Kvantitativní analýza internetového provozu

Ladislav Lhotka
⟨*lhotka@cesnet.cz*⟩

Obsah kurzu

1. Principy komunikace v Internetu, protokoly TCP/IP
2. Hlavní kvantitativní charakteristiky datového provozu IP

   IP toky, způsoby měření, nástroje na analýzu a vizualizaci
3. Charakteristické rysy hlavních aplikačních protokolů (HTTP, FTP, SSH, P2P, XMPP aj.)
4. Objemové veličiny (počty bajtů a paketů), statistická analýza časových řad, metody založené na predikci
5. Rozložení klíčových položek IP toků (např. IP adres) ve vzorcích provozu: entropie a PCA
6. Kvantitativní charakteristiky vícerozměrných vzorků: fraktální a korelační dimenze, multifraktální míry

Osnova dnešní přednášky

- Úvod, motivace
- Historické srovnání: telefonní síť versus Internet
- Komunikační model ISO OSI a protokoly TCP/IP
- Datagram IPv4 a IPv6, adresy
- Směrovací hierarchie
- Spojovaná komunikace: TCP

Proč měřit a analyzovat internetový provoz?
(A proč o tom učit?)

Je to zajímavé

Internet je dnes asi nejrozsáhlejší a nejsložitější systém, který člověk vytvořil. Podle posledních odhadů je připojeno téměř 1,5 miliardy lidí, ve vyspělých státech 50–70 %.

Zpomalení růstu není nikde v dohledu, naopak – integrace mobilních telefonů, připojené domácí spotřebiče, auta, bezdrátové senzory, . . .

Internet je postmoderní komunikační médium, kde se děje úplně všechno. Charakteristika provozu je proto obvykle velmi komplikovaná.

Je to užitečné

Agregované veličiny pomáhají správci sítě v mnoha směrech:

1. Sledování zátěže, plánování rozvoje
2. Indikace výpadků linek nebo síťových prvků
3. Odhalování bezpečnostních problémů, zejména masivních útoků typu DoS nebo nelegálního sdílení

Je to obtížné

Ukládání kompletních dat není možné: saturovaná linka 10 Gb/s znamená 100 TB za den. Problém je v tom, jak z neúplných dat získat co nejvíc informací a jak je efektivně reprezentovat a analyzovat.

Potřebné znalosti:

- protokoly a technologie TCP/IP
- aplikační protokoly
- metody ukládání dat, data mining
- vizualizace
- matematika, statistika

Počátky telefonie

6.4.1875 – Bellův patent 161739 *Transmitters and Receivers for Electric Telegraphs*

10.3.1876 – první telefonní hovor (A. G. Bell): “Mr. Watson, come here, I want to see you.”

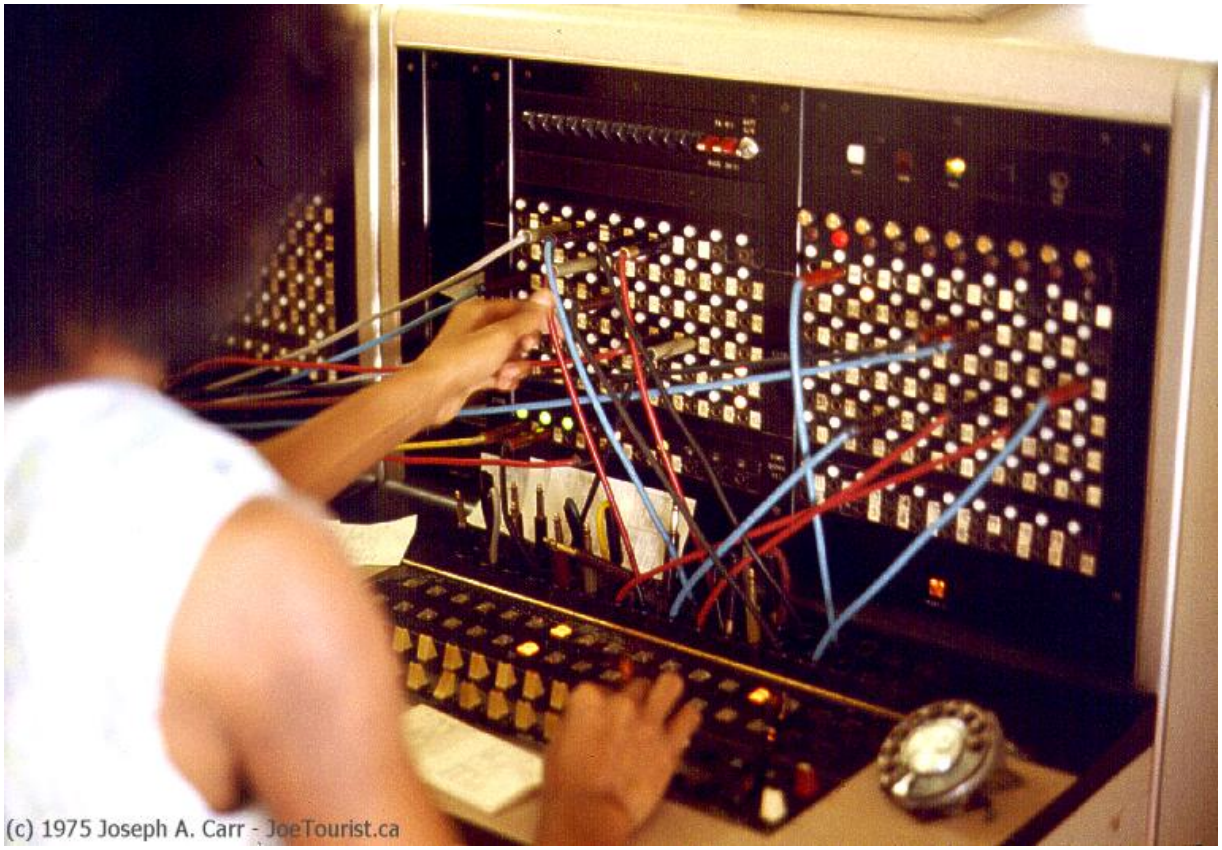
27.4.1877 – Edisonův patent 474230 (uhlíkový mikrofon)

Bellův i Edisonův telefon vyžadoval fyzické vedení mezi oběma stranami.

Telefonní síť

Vodivé spojení mezi telefonujícími stranami se vytváří podle požadavků.

Telefonní číslo je vlastně “program” sestavení cesty.



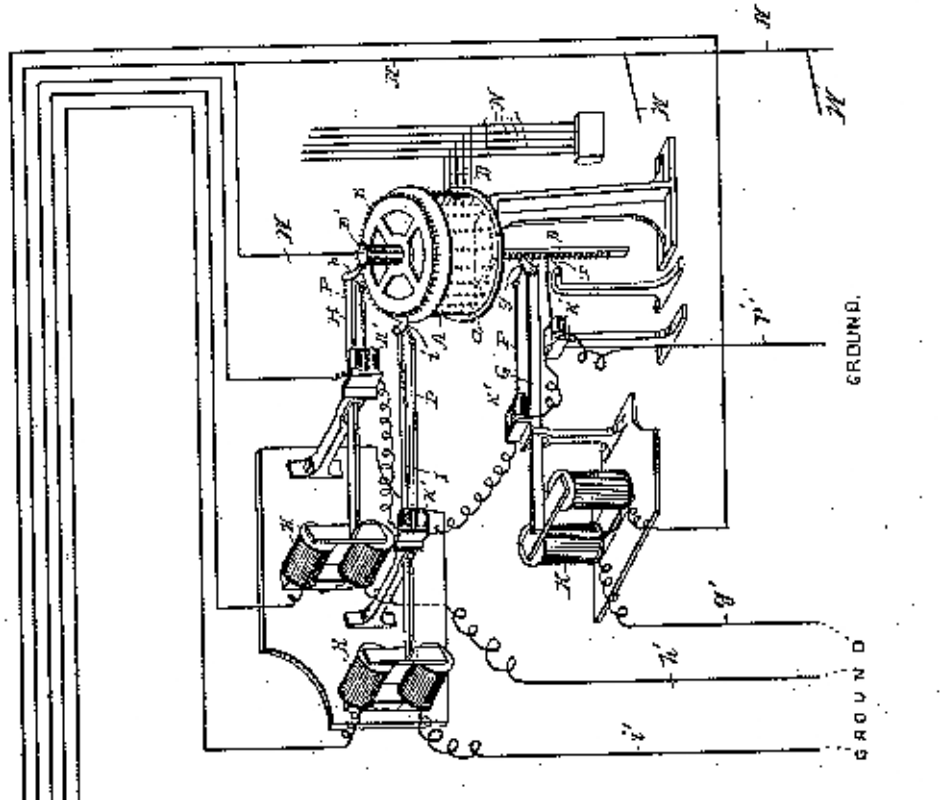
Strowger stepper

(No Model.) 3 Sheets—Sheet 1.

A. B. STROWGER.

AUTOMATIC TELEPHONE EXCHANGE.

No. 447,918. Patented Mar. 10, 1891.



Datové komunikace

Komunikační síť pro přenos dat byla nejdříve utvářena podle telefonního vzoru.

Dva zásadní problémy:

1. Strukturální nespolehlivost: pravděpodobnost chyby roste exponenciálně s počtem zařízení v cestě;
2. Časové zpoždění při sestavování cesty.

60. léta – revoluční myšlenky

- *Paul Baran: Distribuovaná komunikace*

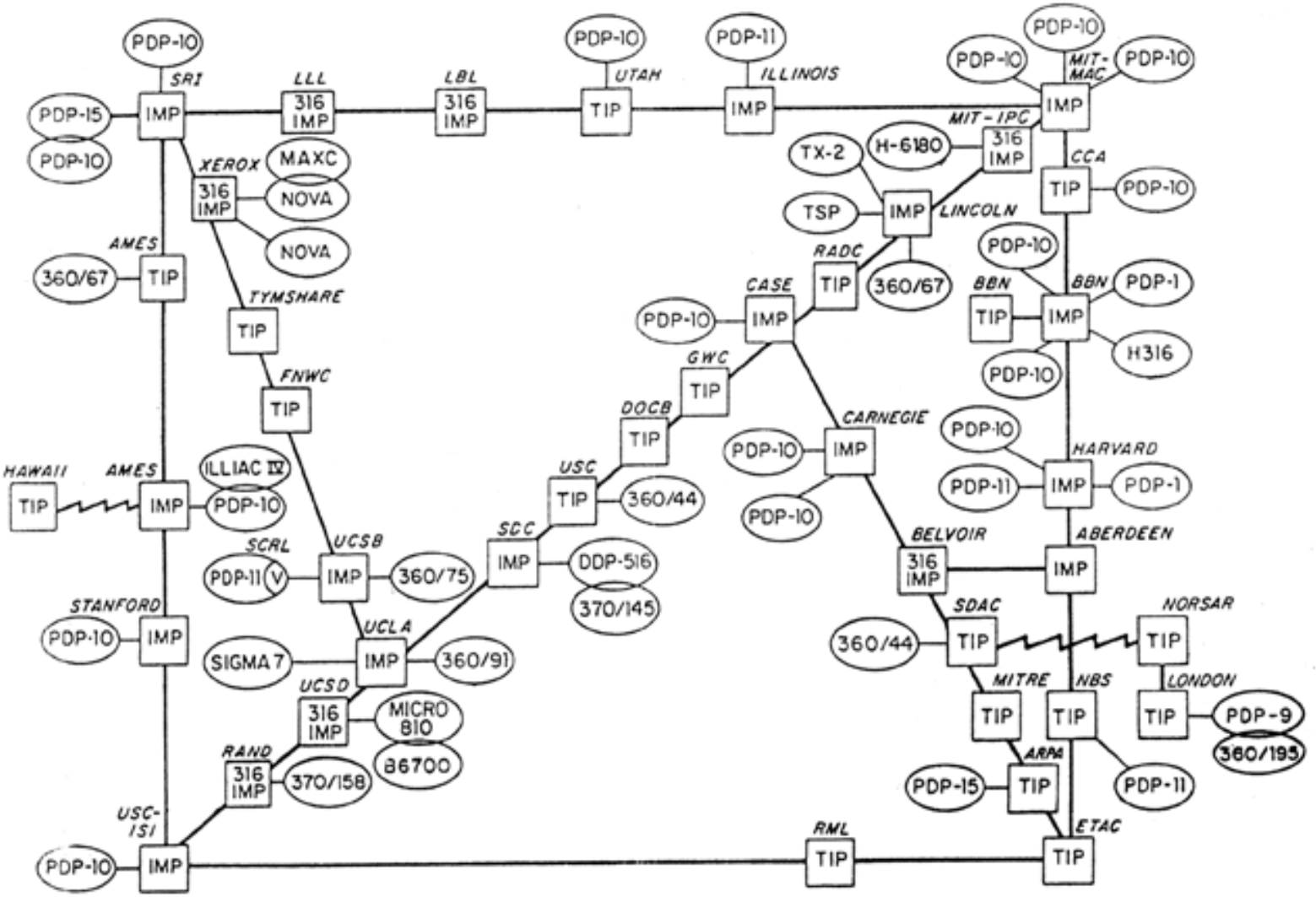
  Hustě propojená síť, next-hop routing

- *Donald Davies: Přepojování datových paketů*

  Zpráva rozsekaná do paketů, každý opatřen hlavičkou, mj. s cílovou adresou.

Telekomunikační komunita je zavrhla, padly ale na úrodnou půdu v ARPA (Advanced Research Projects Agency) $\longrightarrow$ ARPAnet

ARPA NETWORK, LOGICAL MAP, SEPTEMBER 1973



CATENET

Princip přepojování paketů se stal díky ARPAnetu populárním a uznávaným, a v 1. pol. 70. let ho používala kromě něj řada dalších sítí. Tyto sítě spolu však nemohly komunikovat.

Bob Kahn a *Vint Cerf* proto začali v roce 1973 pracovat na specifikacích, které sjednotí protokoly, rozhraní a datové objekty vyměňované mezi těmito sítěmi $\longrightarrow$ TCP/IP.

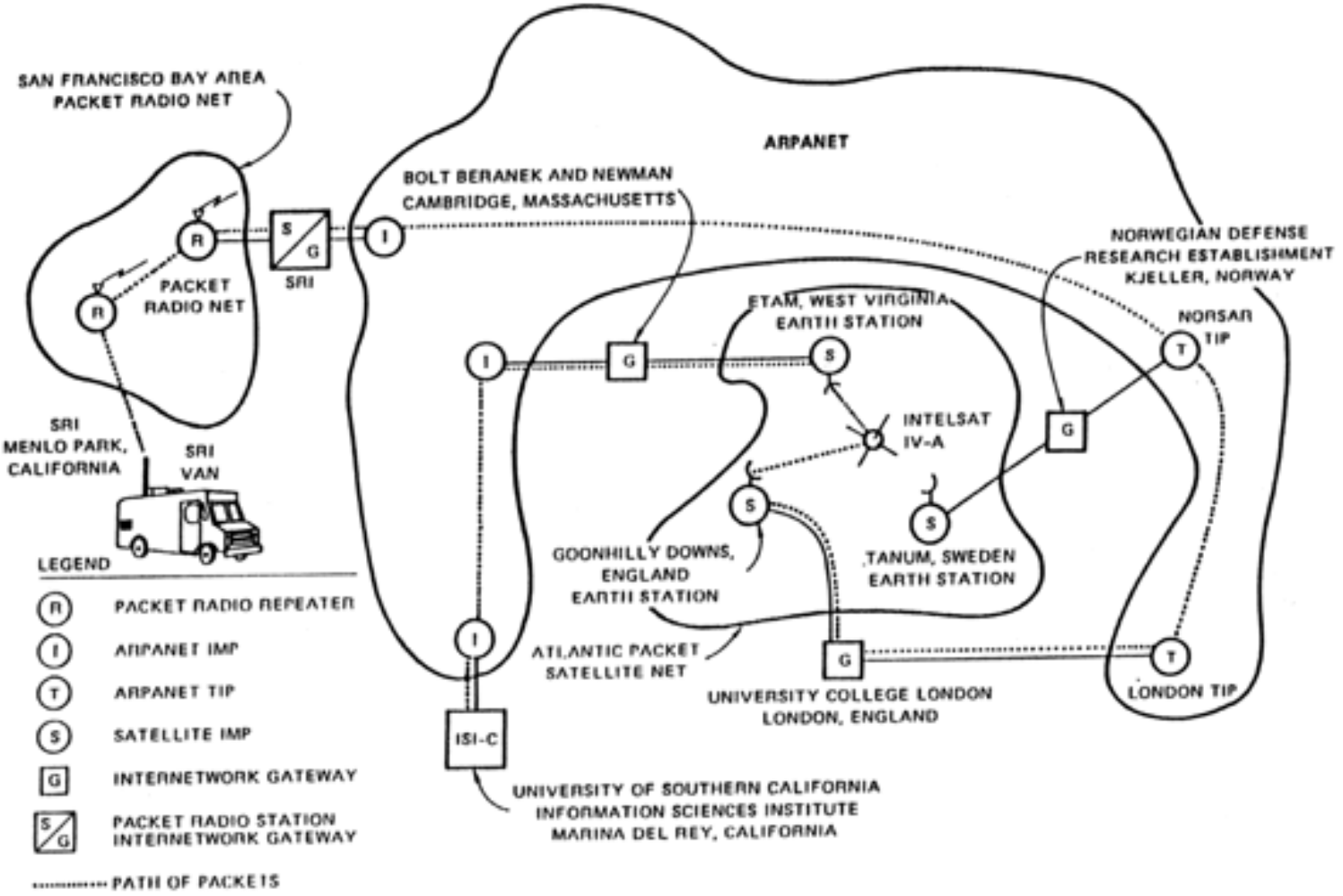
Mimoto rozdělili protokoly a příslušný software do vrstev, které poskytují různé úrovně abstrakce.

Tato práce je zárodkem Internetu jakožto překryvné sítě nad různými transportními technologiemi.

End-to-end Principle

Většinu komunikačních funkcí lze lépe a efektivněji implementovat na samotných koncích spojení než uvnitř síťové infrastruktury.

Síť nemusí být bezchybná, koncové aplikace se s přiměřeným množstvím chyb dovedou vyrovnat.


SAN FRANCISCO BAY AREA
PACKET RADIO NET
PACKET
RADIO NET
SRI
SRI
MENLO PARK,
CALIFORNIA
SRI
VAN
ARPANET
BOLT BERANEK AND NEWMAN
CAMBRIDGE, MASSACHUSETTS
NORWEGIAN DEFENSE
RESEARCH ESTABLISHMENT
KJELLER, NORWAY
ETAM, WEST VIRGINIA
EARTH STATION
NORSAR
TIP
INTELSAT
IV-A
GOONHILLY DOWNS,
ENGLAND
EARTH STATION
TANUM, SWEDEN
EARTH STATION
ATLANTIC PACKET
SATELLITE NET
UNIVERSITY COLLEGE LONDON
LONDON, ENGLAND
LONDON TIP
ISI-C
UNIVERSITY OF SOUTHERN CALIFORNIA
INFORMATION SCIENCES INSTITUTE
MARINA DEL REY, CALIFORNIA
LEGEND
PACKET RADIO REPEATER
ARPANET IMP
ARPANET TIP
SATELLITE IMP
INTERNETWORK GATEWAY
PACKET RADIO STATION
INTERNETWORK GATEWAY
PATH OF PACKETS

RFC 1149

D. Waitzman: *A Standard for the Transmission of IP Datagrams on Avian Carriers.* IETF, 1 April 1990.

Bergen, Norsko
28.4.2001

TCP/IP Stack

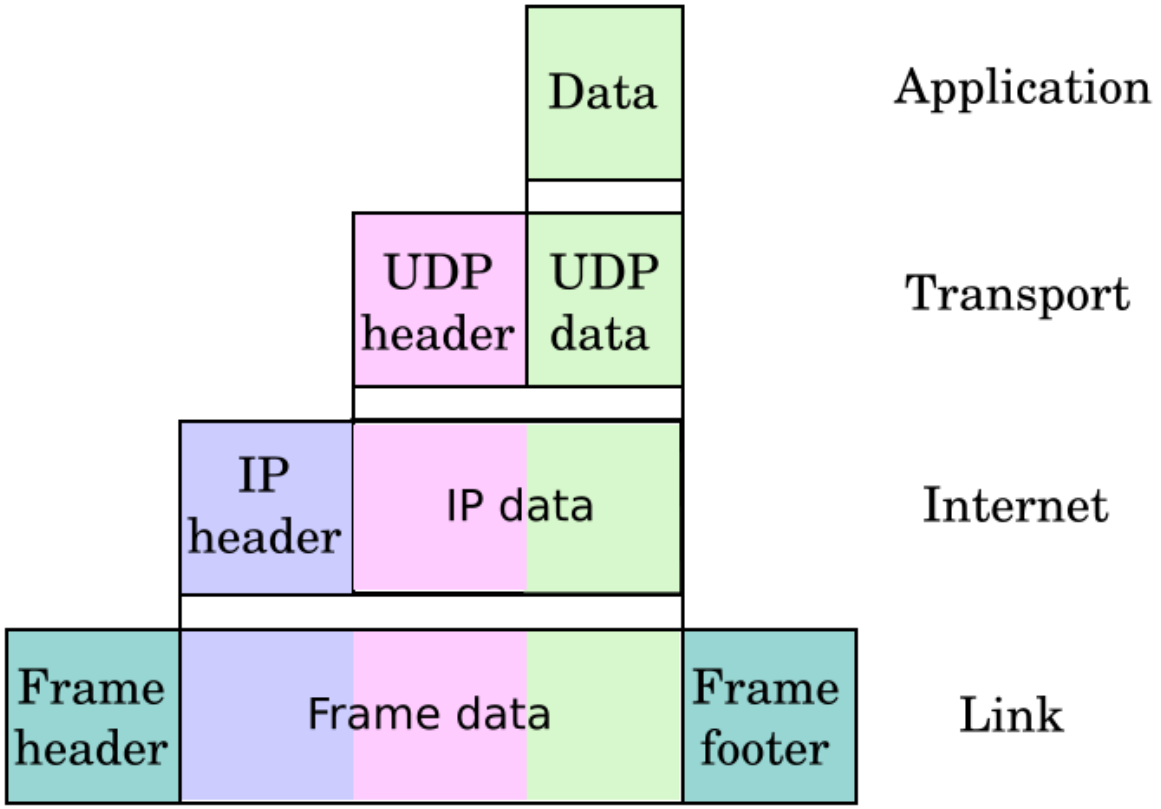
Application layer: HTTP, SSH, SMTP, DNS, . . .

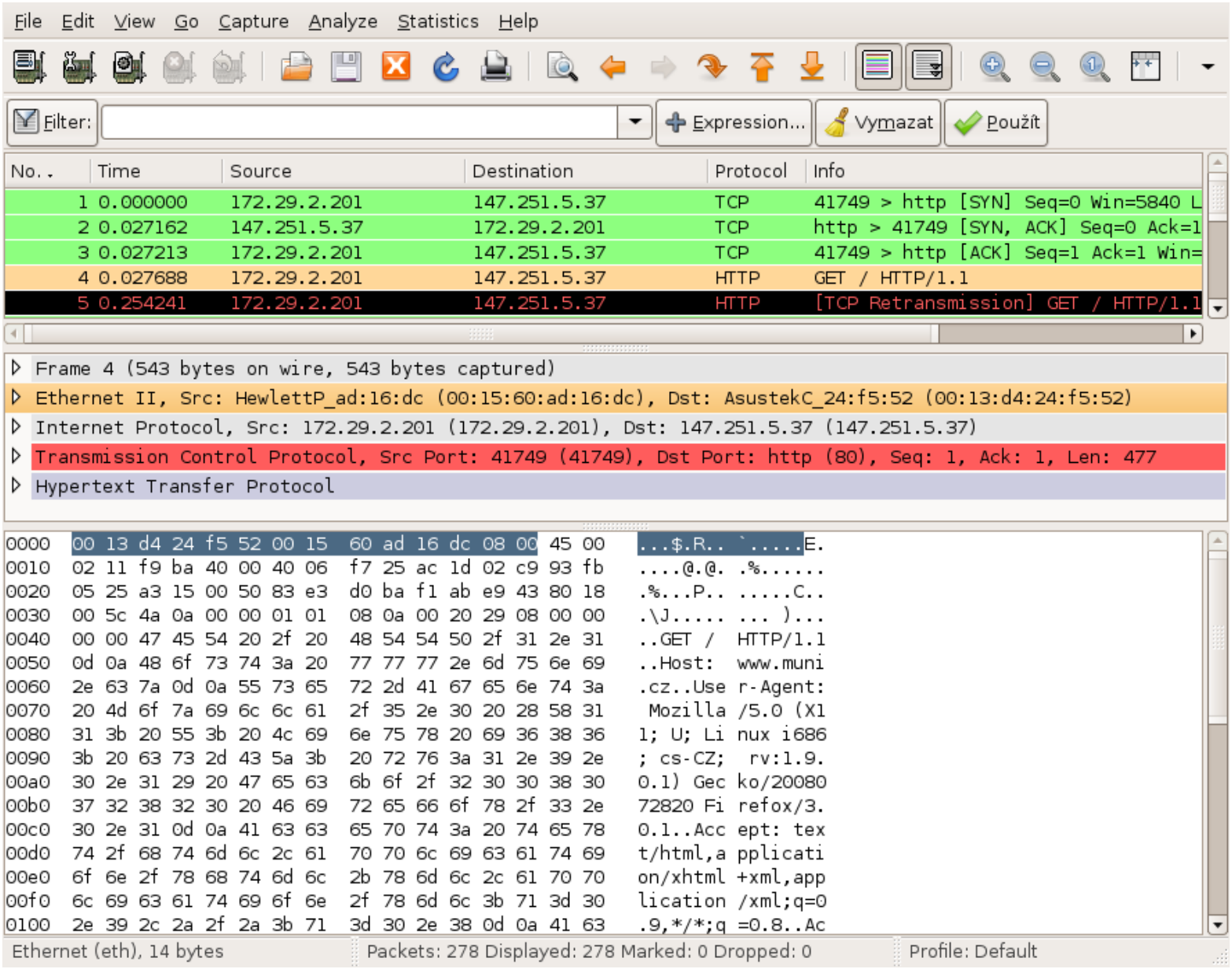
Transport layer: TCP, UDP

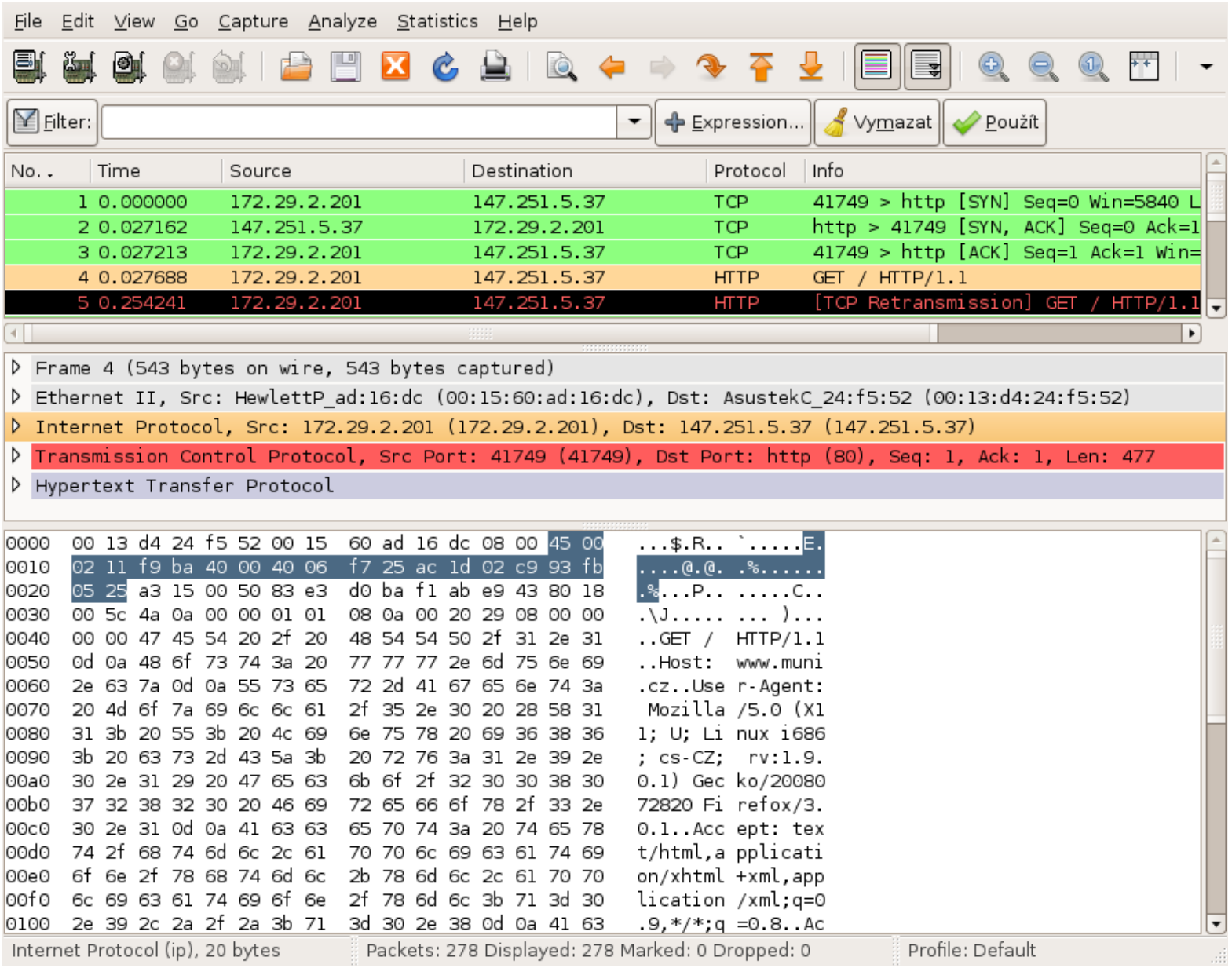
Internet layer: IP, ICMP

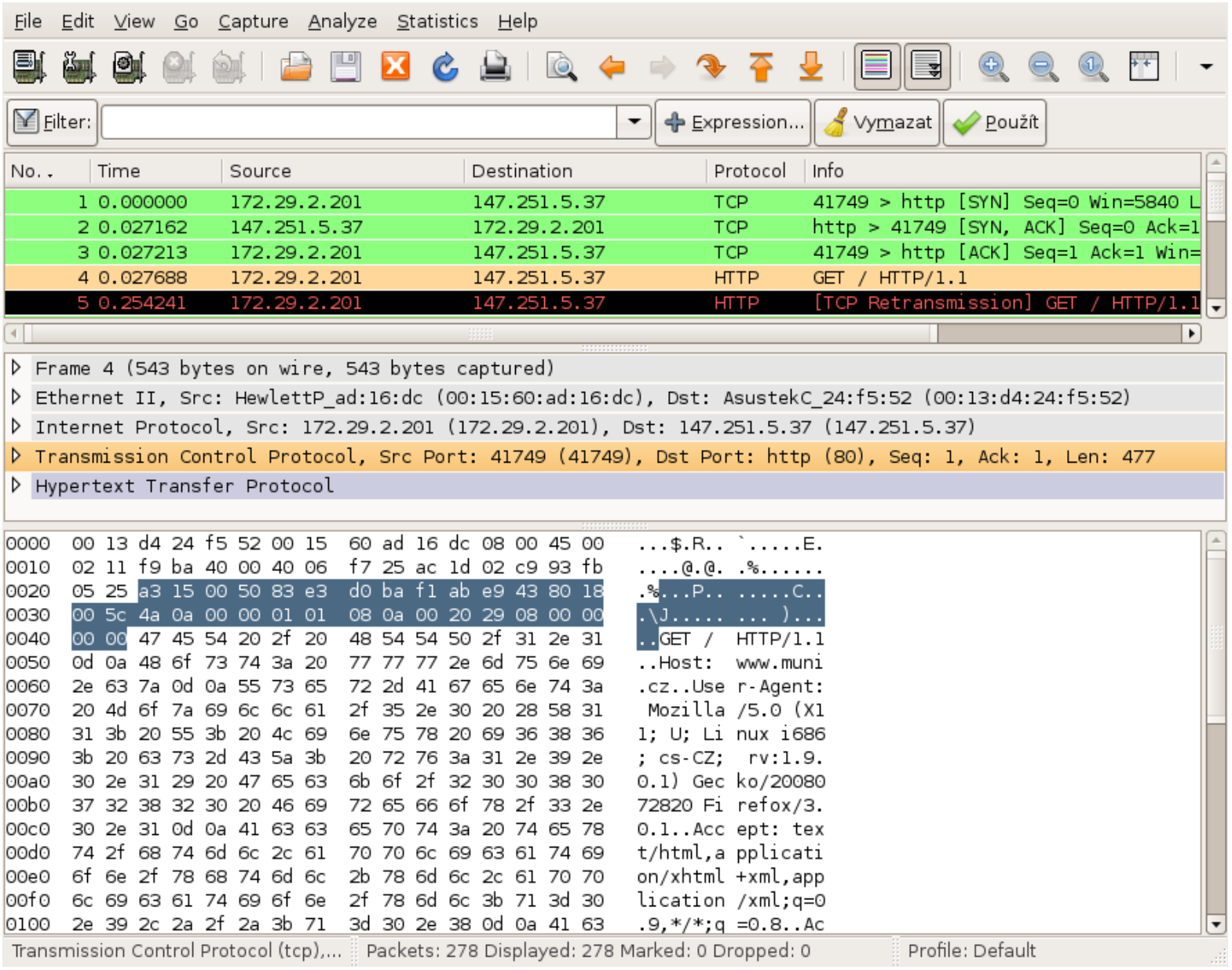
Link layer: Ethernet, GPRS, satelit

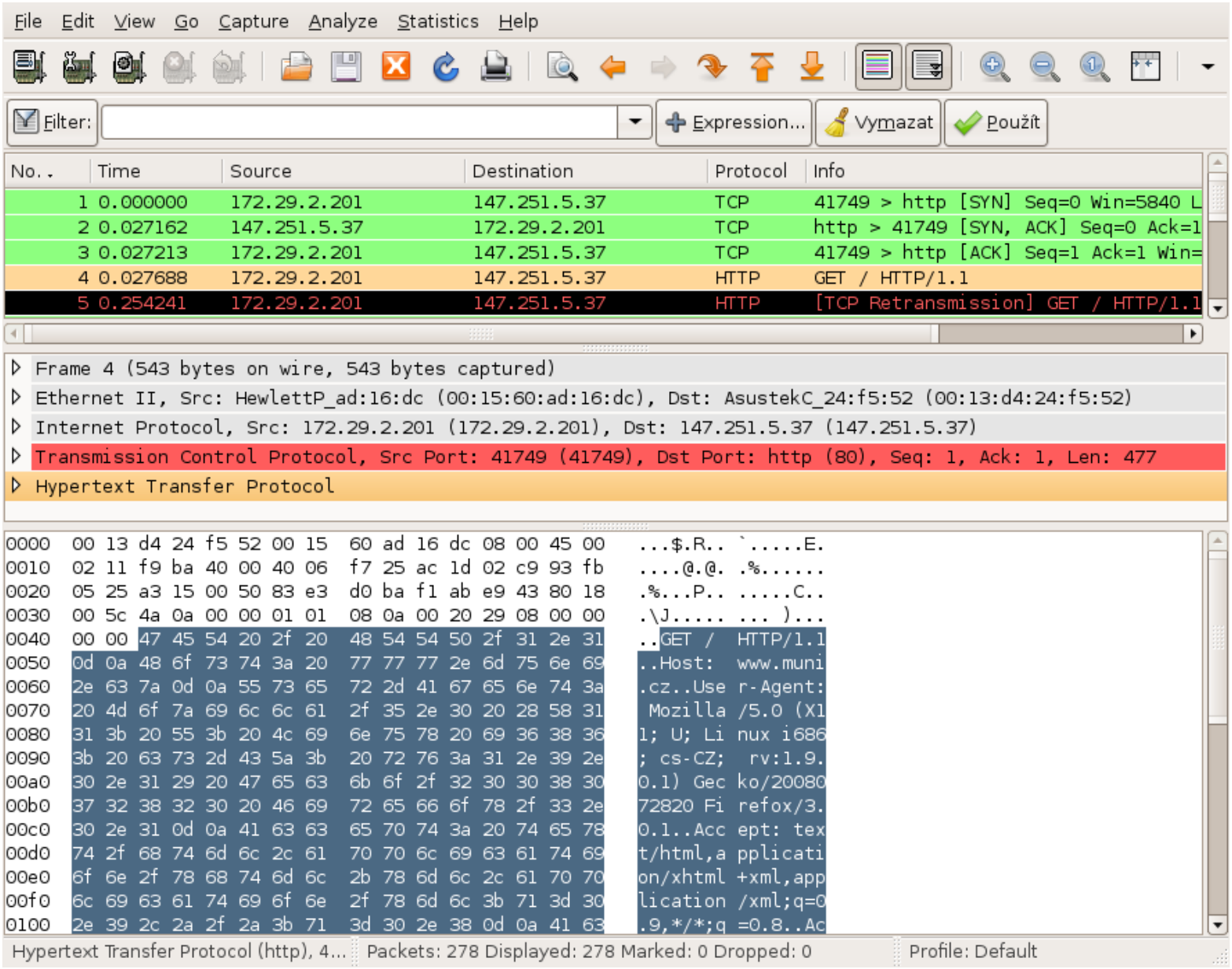
Enkapsulace v paketu



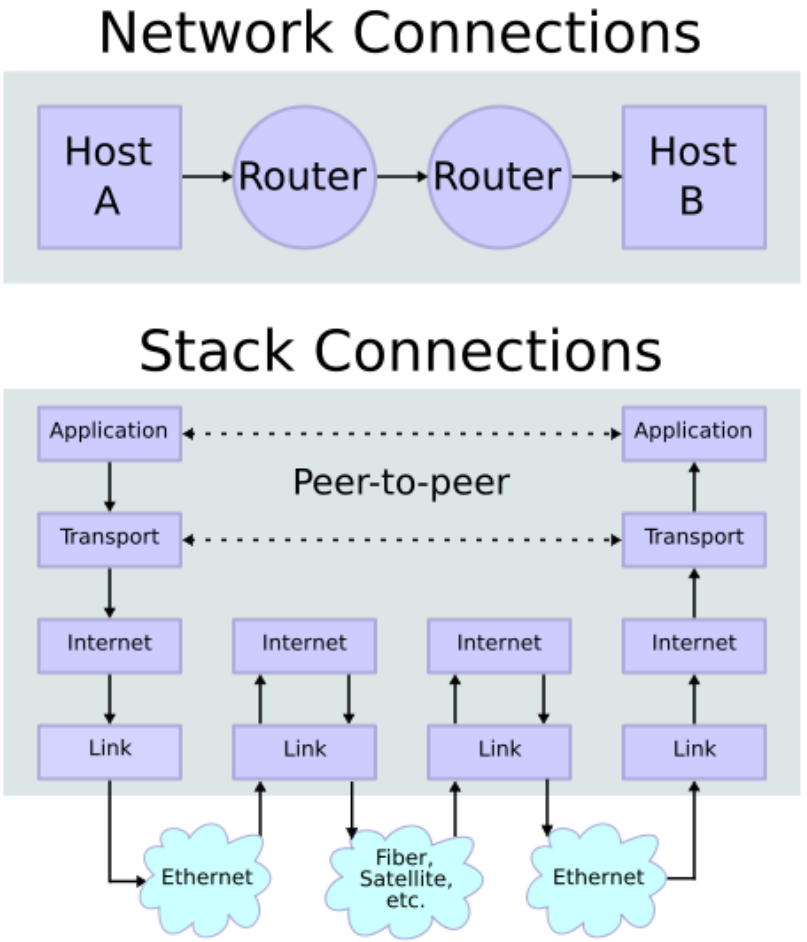

File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Vymazat
Použít
No. Time Source Destination Protocol Info
1 0.000000 172.29.2.201 147.251.5.37 TCP 41749 > http [SYN] Seq=0 Win=5840 L
2 0.027162 147.251.5.37 172.29.2.201 TCP http > 41749 [SYN, ACK] Seq=0 Ack=1
3 0.027213 172.29.2.201 147.251.5.37 TCP 41749 > http [ACK] Seq=1 Ack=1 Win=
4 0.027688 172.29.2.201 147.251.5.37 HTTP GET / HTTP/1.1
5 0.254241 172.29.2.201 147.251.5.37 HTTP [TCP Retransmission] GET / HTTP/1.1
Frame 4 (543 bytes on wire, 543 bytes captured)
Ethernet II, Src: HewlettP_ad:16:dc (00:15:60:ad:16:dc), Dst: AsustekC_24:f5:52 (00:13:d4:24:f5:52)
Internet Protocol, Src: 172.29.2.201 (172.29.2.201), Dst: 147.251.5.37 (147.251.5.37)
Transmission Control Protocol, Src Port: 41749 (41749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
0000 00 13 d4 24 f5 52 00 15 60 ad 16 dc 08 00 45 00 ...$.R.. `.....E.
0010 02 11 f9 ba 40 00 40 06 f7 25 ac 1d 02 c9 93 fb ....@.@. .%......
0020 05 25 a3 15 00 50 83 e3 d0 ba f1 ab e9 43 80 18 .%...P.. .....C..
0030 00 5c 4a 0a 00 00 01 01 08 0a 00 20 29 08 00 00 .\J..... ...)...
0040 00 00 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 75 6e 69 ..Host: www.muni
0060 2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a .cz..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36 1; U; Li nux i686
0090 3b 20 63 73 2d 43 5a 3b 20 72 76 3a 31 2e 39 2e ; cs-CZ; rv:1.9.
00a0 30 2e 31 29 20 47 65 63 6b 6f 2f 32 30 30 38 30 0.1) Gec ko/20080
00b0 37 32 38 32 30 20 46 69 72 65 66 6f 78 2f 33 2e 72820 Fi refox/3.
00c0 30 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 0.1..Acc ept: tex
00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati
00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml +xml,app
00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0
0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 .9,*/*;q =0.8..Ac
Ethernet (eth), 14 bytes
Packets: 278 Displayed: 278 Marked: 0 Dropped: 0
Profile: Default


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Vymazat
Použít
No. Time Source Destination Protocol Info
1 0.000000 172.29.2.201 147.251.5.37 TCP 41749 > http [SYN] Seq=0 Win=5840 L
2 0.027162 147.251.5.37 172.29.2.201 TCP http > 41749 [SYN, ACK] Seq=0 Ack=1
3 0.027213 172.29.2.201 147.251.5.37 TCP 41749 > http [ACK] Seq=1 Ack=1 Win=
4 0.027688 172.29.2.201 147.251.5.37 HTTP GET / HTTP/1.1
5 0.254241 172.29.2.201 147.251.5.37 HTTP [TCP Retransmission] GET / HTTP/1.1
Frame 4 (543 bytes on wire, 543 bytes captured)
Ethernet II, Src: HewlettP_ad:16:dc (00:15:60:ad:16:dc), Dst: AsustekC_24:f5:52 (00:13:d4:24:f5:52)
Internet Protocol, Src: 172.29.2.201 (172.29.2.201), Dst: 147.251.5.37 (147.251.5.37)
Transmission Control Protocol, Src Port: 41749 (41749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
0000 00 13 d4 24 f5 52 00 15 60 ad 16 dc 08 00 45 00 ...$.R.. `.....E.
0010 02 11 f9 ba 40 00 40 06 f7 25 ac 1d 02 c9 93 fb ....@.@. .%......
0020 05 25 a3 15 00 50 83 e3 d0 ba f1 ab e9 43 80 18 .%...P.. .....C..
0030 00 5c 4a 0a 00 00 01 01 08 0a 00 20 29 08 00 00 .\J..... ...)...
0040 00 00 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 75 6e 69 ..Host: www.muni
0060 2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a .cz..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36 1; U; Li nux i686
0090 3b 20 63 73 2d 43 5a 3b 20 72 76 3a 31 2e 39 2e ; cs-CZ; rv:1.9.
00a0 30 2e 31 29 20 47 65 63 6b 6f 2f 32 30 30 38 30 0.1) Gec ko/20080
00b0 37 32 38 32 30 20 46 69 72 65 66 6f 78 2f 33 2e 72820 Fi refox/3.
00c0 30 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 0.1..Acc ept: tex
00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati
00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml +xml,app
00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0
0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 .9,*/*;q =0.8..Ac
Internet Protocol (ip), 20 bytes
Packets: 278 Displayed: 278 Marked: 0 Dropped: 0
Profile: Default

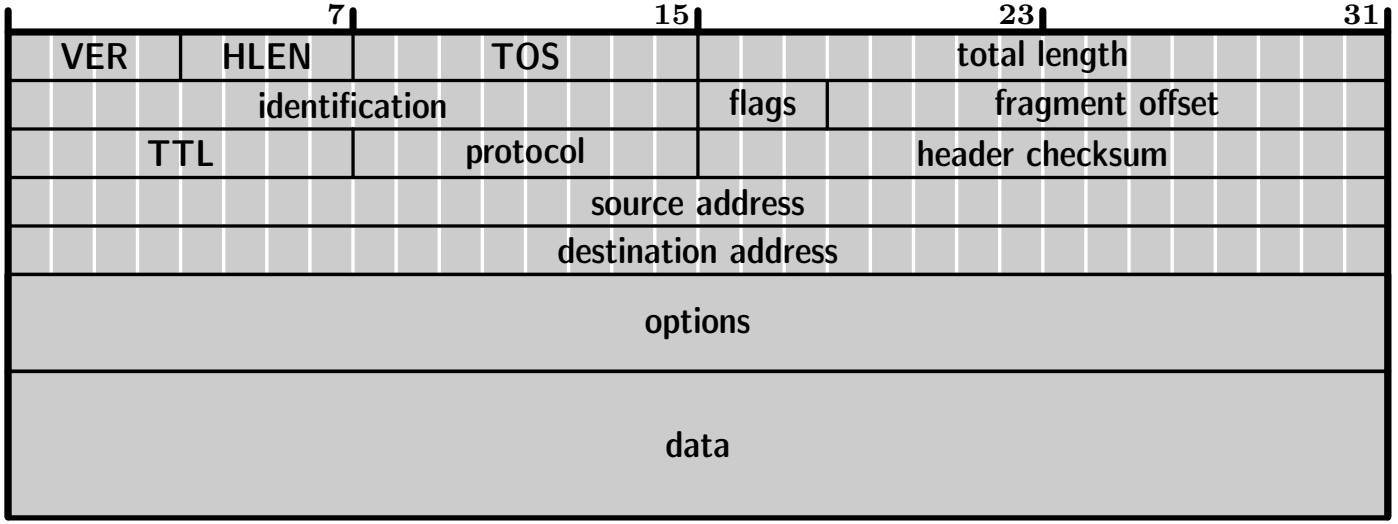

File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Vymazat
Použít
No. Time Source Destination Protocol Info
1 0.000000 172.29.2.201 147.251.5.37 TCP 41749 > http [SYN] Seq=0 Win=5840 L
2 0.027162 147.251.5.37 172.29.2.201 TCP http > 41749 [SYN, ACK] Seq=0 Ack=1
3 0.027213 172.29.2.201 147.251.5.37 TCP 41749 > http [ACK] Seq=1 Ack=1 Win=
4 0.027688 172.29.2.201 147.251.5.37 HTTP GET / HTTP/1.1
5 0.254241 172.29.2.201 147.251.5.37 HTTP [TCP Retransmission] GET / HTTP/1.1
Frame 4 (543 bytes on wire, 543 bytes captured)
Ethernet II, Src: HewlettP_ad:16:dc (00:15:60:ad:16:dc), Dst: AsustekC_24:f5:52 (00:13:d4:24:f5:52)
Internet Protocol, Src: 172.29.2.201 (172.29.2.201), Dst: 147.251.5.37 (147.251.5.37)
Transmission Control Protocol, Src Port: 41749 (41749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
0000 00 13 d4 24 f5 52 00 15 60 ad 16 dc 08 00 45 00 ...$.R.. `.....E.
0010 02 11 f9 ba 40 00 40 06 f7 25 ac 1d 02 c9 93 fb ....@.@. .%......
0020 05 25 a3 15 00 50 83 e3 d0 ba f1 ab e9 43 80 18 .%...P.. .....C..
0030 00 5c 4a 0a 00 00 01 01 08 0a 00 20 29 08 00 00 .\J..... ...)...
0040 00 00 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 75 6e 69 ..Host: www.muni
0060 2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a .cz..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36 1; U; Li nux i686
0090 3b 20 63 73 2d 43 5a 3b 20 72 76 3a 31 2e 39 2e ; cs-CZ; rv:1.9.
00a0 30 2e 31 29 20 47 65 63 6b 6f 2f 32 30 30 38 30 0.1) Gec ko/20080
00b0 37 32 38 32 30 20 46 69 72 65 66 6f 78 2f 33 2e 72820 Fi refox/3.
00c0 30 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 0.1..Acc ept: tex
00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati
00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml +xml,app
00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0
0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 .9,*/*;q =0.8..Ac
Transmission Control Protocol (tcp),...
Packets: 278 Displayed: 278 Marked: 0 Dropped: 0
Profile: Default


File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Vymazat
Použít
No. Time Source Destination Protocol Info
1 0.000000 172.29.2.201 147.251.5.37 TCP 41749 > http [SYN] Seq=0 Win=5840 L
2 0.027162 147.251.5.37 172.29.2.201 TCP http > 41749 [SYN, ACK] Seq=0 Ack=1
3 0.027213 172.29.2.201 147.251.5.37 TCP 41749 > http [ACK] Seq=1 Ack=1 Win=
4 0.027688 172.29.2.201 147.251.5.37 HTTP GET / HTTP/1.1
5 0.254241 172.29.2.201 147.251.5.37 HTTP [TCP Retransmission] GET / HTTP/1.1
Frame 4 (543 bytes on wire, 543 bytes captured)
Ethernet II, Src: HewlettP_ad:16:dc (00:15:60:ad:16:dc), Dst: AsustekC_24:f5:52 (00:13:d4:24:f5:52)
Internet Protocol, Src: 172.29.2.201 (172.29.2.201), Dst: 147.251.5.37 (147.251.5.37)
Transmission Control Protocol, Src Port: 41749 (41749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 477
Hypertext Transfer Protocol
0000 00 13 d4 24 f5 52 00 15 60 ad 16 dc 08 00 45 00 ...$.R.. `.....E.
0010 02 11 f9 ba 40 00 40 06 f7 25 ac 1d 02 c9 93 fb ....@.@. .%......
0020 05 25 a3 15 00 50 83 e3 d0 ba f1 ab e9 43 80 18 .%...P.. .....C..
0030 00 5c 4a 0a 00 00 01 01 08 0a 00 20 29 08 00 00 .\J..... ...)...
0040 00 00 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 75 6e 69 ..Host: www.muni
0060 2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a .cz..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36 1; U; Li nux i686
0090 3b 20 63 73 2d 43 5a 3b 20 72 76 3a 31 2e 39 2e ; cs-CZ; rv:1.9.
00a0 30 2e 31 29 20 47 65 63 6b 6f 2f 32 30 30 38 30 0.1) Gec ko/20080
00b0 37 32 38 32 30 20 46 69 72 65 66 6f 78 2f 33 2e 72820 Fi refox/3.
00c0 30 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 0.1..Acc ept: tex
00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati
00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml +xml,app
00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0
0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 .9,*/*;q =0.8..Ac
Hypertext Transfer Protocol (http), 4...
Packets: 278 Displayed: 278 Marked: 0 Dropped: 0
Profile: Default

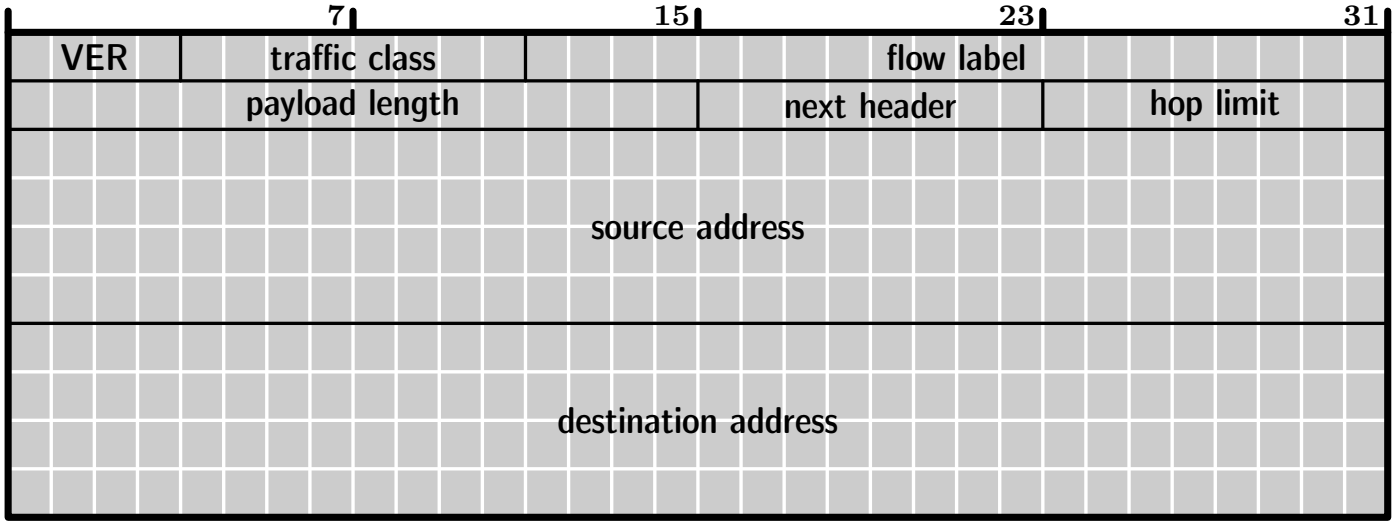
Princip komunikace



Datagram IPv4



Datagram IPv6



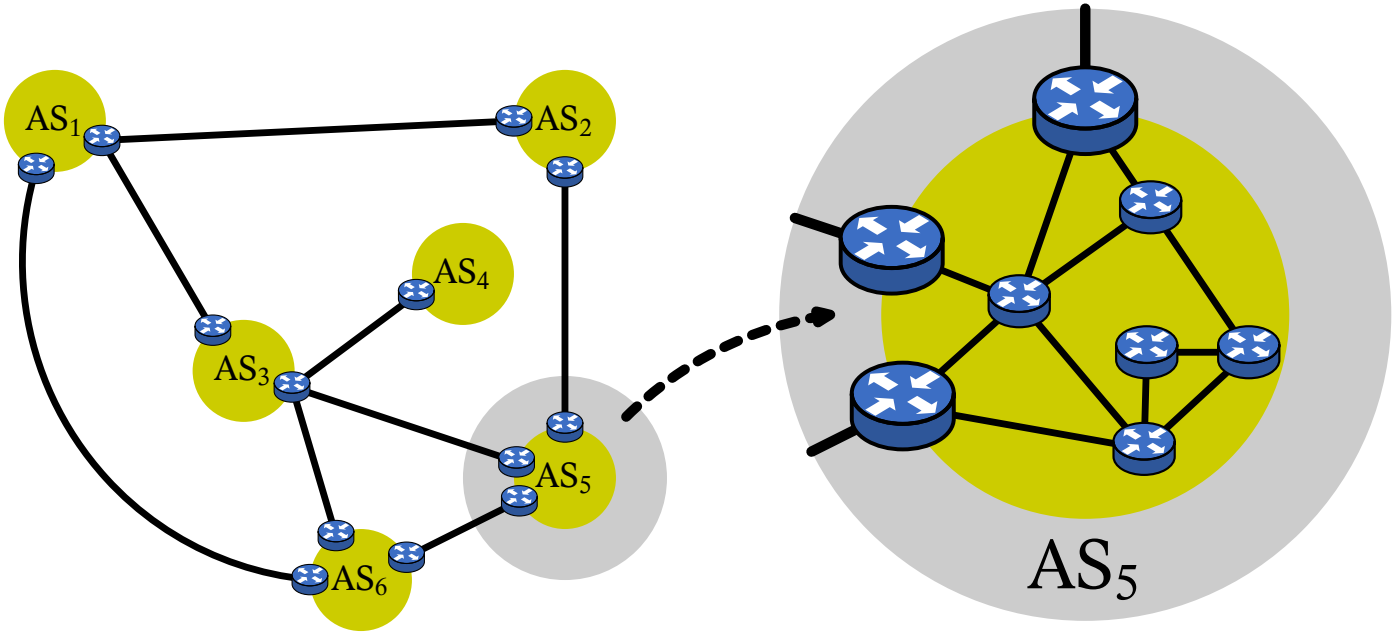
Směrovací hierarchie

Směrování se v Internetu odehráva ve dvou základních úrovních:

- exterior (inter-AS) routing
- interior (intra-AS) routing

Autonomní systém (AS): propojený soubor sítí a směrovačů pod koordinovanou správou, která vůči zbytku Internetu vystupuje jako konzistentní jednotka. Nazývá se též směrovací doména (routing domain).

Každý AS je identifikován šestnáctibitovým číslem (ASN = AS number), přiděleným regionálním internetovým registrem (RIR).


AS1
AS2
AS4
AS3
AS5
AS6
AS5

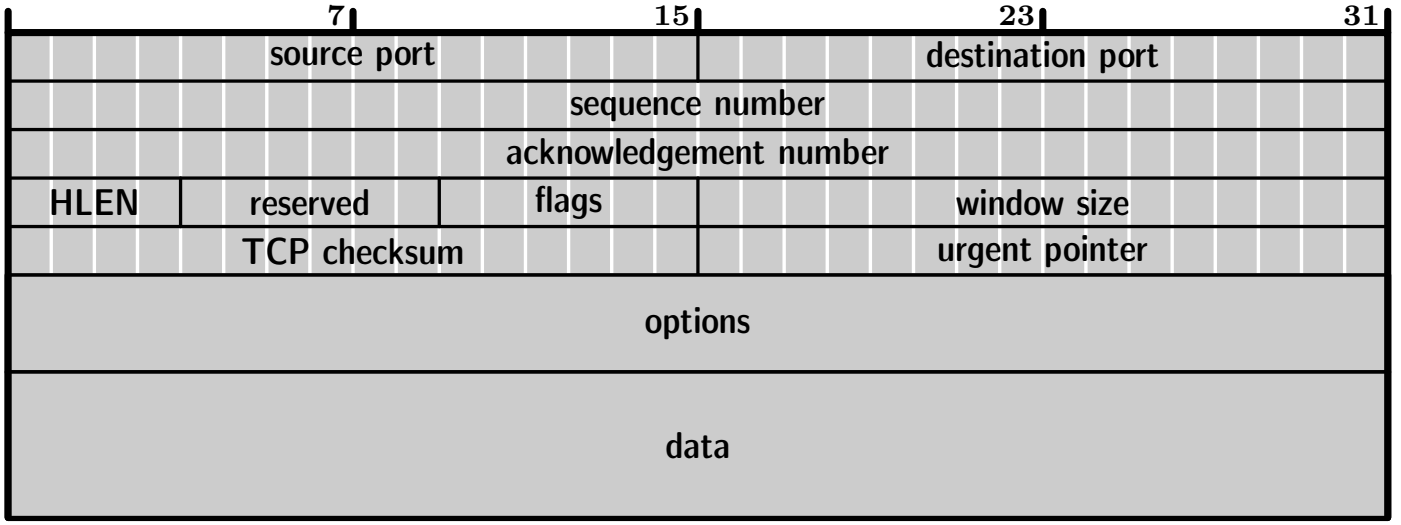
Transmission Control Protocol

TCP vytváří pro aplikaci abstrakci *proudu* – spojitého datového toku (virtuální roura). Je to *spolehlivý* protokol, tzn. zaručuje bezchybné doručení všech dat v pořadí, jak byla odeslána.

Pozitivní potvrzování: přijímající strana odesílá sekvenční číslo prvního bajtu, který dosud nebyl (řádně) doručen.

TCP také obsahuje mechanismus pro řízení rychlosti odesílání dat.

Hlavička TCP



Flags: URG ACK PSH RST SYN FIN

Řízení datového toku