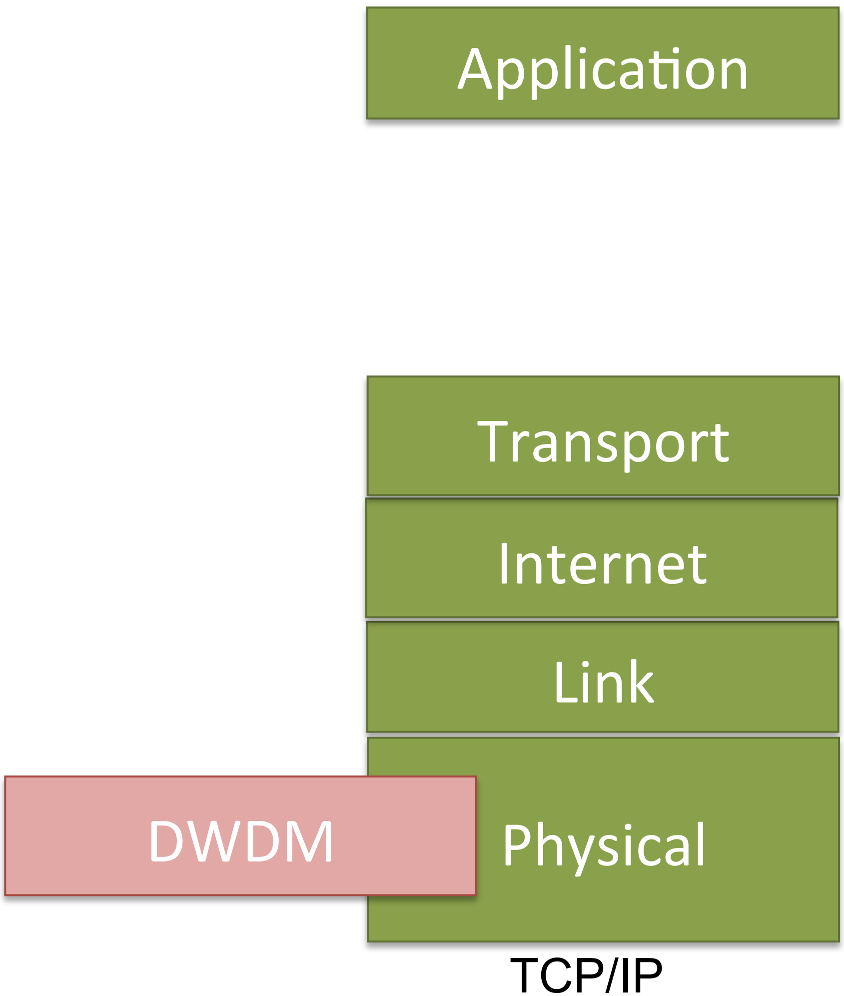
Ale vždyť to už přece známe



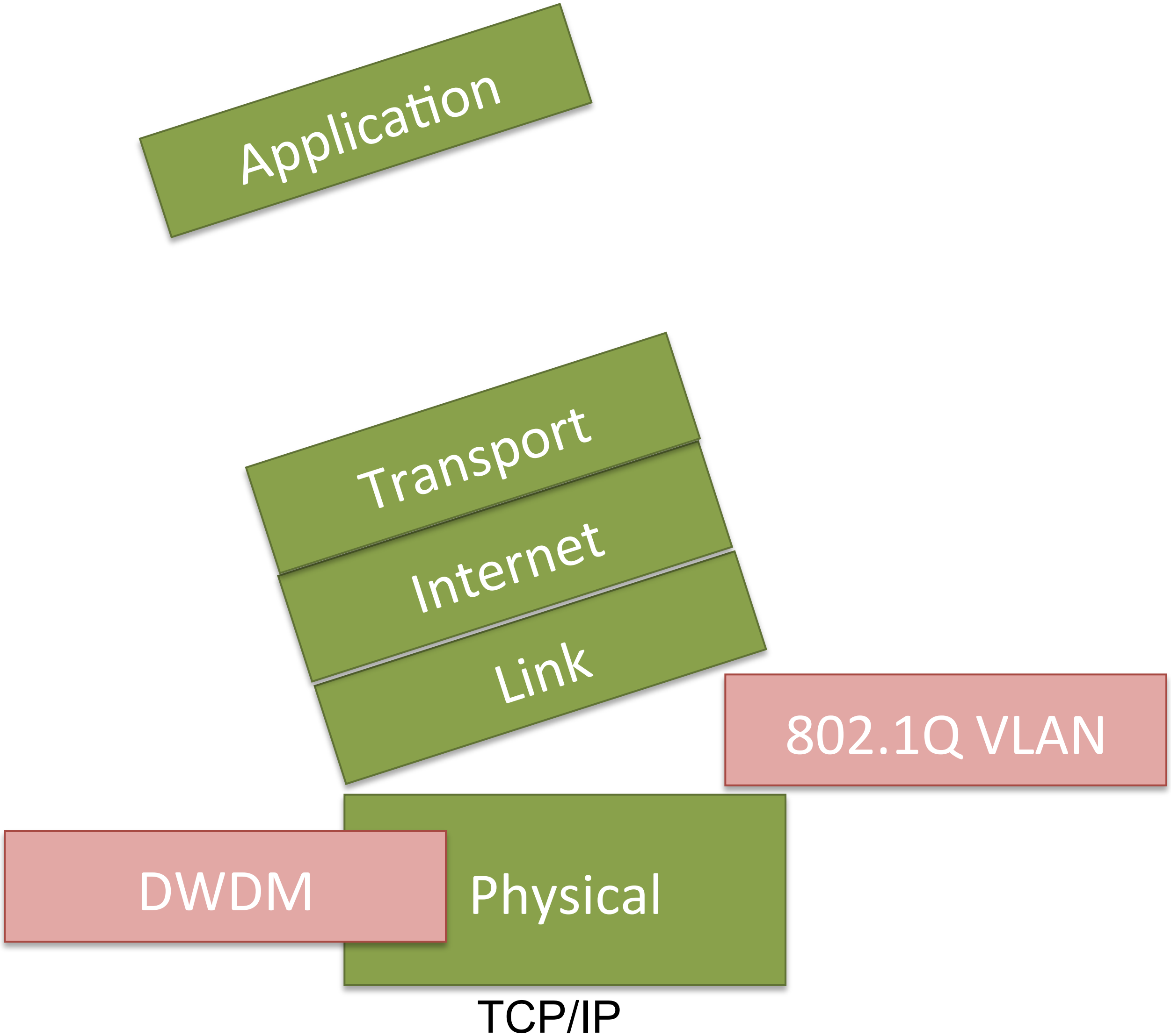
ISO/OSI

TCP/IP

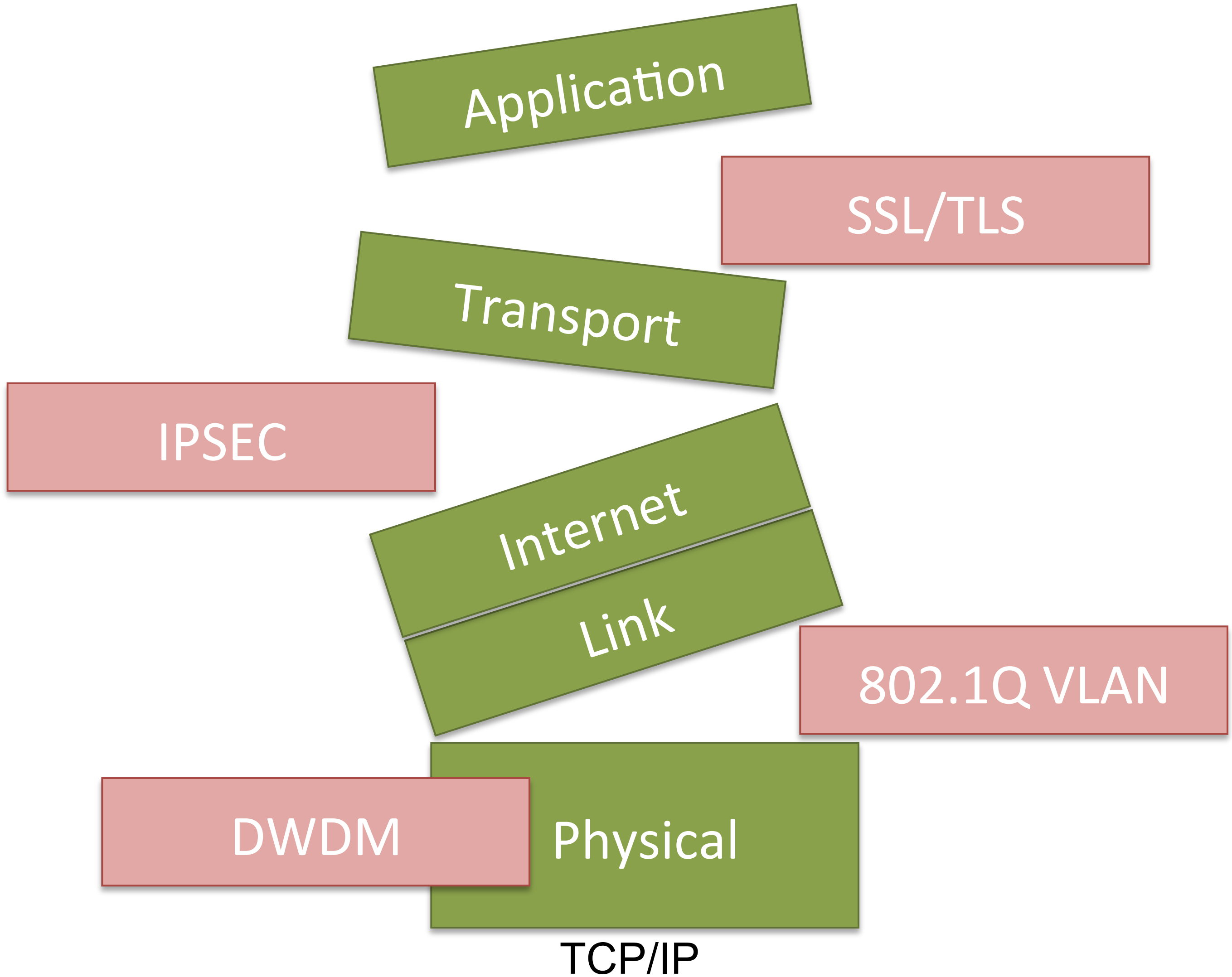
Ale vždyť to už přece známe



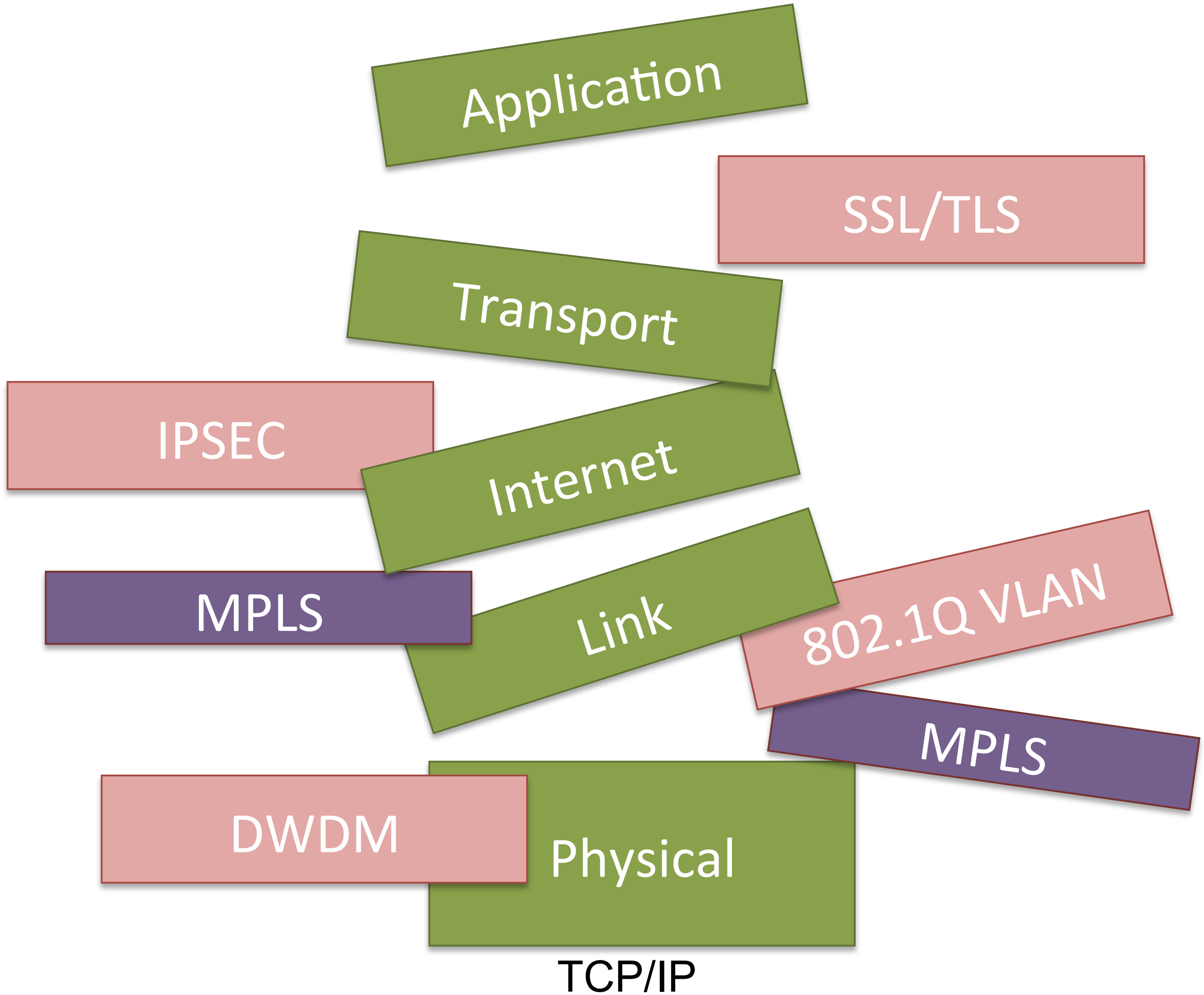
Ale vždyť to už přece známe



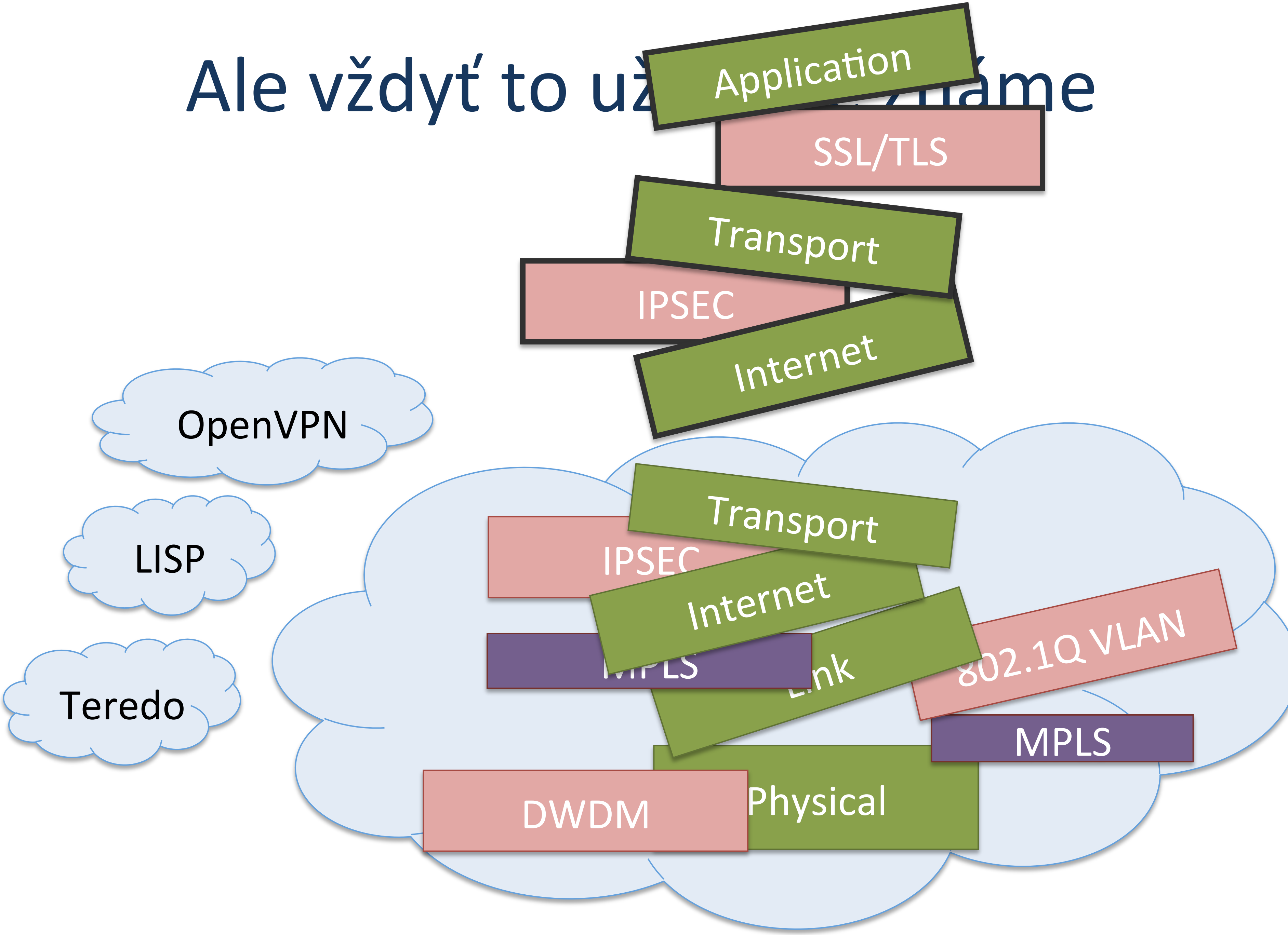
Ale vždyť to už přece známe



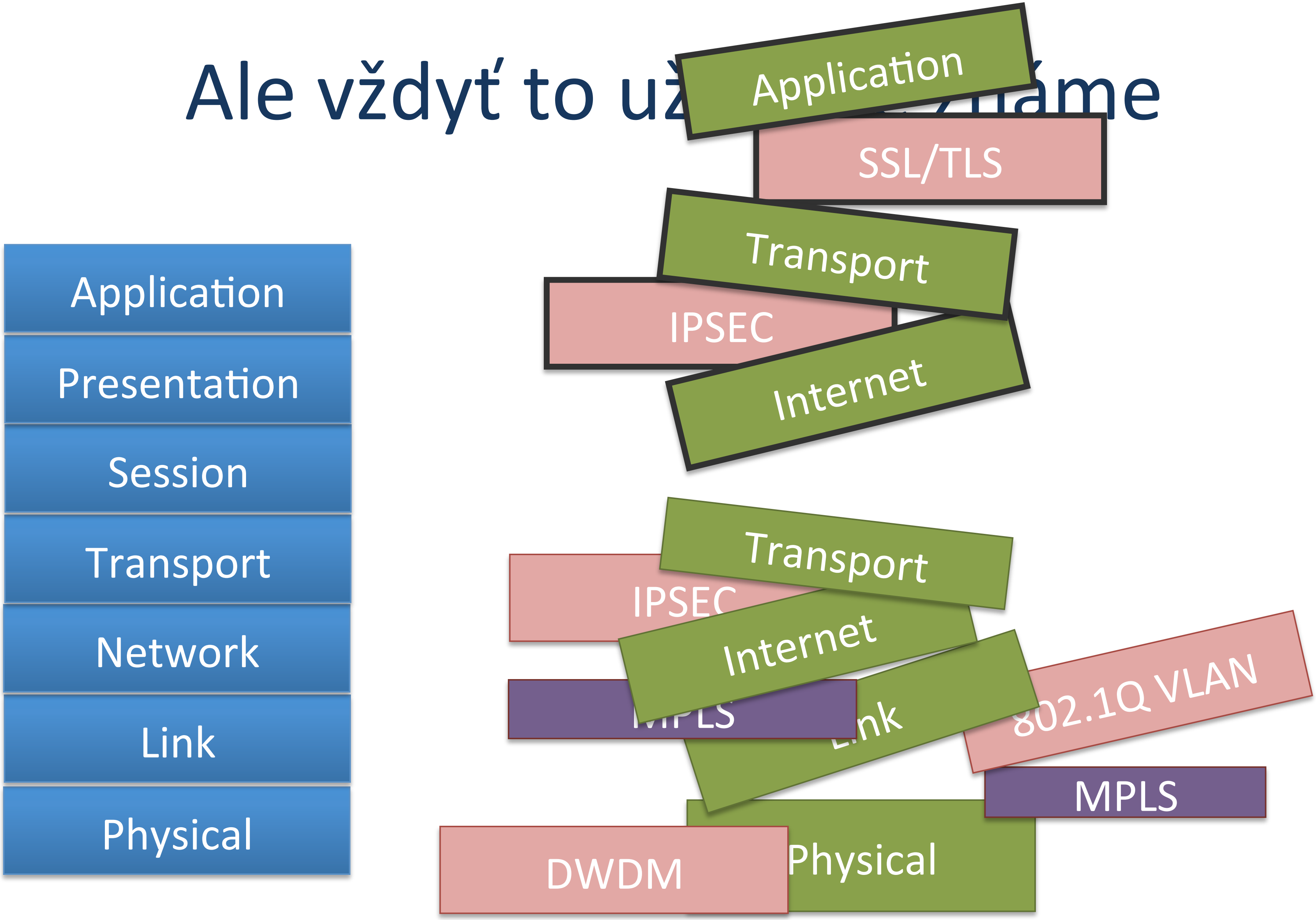
Ale vždyť to už přece známe



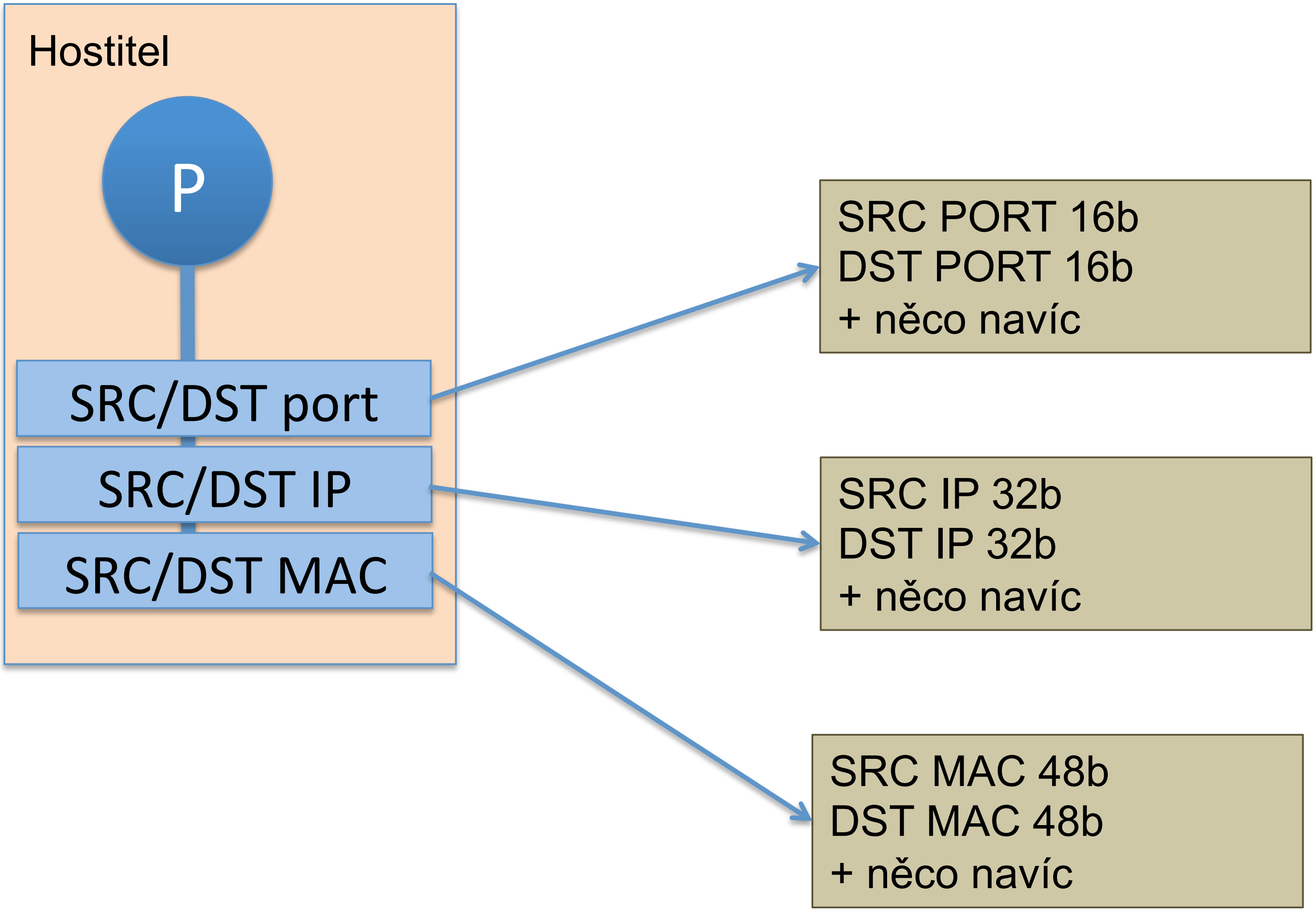
Ale vždyť to už známe



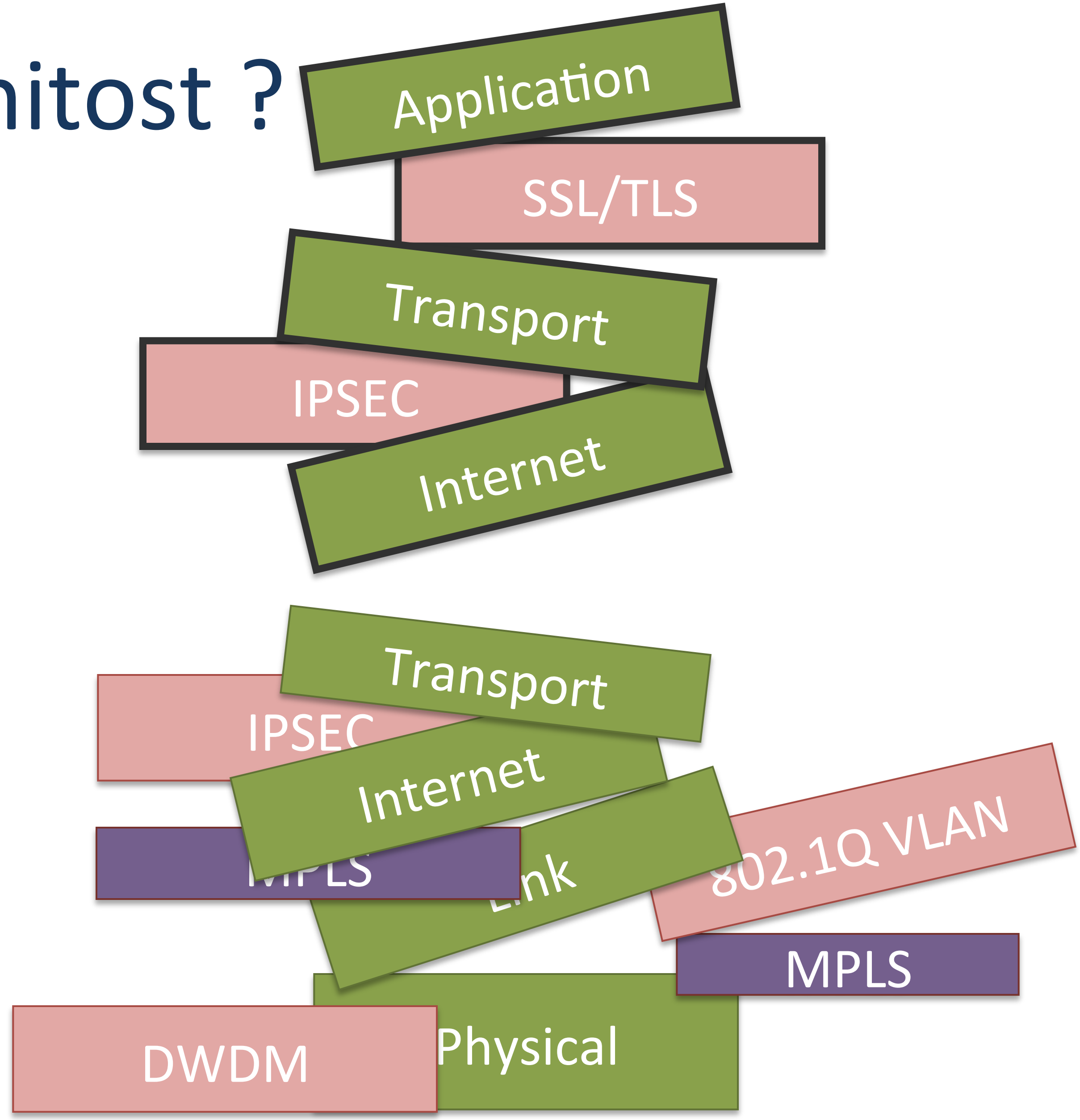
Ale vždyť to už známe

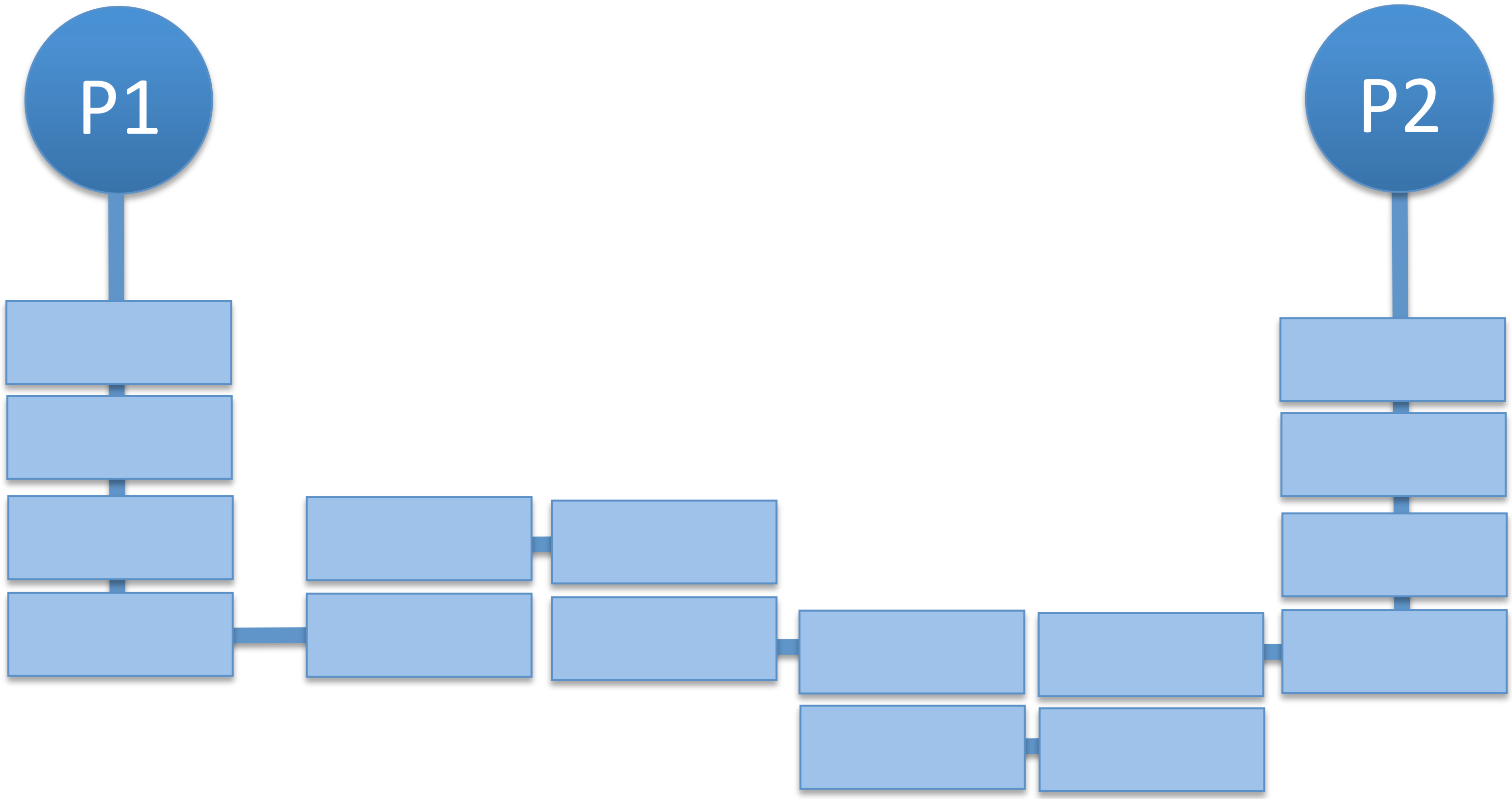


ISO/OSI


Hostitel
P
SRC/DST port
SRC/DST IP
SRC/DST MAC
SRC PORT 16b
DST PORT 16b
+ něco navíc
SRC IP 32b
DST IP 32b
+ něco navíc
SRC MAC 48b
DST MAC 48b
+ něco navíc

Nějaká zákonitost ?





- Skutečně musíme mít různé vrstvy, které dělají totéž?

RINA

A Better Network Structure

Převzato z:

Recursive InterNetwork Architecture

http://csr.bu.edu/rina/index.html

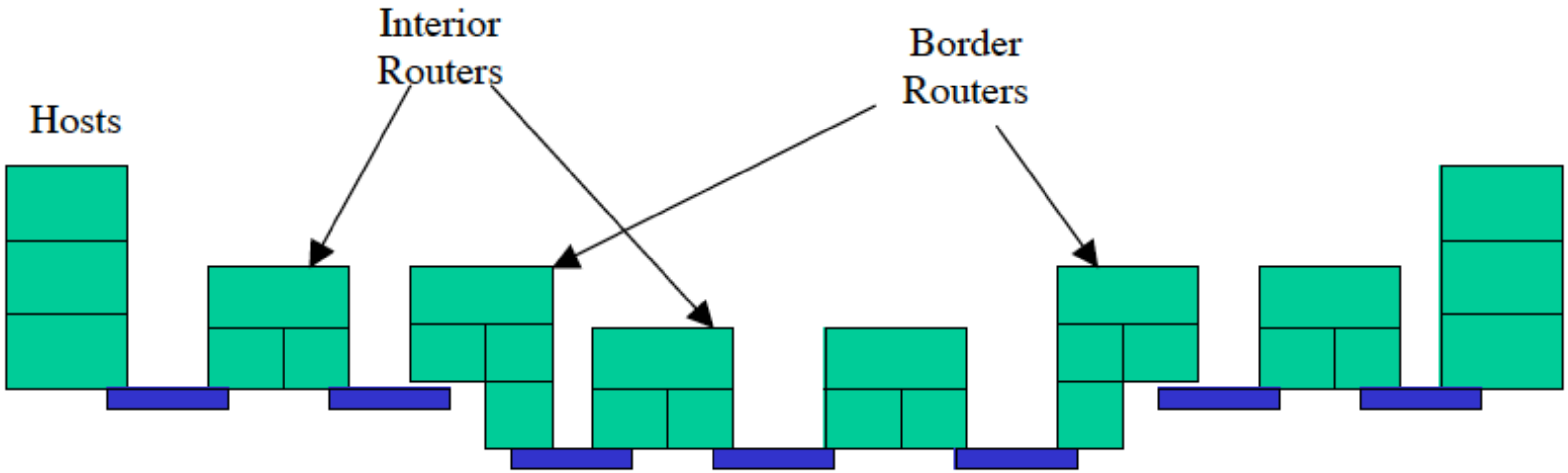
John Day, Ibrahim Matta, Karim Mattar

Metropolitan College College of Arts & Science

Computer Science, Boston University

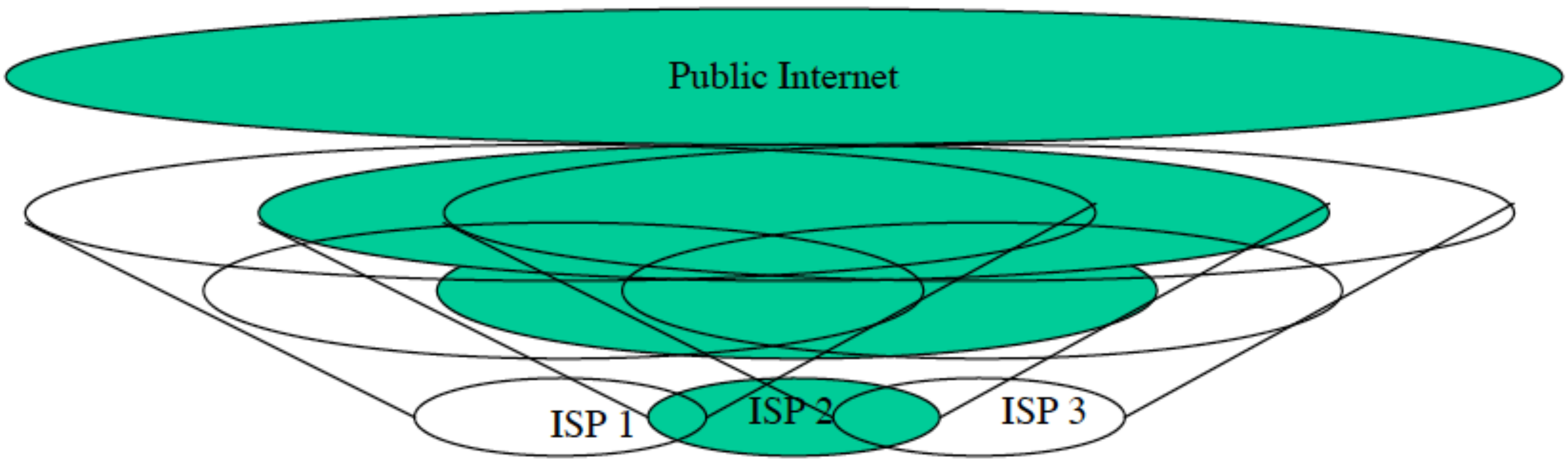
fday, matta, kmattarg@bu.edu

3 základní druhy zařízení



- Koncová zařízení
- Vnitřní směrovače
- Hraniční směrovače

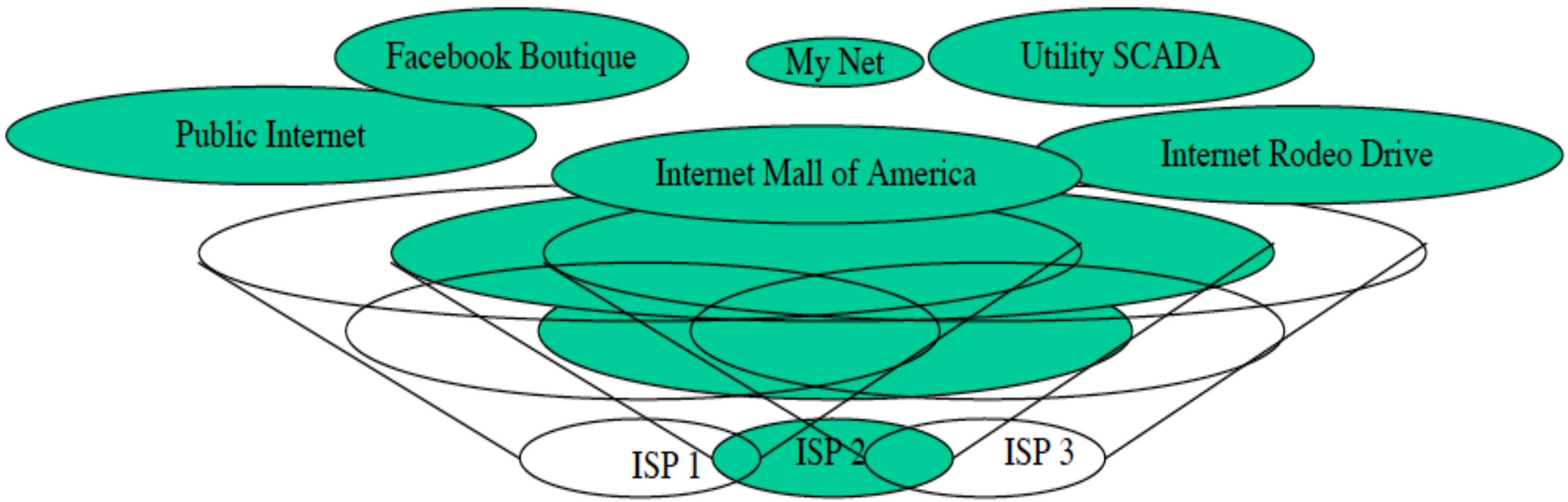
Struktura vrstev



RINA - vlastnosti

- Není nutný globální adresový prostor
- Každá vrstva (DIF) použije vlastní adresní schéma
- Zařízení uvnitř vrstvy jsou “skrytá” před okolním světem
- Nutný globální adresář – nemusí být však jeden

Současný Internet je jen jednou z entit



Amazon.com: Patterns in Network Architecture: A Return to Fundamentals (paperback): A Return to Fundamentals (9780137063383): John Day: Books

Amazon.com: Patterns in Netwo...

www.amazon.com/Patterns-Network-Architecture-Fundamentals-pape

Google

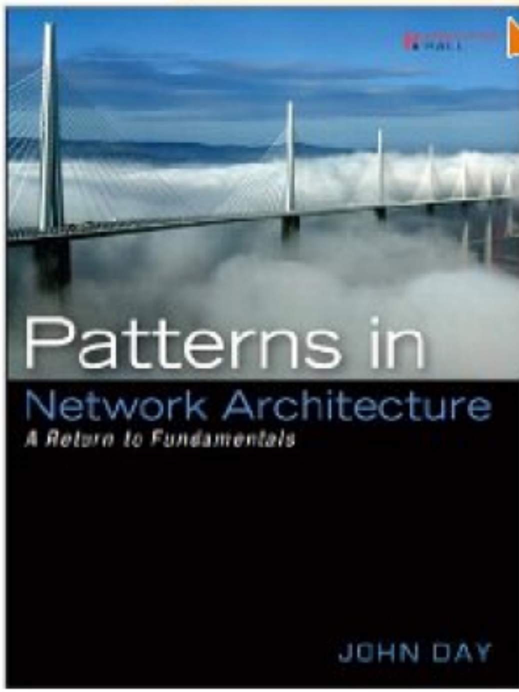
Shop by **Department**

Search Books **Go**

Hello. **Your**

Books Advanced Search New Releases Best Sellers The New York Times® Best Sellers Children's Books Textb

Click to LOOK INSIDE!



Click to open expanded view

Patterns in Network Architecture: A Return to Fundamentals (paperback): A Return to Fundamentals [Paperback]

John Day (Author)

(8 customer reviews)

List Price: ~~$64.99~~

Price: $43.10 & **FREE Shipping**. Details

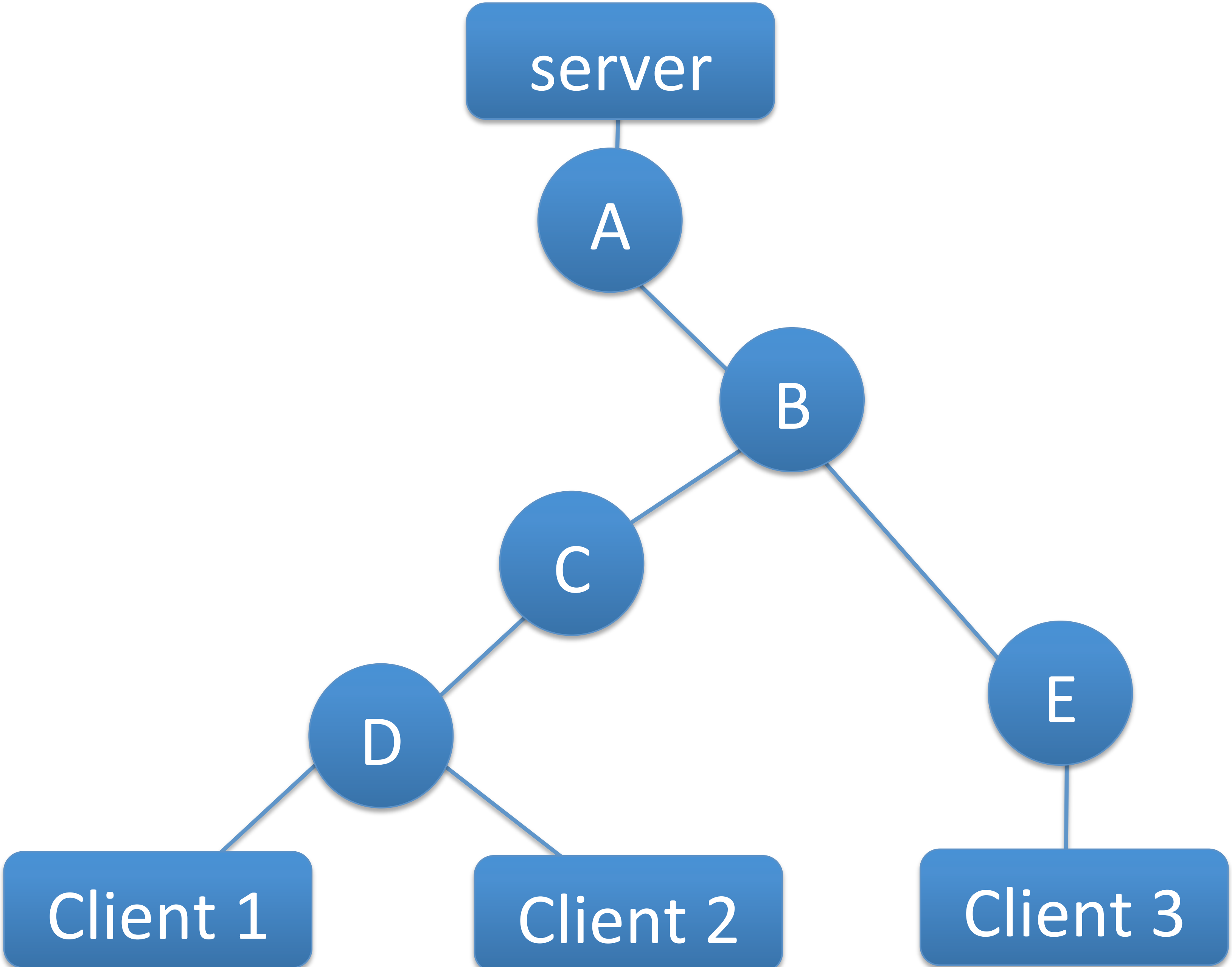
You Save: $21.89 (34%)

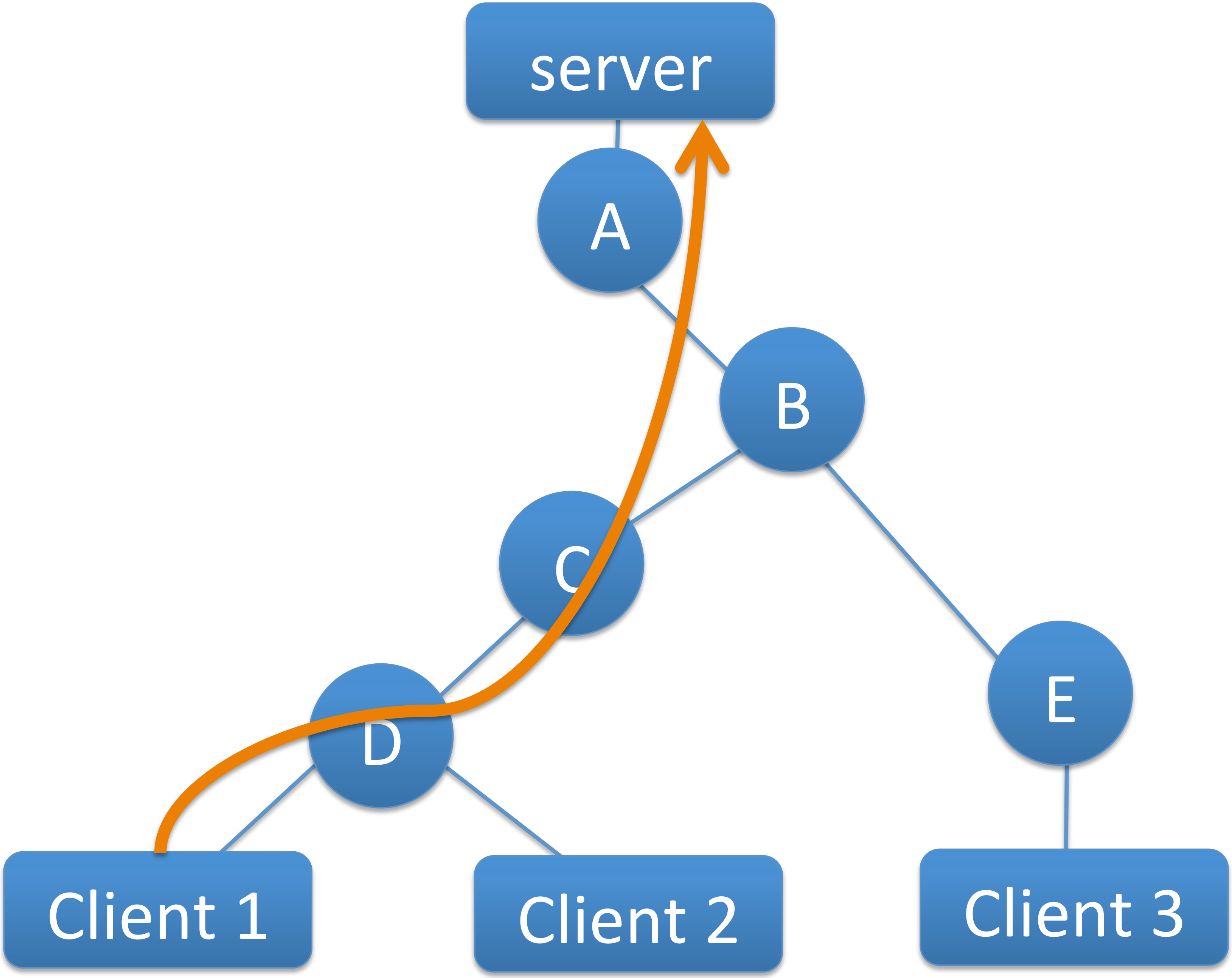
Only 1 left in stock (more on the way).

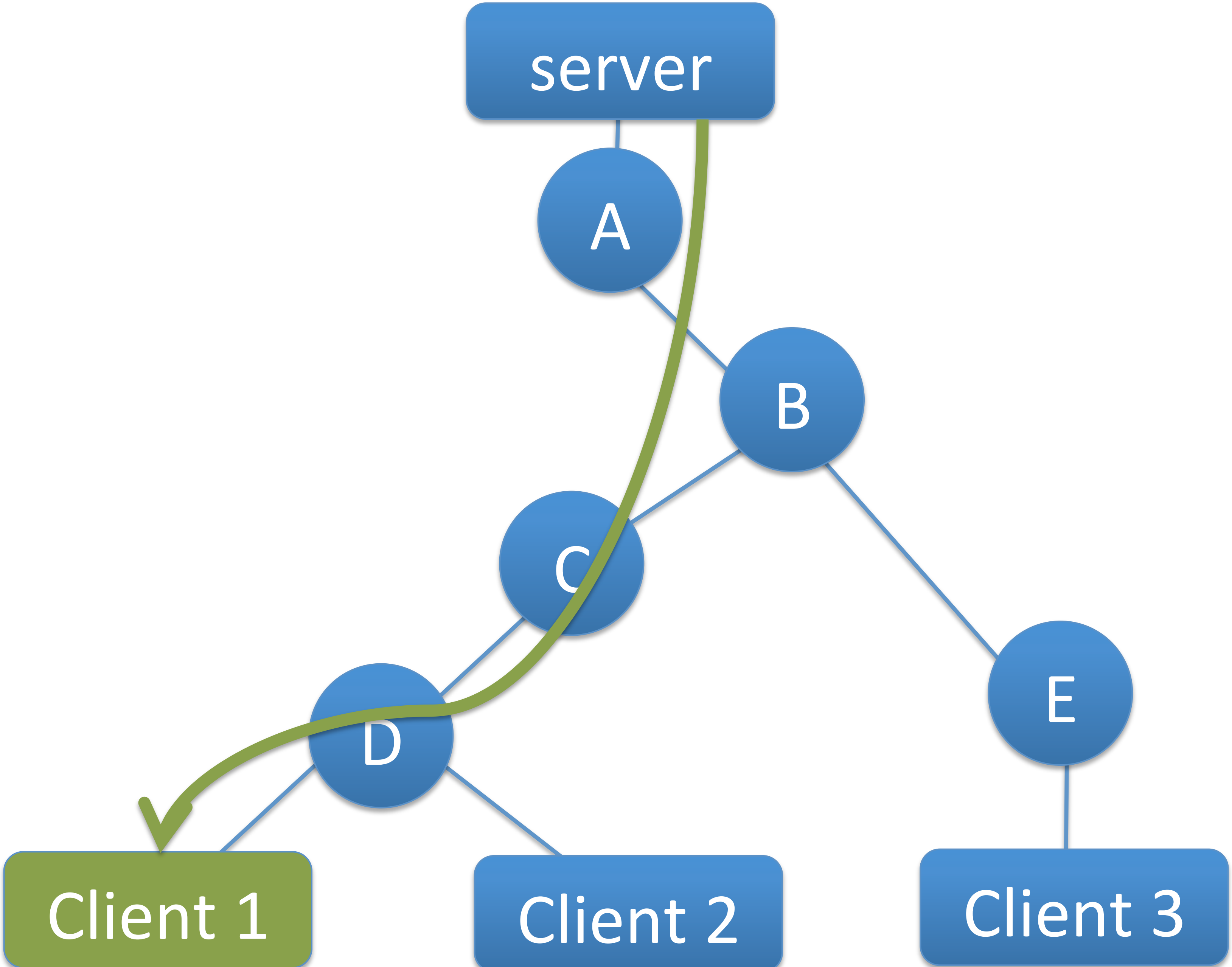
Ships from and sold by **Amazon.com**. Gift-wrap available.

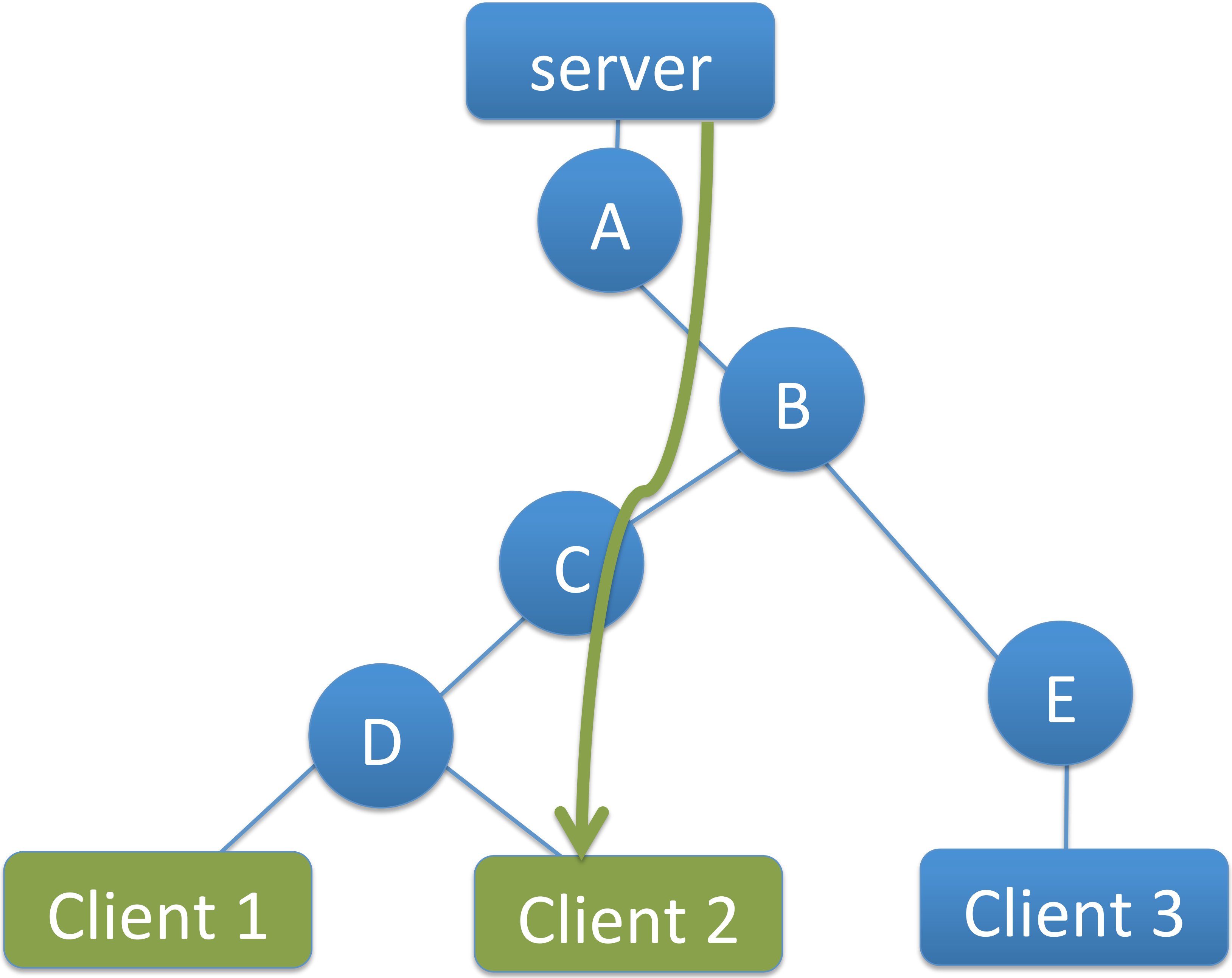
Want it Monday, May 6? Order within **4 hrs 8 mins** and choose **One-Day Shipping** at checkout. Details

18 new from $43.10 **13 used** from $30.00


server
A
B
C
D
E
Client 1
Client 2
Client 3


server
A
B
C
D
E
Client 1
Client 2
Client 3


server
A
B
C
D
E
Client 1
Client 2
Client 3


server
A
B
C
D
E
Client 1
Client 2
Client 3

Jsou “adresy” skutečně nejzávažnější problém Internetu ?

- Online distribuce například sportovního přenosu, výsledků voleb (1 mln diváků) ?
  - Unicast (1 000 000 x 1Mb/s = 1Tb/s) ?
  - Multicast (máte jej doma ?, Viděli jste jej někdy v reálné sítí ?, Jaké to bylo ?)
- A co třeba distribuce SW
  - Q1/2013 prodáno 47mln zařízení s iOS
  - Multicast (různé požadavky v různém čase)

Převzato z:

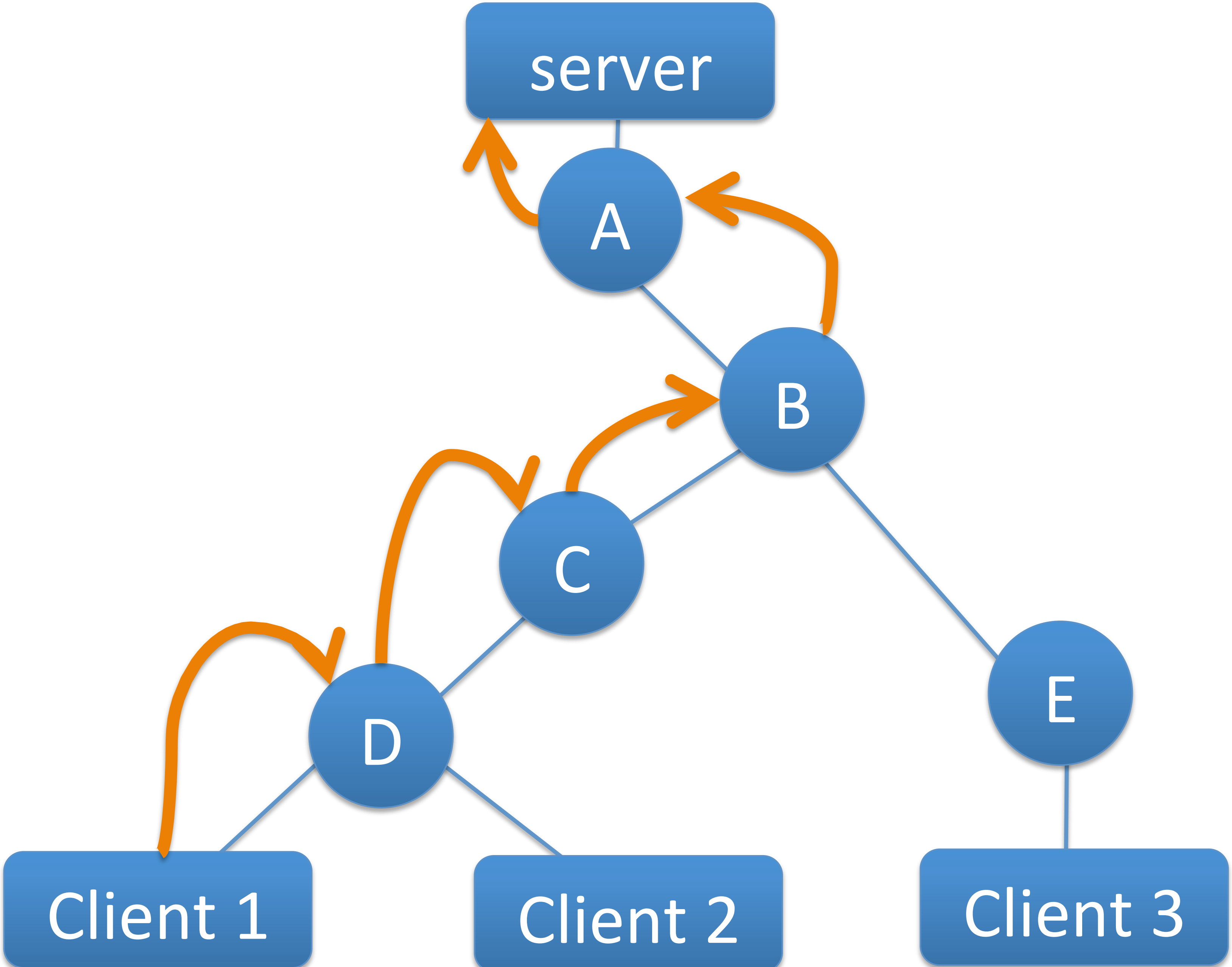
Networking Named Content

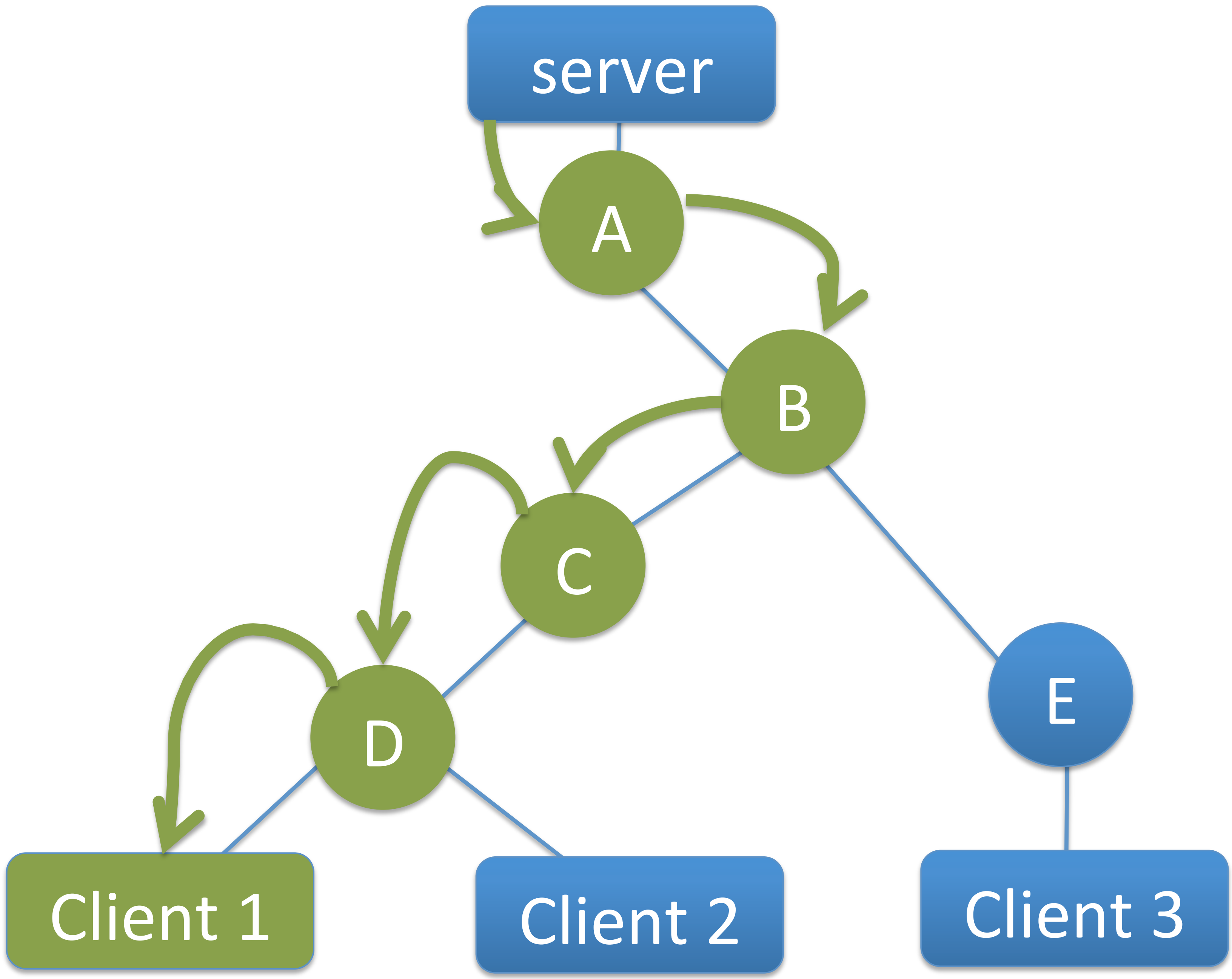
http://www.ccnx.org/documentation/

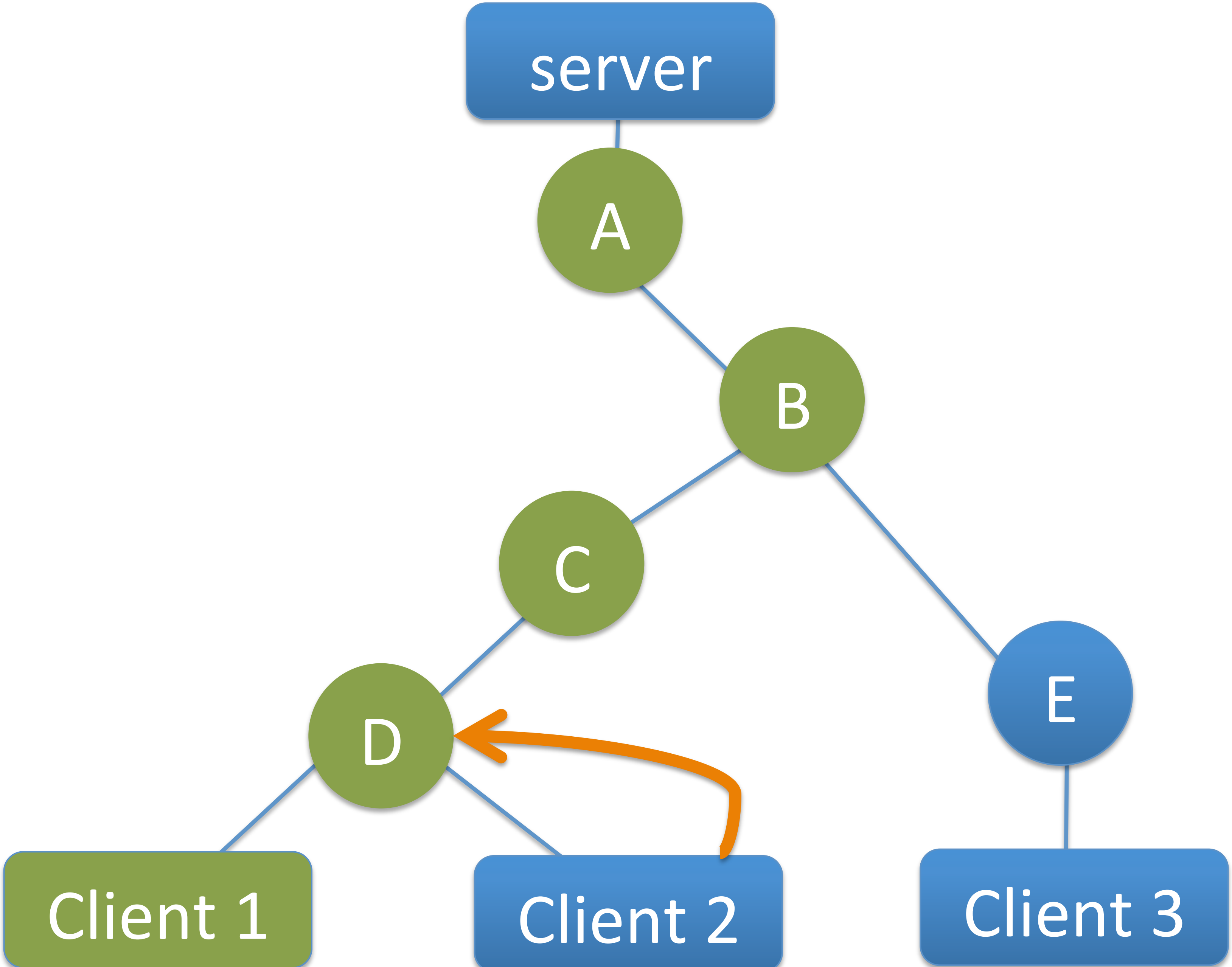
Van Jacobson Diana K. Smetters James D. Thornton Michael F. Plass Nicholas H. Briggs Rebecca L. Braynard

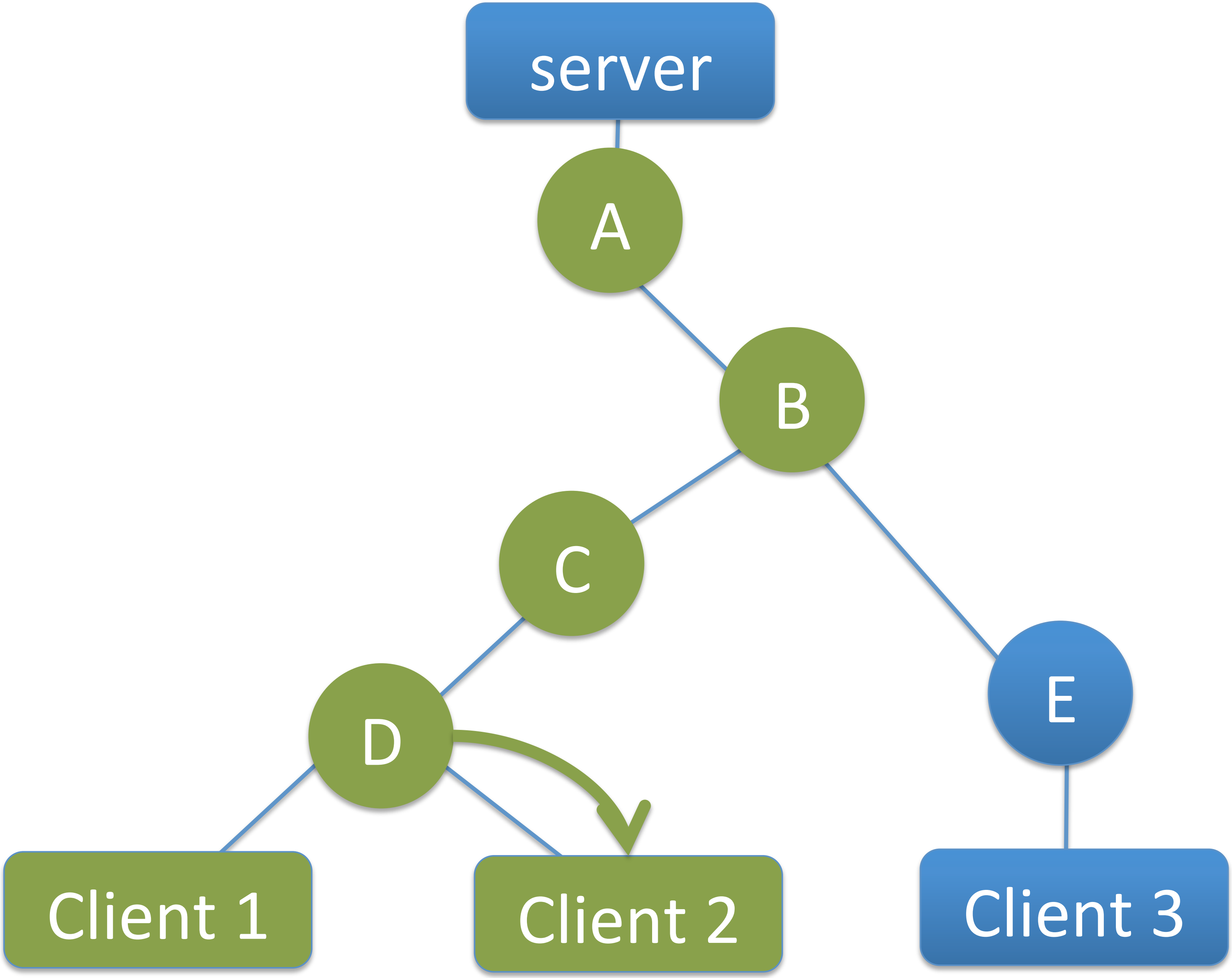
Palo Alto Research Center

Palo Alto, CA, USA

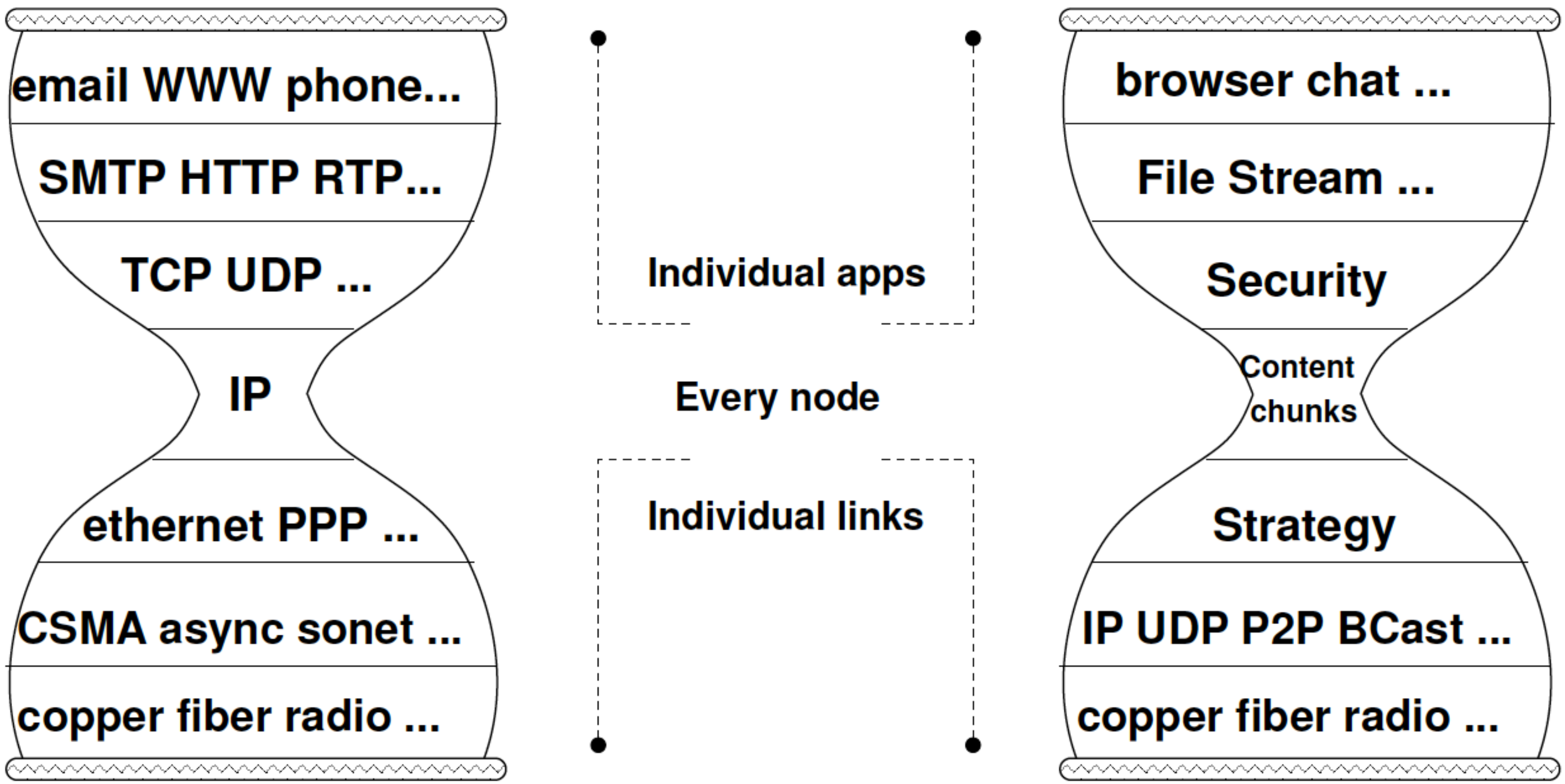

server
A
B
C
D
E
Client 1
Client 2
Client 3


server
A
B
C
D
E
Client 1
Client 2
Client 3

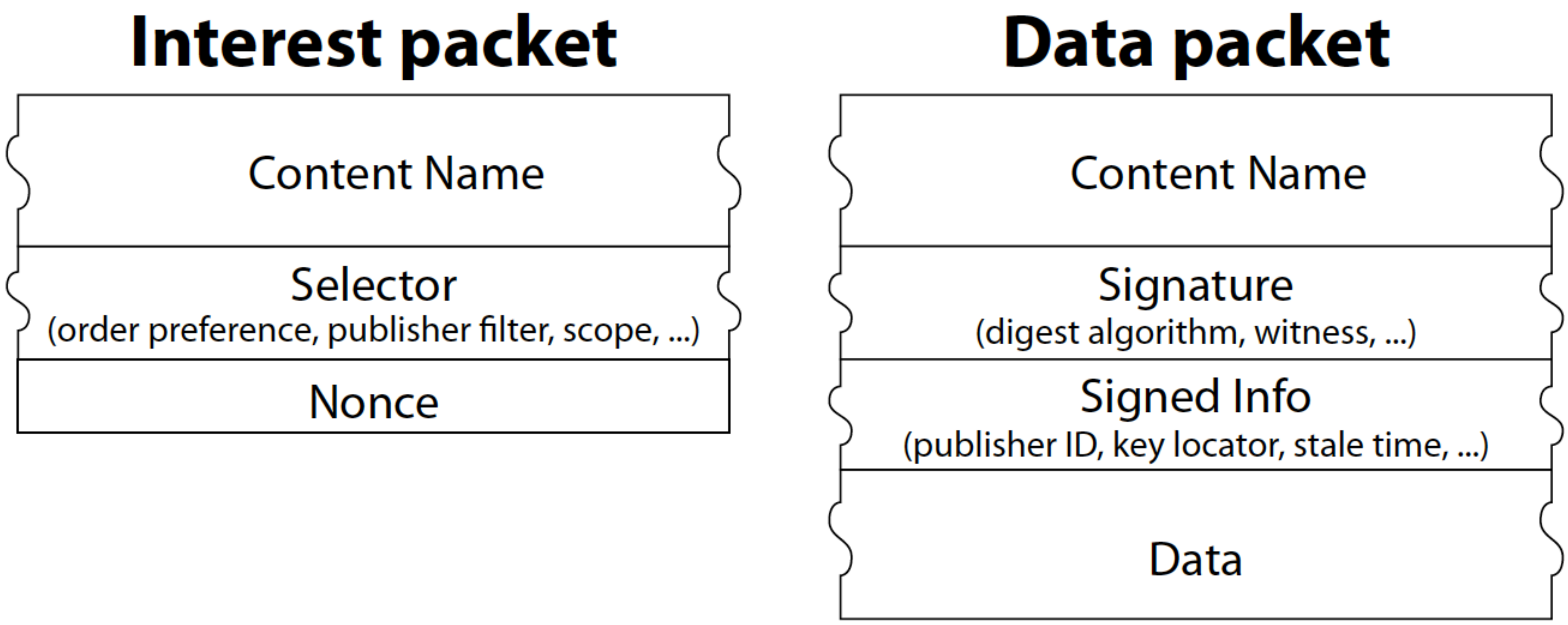

server
A
B
C
D
E
Client 1
Client 2
Client 3


server
A
B
C
D
E
Client 1
Client 2
Client 3

CCN – koncept sítě



CCN základní typy paketů



CCNx

CCNx

https://www.ccnx.org

Google

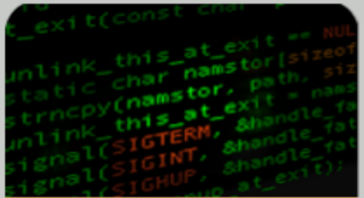
enter search term and press 'Enter'

ABOUT DOCUMENTATION SUPPORT DOWNLOAD FAQ CONTACT

Download

Documentation

Support



Developer

Latest Wiki Updates

- WebHome
- InstallingCCNx
- CCNxCon2012
- HowToPublishToThisWiki
- WebNotify

Subscribe

Mailing lists are perhaps the best way to get information on any open source project.

Subscribe to the mailing lists

Website Hosted By

Van Jacobson TechTalk at Google

PARC Research Fellow Van Jacobson spoke about Content-Centric Networking in a Google TechTalk in 20 ...

Slider by IWEBIX

CCNxCon 2013 Call for Submissions.

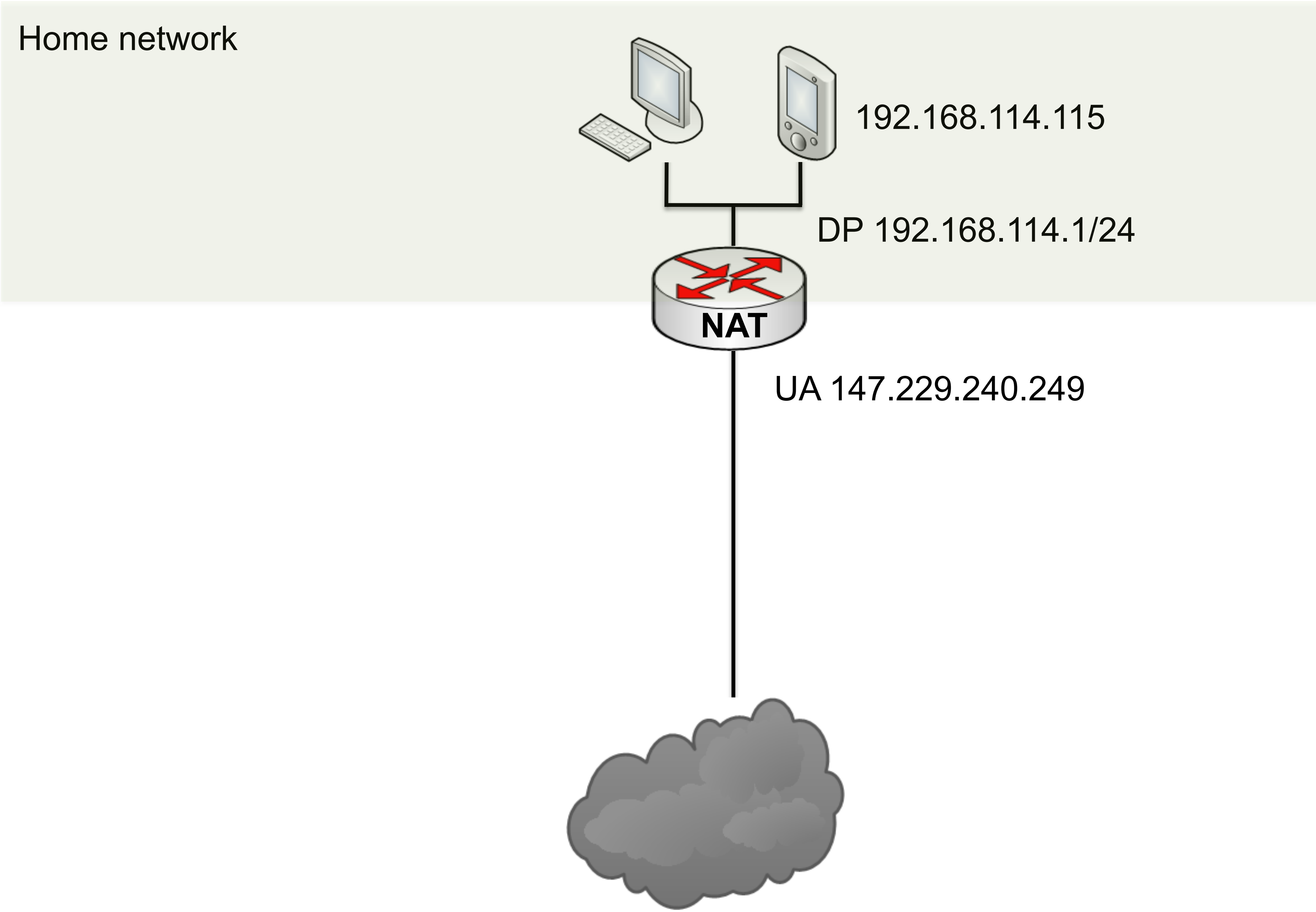
CCNxCon - CCNx Community Meeting September 2013

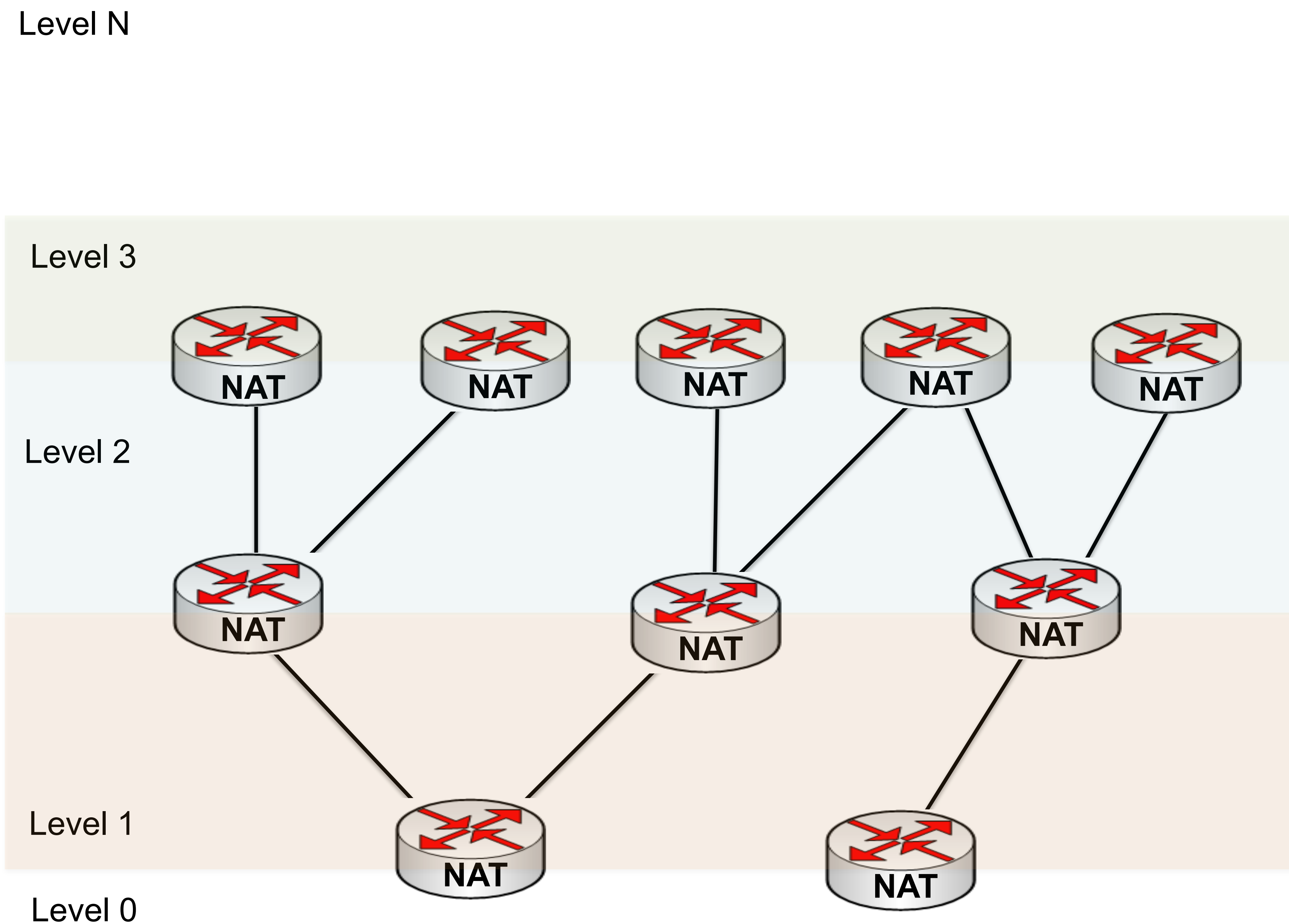
IP45

http://www.ip45.org/

IPv4.5 (IP45)

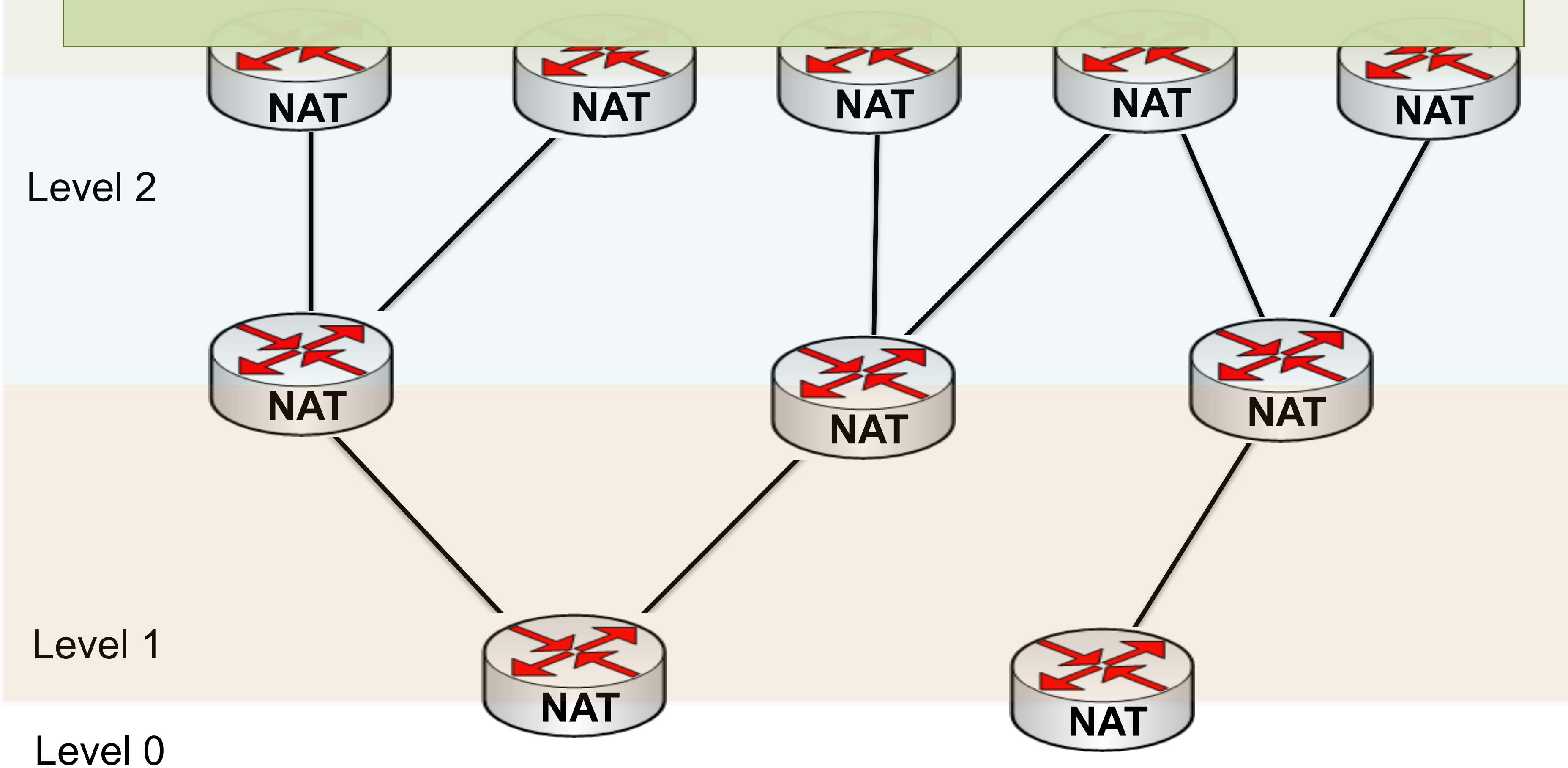
Brno University of Technology


Home network
192.168.114.115
DP 192.168.114.1/24
NAT
UA 147.229.240.249


Level N
Level 3
Level 2
Level 1
Level 0
NAT
NAT
NAT
NAT
NAT
NAT
NAT
NAT
NAT
NAT

Level N

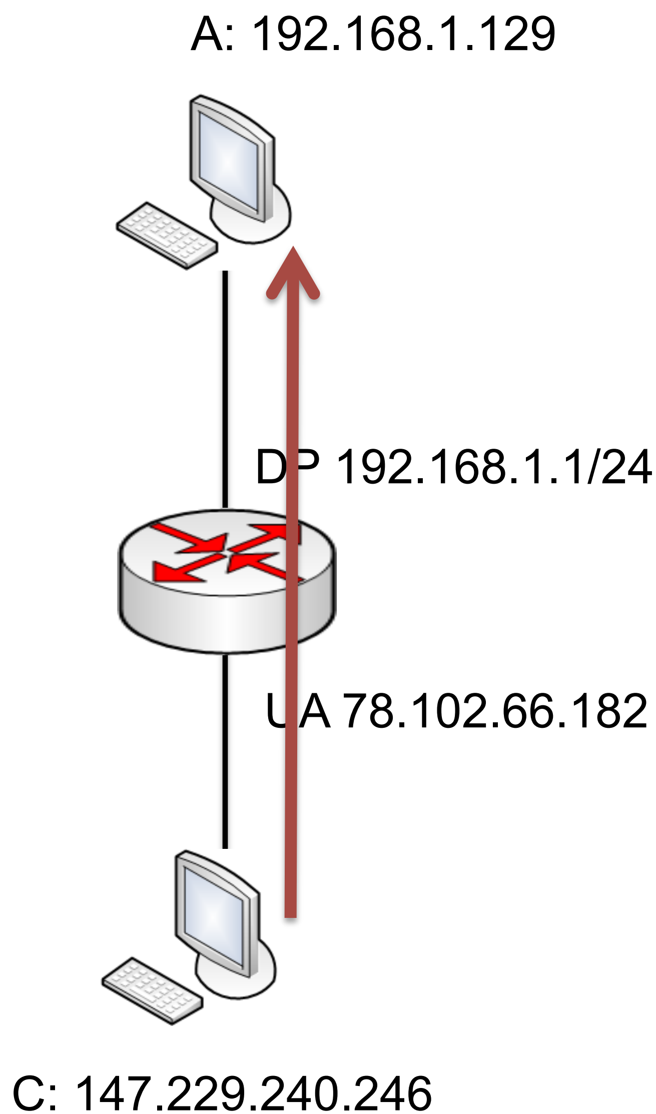
- Adresový prostor za NATem je nezávislý na nadřazeném adresovém prostoru
- NAT lze řetězit – prakticky nekonečně



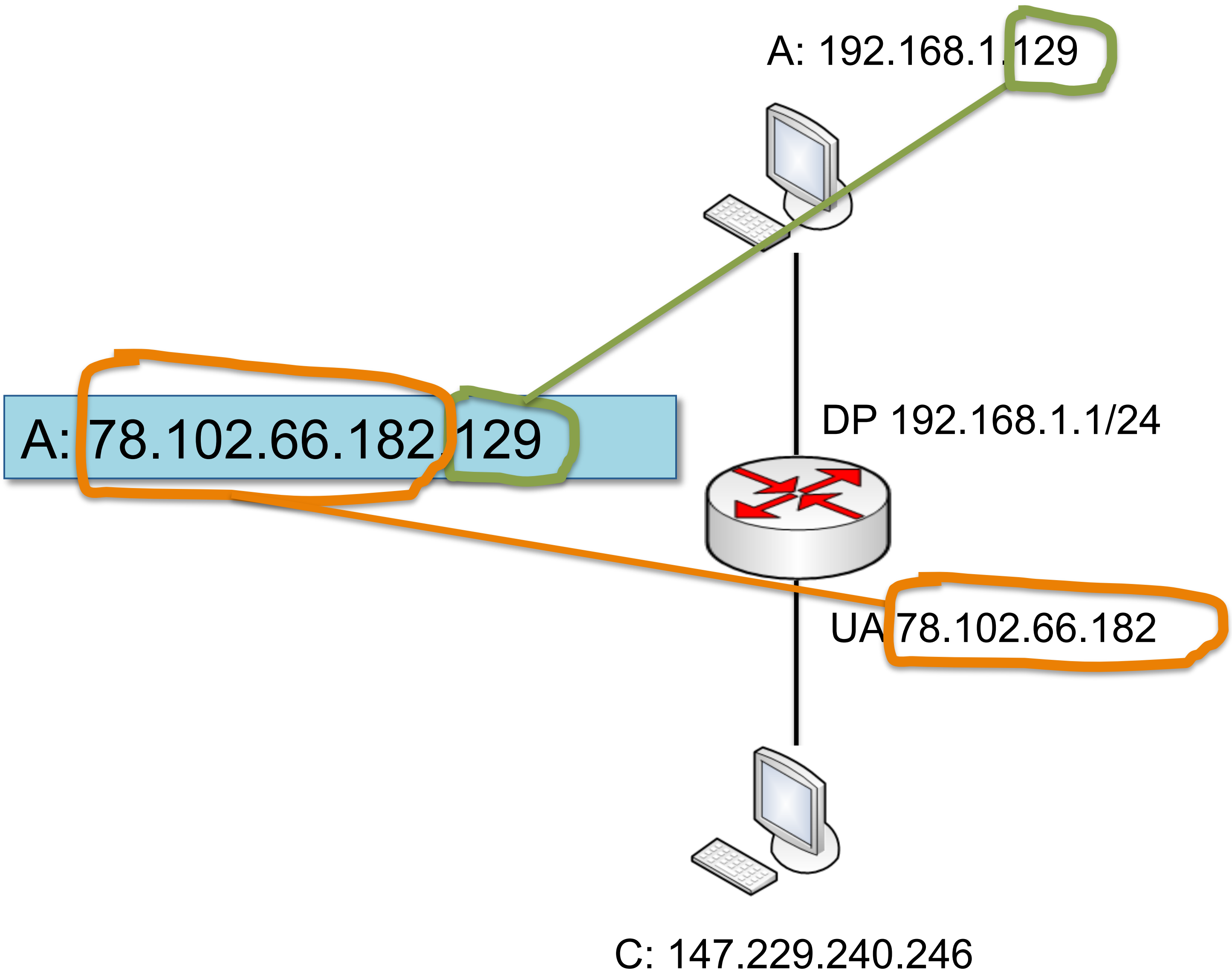
Level N

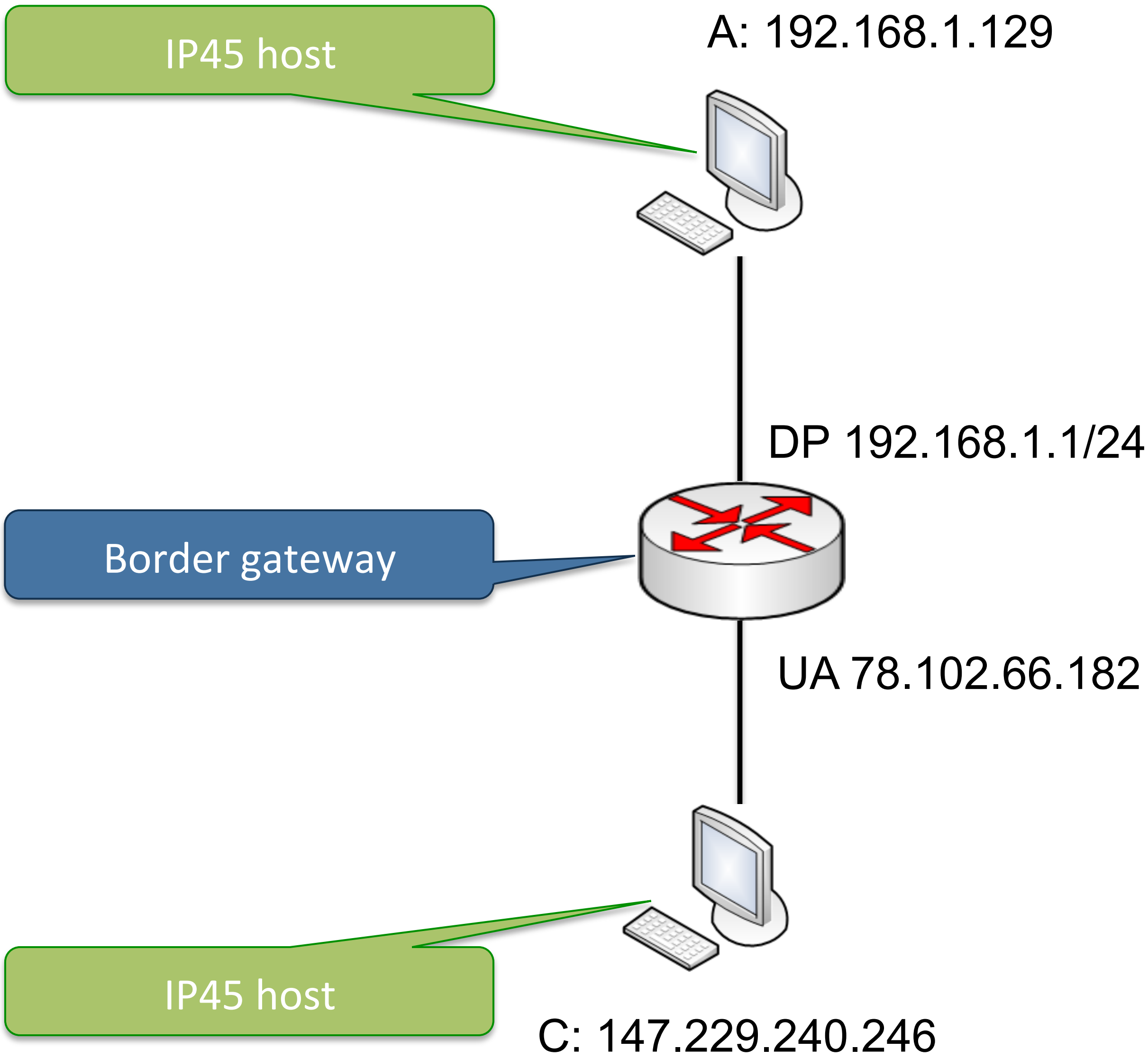
- Adresový prostor za NATem je nezávislý na nadřazeném adresovém prostoru
- NAT lze řetězit – prakticky nekonečně

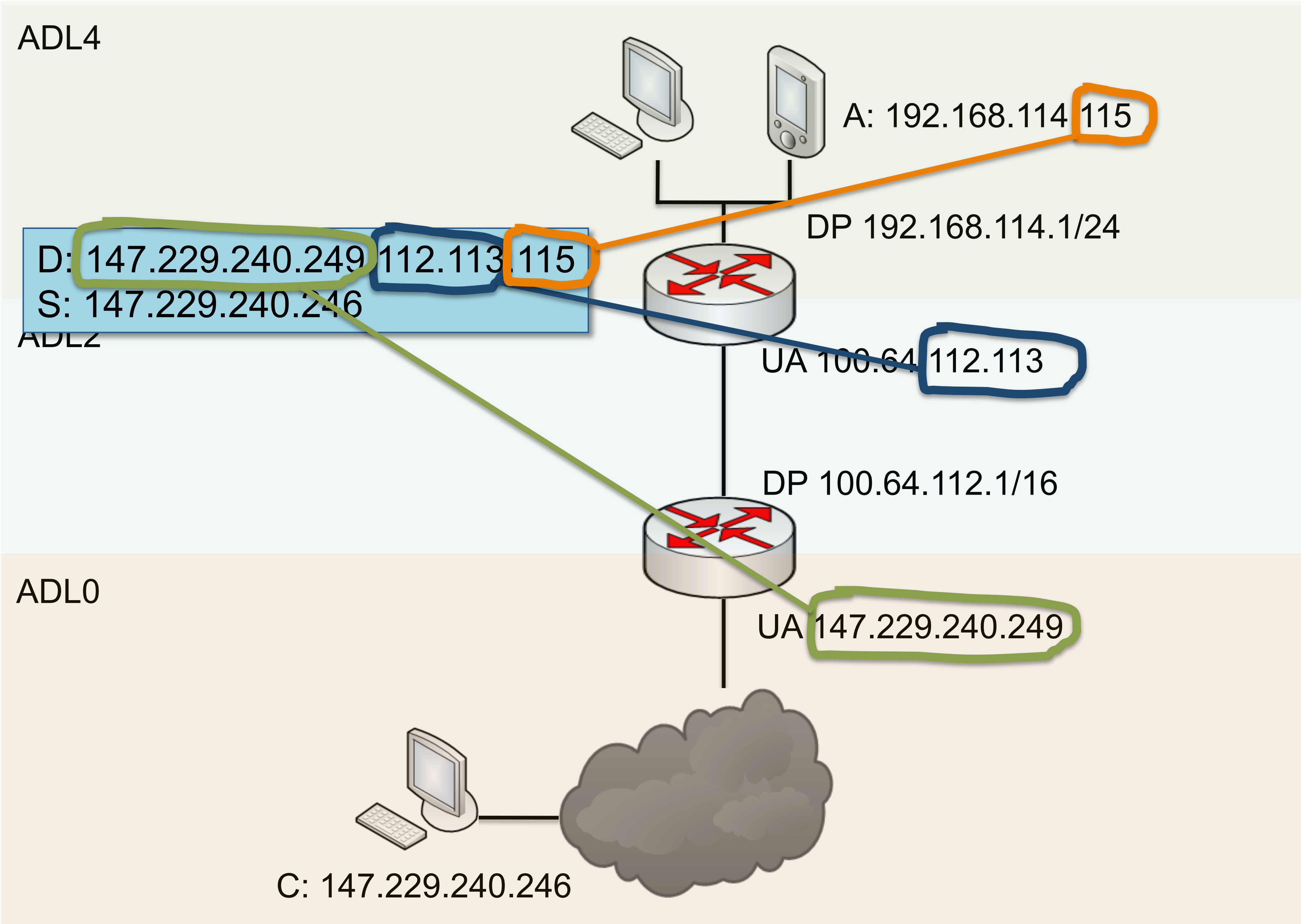
- Zařízení za NATem jsou obtížně adresovatelná
- NAT musí udržovat stavovou informaci
  - Jedno PC trvale udržuje cca 100 relací/flow
  - 10 tis. pc = 1 mln. relací/flow (flow cca 24B)
- NAT musí zpracovávat stavy
- Může dojít k vyčerpání kombinace srcaddr/**srcport**/dstaddr cca 60 tis.


A: 192.168.1.129
DP 192.168.1.1/24
UA 78.102.66.182
C: 147.229.240.246

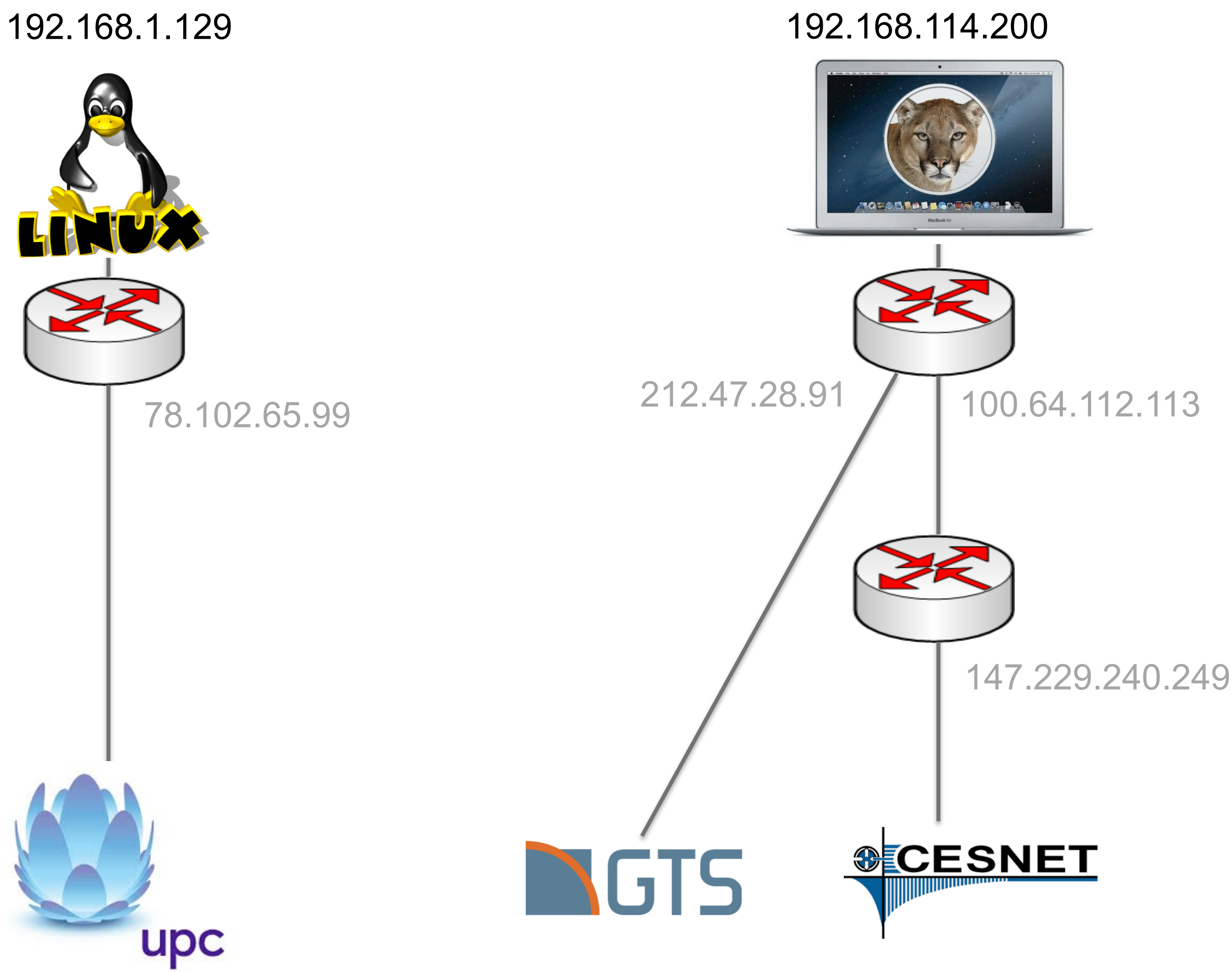
```
[tpoder@test11 ~]$
[tpoder@test11 ~]$ ssh 78.102.66.182.129
Password:
Last login: Tue May  7 15:54:21 2013 from localhost
Tomas-Podermanskis-iMac:~ tpoder$
```

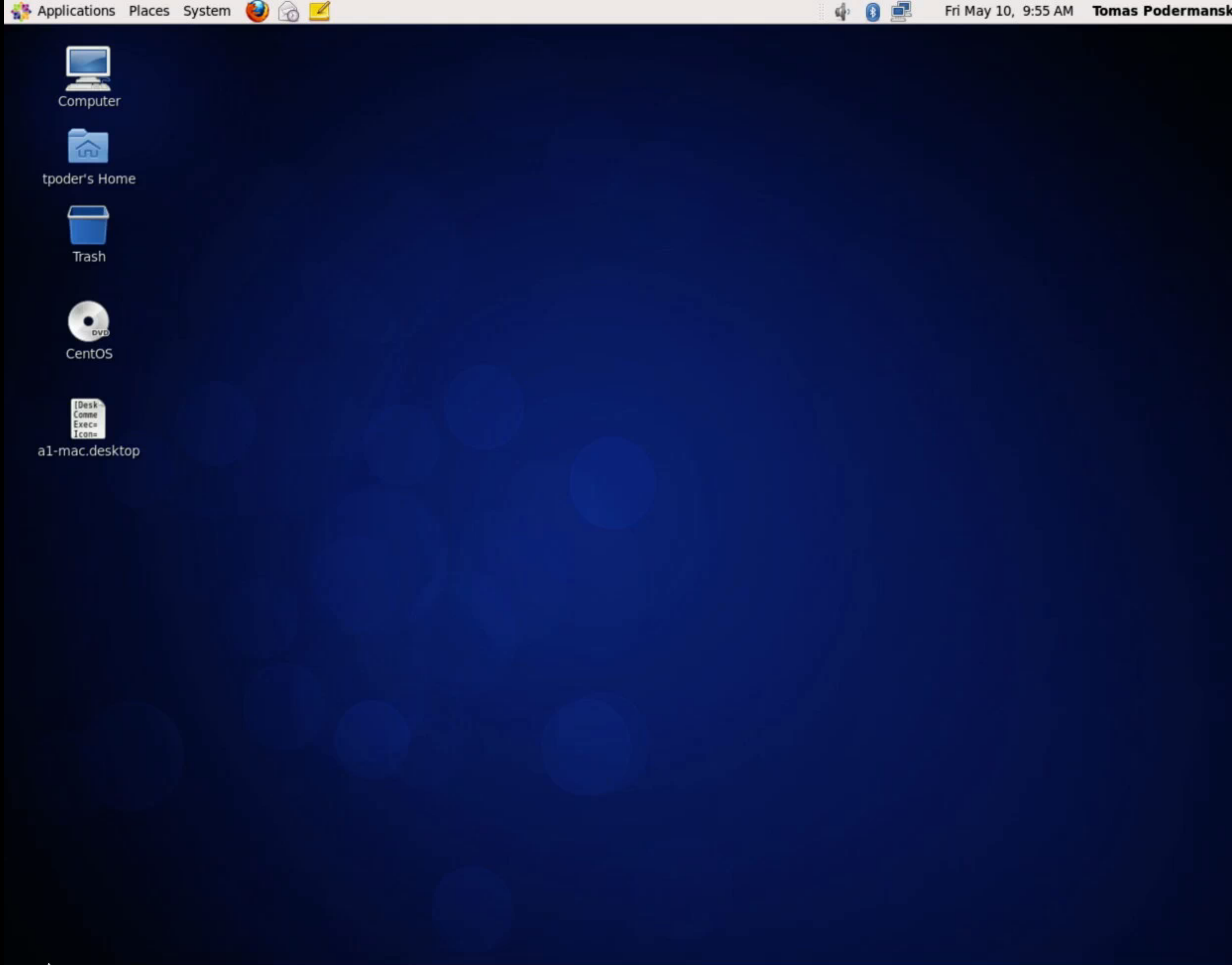

A: 192.168.1.129
DP 192.168.1.1/24
A: 78.102.66.182.129
UA 78.102.66.182
C: 147.229.240.246


IP45 host
A: 192.168.1.129
DP 192.168.1.1/24
Border gateway
UA 78.102.66.182
IP45 host
C: 147.229.240.246



ADL4
A: 192.168.114.115
DP 192.168.114.1/24
D: 147.229.240.249.112.113.115
S: 147.229.240.246
ADL2
UA 100.64.112.113
DP 100.64.112.1/16
ADL0
UA 147.229.240.249
C: 147.229.240.246


192.168.1.129
192.168.114.200
78.102.65.99
212.47.28.91
100.64.112.113
147.229.240.249
upc
GTS
CESNET


Applications
Places
System
Fri May 10, 9:55 AM
Tomas Podermanski
Computer
tpoder's Home
Trash
CentOS
a1-mac.desktop

IP45 : Vlastnosti

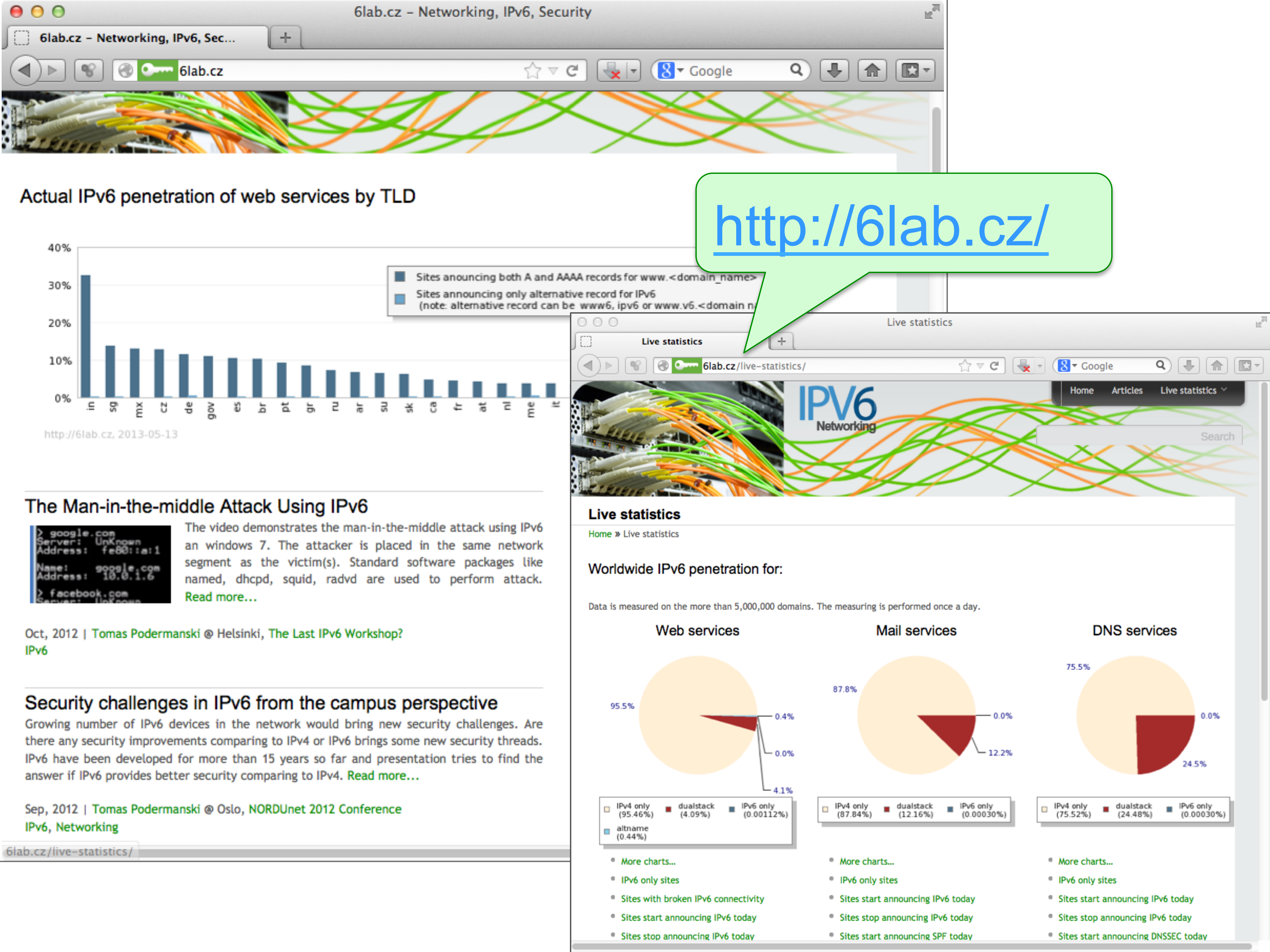
- Výsledná adresa je odvozena od topologie sítě
  - Změna ISP má sice za důsledek změnu adresy všech zařízení**, ALE bez nutnosti přeadresování**
  - Náročnější podvržení zdrojové adresy - Identifikace zdroje útoků
- Implementace BGW (Border Gateway) je triviální
- Hlavička má pevnou délku, žádné proměnlivé položky (neobsahuje IP options, ext. hdrs)
- Multihoming (mobilita) je přímým důsledkem architektury
- Kompatibilita s IPv4, IPv6 – tam kde je to možné
  - Infrastruktura, Serverové aplikace (i IPv4 only)
- Každá IPv6 ready aplikace umí IP45
- Na rozdíl od IPv6 není nutná výměna "všeho"

IP45 : Vlastnosti - negativní

- Hlavička je zbytečně velká: 6B nadbytečných
- Nutné přepočítání dvou kontrolních součtů v hlavičce
- Nutná podpora na koncových zařízeních
  - Zásahy do jádra, velký problém u uzavřených systémů
  - nebo s podporou dopňujícího SW
- Pouze “hračka” , ukázka konceptu

Rozpracování

- Základní specifikace
- Patch do jádra Linux
  - Základní funkcionalita koncového bodu IP45 (1000 řádků)
- Patch do libc
  - Podpora konverze adres ve formatu IP45 (191 řádků)
- Userspace modul zajišťující podporu v uzavřených systémech (MAC OS, v přípravě MS WIN)
- Modul do iptables realizující BGW (border gateway)
  - Použitelný v jakémkoliv Linux-like systému
- Patch do nástroje tcpdump
- Dokumetace bude brzo zpřístupněna na http://ip45.org



http://6lab.cz/
6lab.cz – Networking, IPv6, Security
6lab.cz
Actual IPv6 penetration of web services by TLD
40%
30%
20%
10%
0%
Sites anouncing both A and AAAA records for www.<domain_name>
Sites announcing only alternative record for IPv6
(note: alternative record can be www6, ipv6 or www.v6.<domain n
in sg mx cz de gov es br pt gr ru ar su sk ca fr at nl me it
http://6lab.cz, 2013-05-13
The Man-in-the-middle Attack Using IPv6
The video demonstrates the man-in-the-middle attack using IPv6 an windows 7. The attacker is placed in the same network segment as the victim(s). Standard software packages like named, dhcpd, squid, radvd are used to perform attack. Read more…
Oct, 2012 | Tomas Podermanski @ Helsinki, The Last IPv6 Workshop?
IPv6
Security challenges in IPv6 from the campus perspective
Growing number of IPv6 devices in the network would bring new security challenges. Are there any security improvements comparing to IPv4 or IPv6 brings some new security threads. IPv6 have been developed for more than 15 years so far and presentation tries to find the answer if IPv6 provides better security comparing to IPv4. Read more…
Sep, 2012 | Tomas Podermanski @ Oslo, NORDUnet 2012 Conference
IPv6, Networking
6lab.cz/live-statistics/
Live statistics
6lab.cz/live-statistics/
IPV6 Networking
Home Articles Live statistics
Search
Live statistics
Home » Live statistics
Worldwide IPv6 penetration for:
Data is measured on the more than 5,000,000 domains. The measuring is performed once a day.
Web services
95.5% 0.4% 0.0% 4.1%
IPv4 only (95.46%) dualstack (4.09%) IPv6 only (0.00112%) altname (0.44%)
Mail services
87.8% 0.0% 12.2%
IPv4 only (87.84%) dualstack (12.16%) IPv6 only (0.00030%)
DNS services
75.5% 0.0% 24.5%
IPv4 only (75.52%) dualstack (24.48%) IPv6 only (0.00030%)
More charts...
IPv6 only sites
Sites with broken IPv6 connectivity
Sites start announcing IPv6 today
Sites stop announcing IPv6 today
More charts...
IPv6 only sites
Sites start announcing IPv6 today
Sites stop announcing IPv6 today
Sites start announcing SPF today
More charts...
IPv6 only sites
Sites start announcing IPv6 today
Sites stop announcing IPv6 today
Sites start announcing DNSSEC today

S IPv6 na věčné časy a n~~i~~ěkdy jinak

síťové architektury a jejich budoucnost

CVIS
CENTRUM VÝPOČETNÍCH A INFORMAČNÍCH SLUŽEB

Konference Internet a Technologie 13, Praha 2013

Tomáš Podermanski, tpoder@cis.vutbr.cz

Vysoké učení technické v Brně

FIT
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ