Počítačové a komunikačné siete
Sieťová vrstva / Subnetting
Linková vrstva / Ethernet

Prednáška 7

STU FIIT

Obsah

» Opakovanie subnettingu

» Network adress translation (NAT)

» Linková vrstva – Formát Ethernet rámca

Opakovanie minulej prednášky

» Príklad na subnetting
  – CIDR
  – VLSM

NAT

(Network Address Translator)

» Cieľ: šetriť IP adresy a zvýšiť bezpečnosť

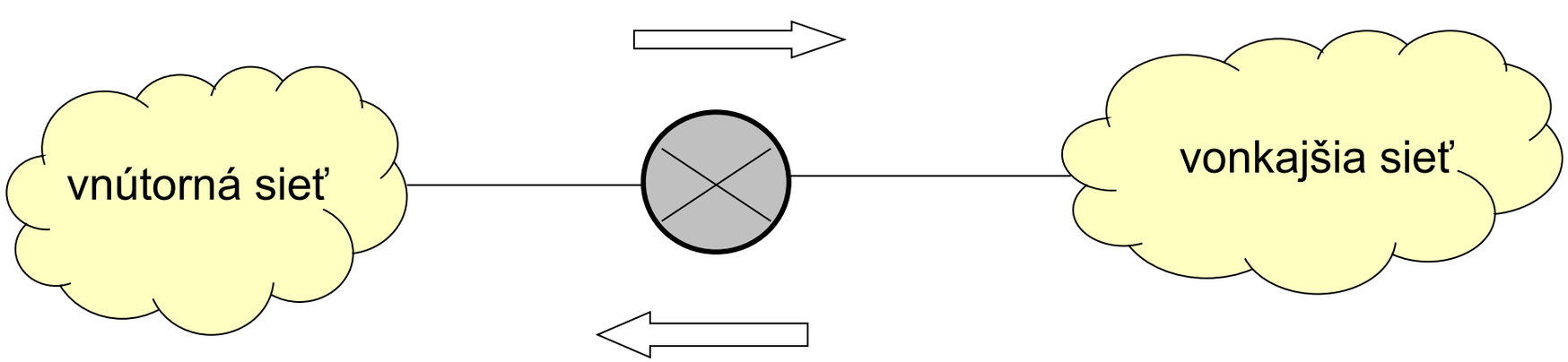
» transformácie adries v smerovači
oddeľujúcom vnútornú sieť od vonkajšej
(prístupový smerovač)
– zdrojové alebo/a cieľové adresy

» transparentnosť pre koncové uzly

STU FIIT

Smerovače s NAT

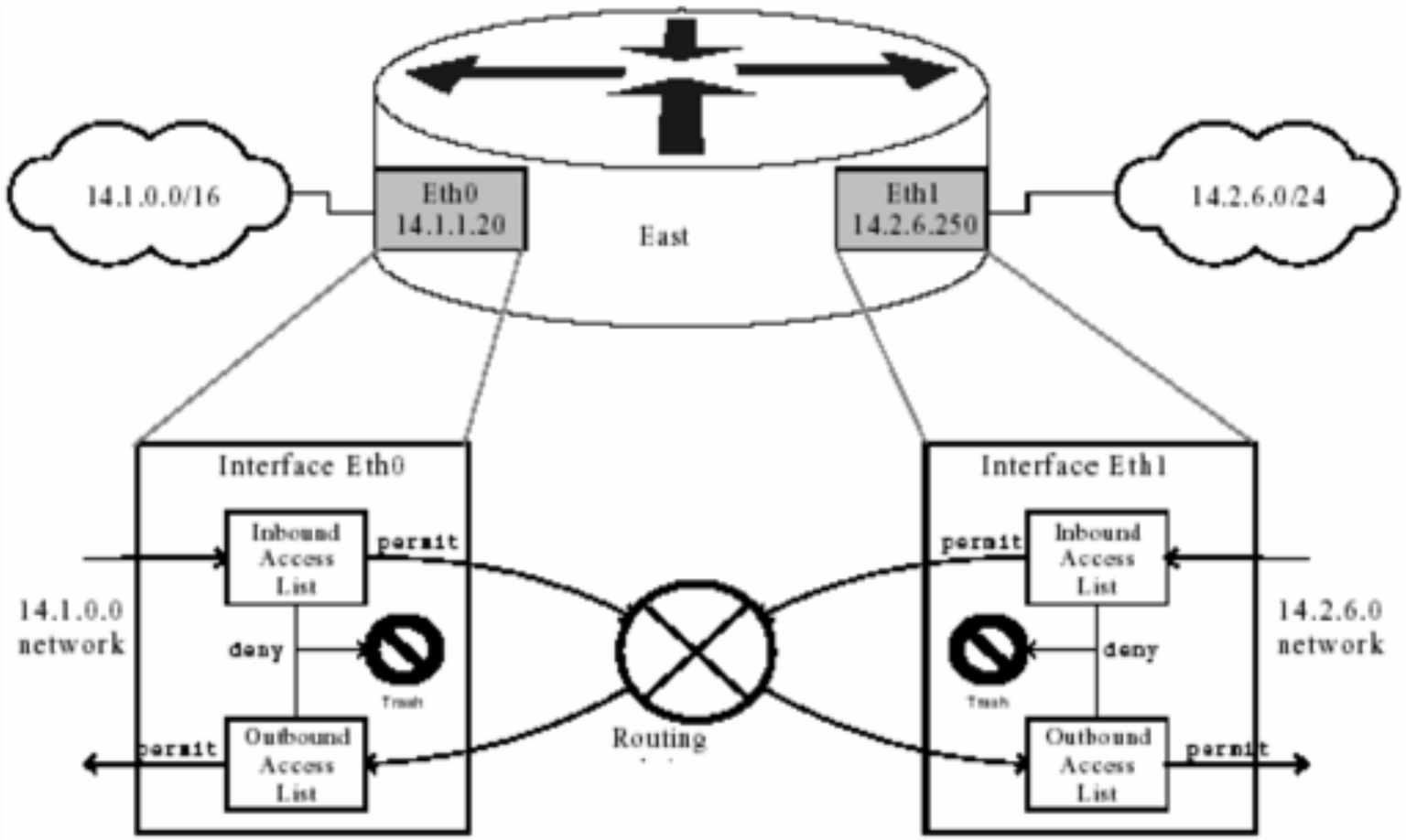
smerovanie -> NAT



smerovanie <- NAT

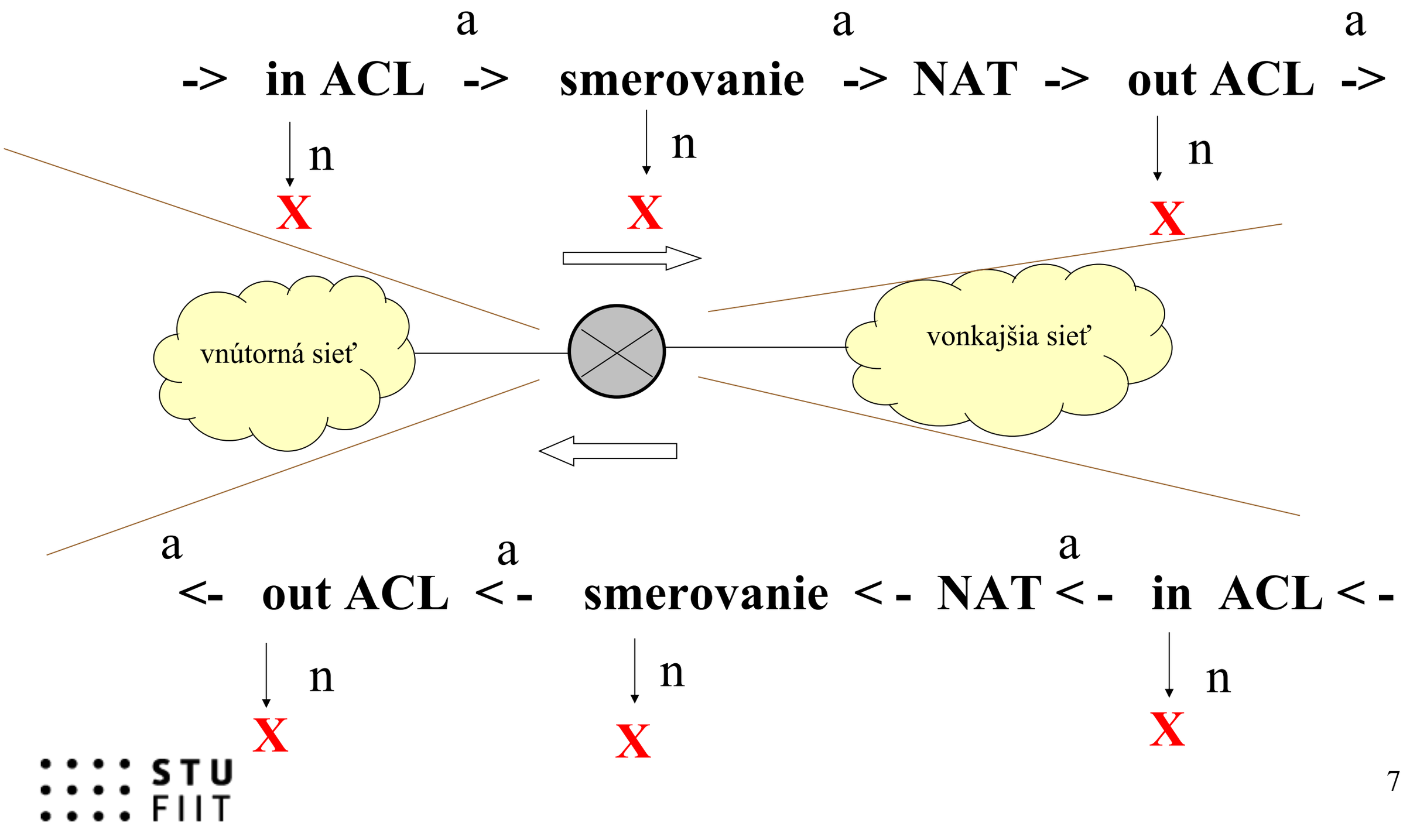
Smerovače s filtrovaním paketov

- Vytvorenie filtra
  - definovanie pravidiel (access-list)
  - aktivovanie filtra na konkrétnom rozhraní smerovača a určenie smeru filtrácie



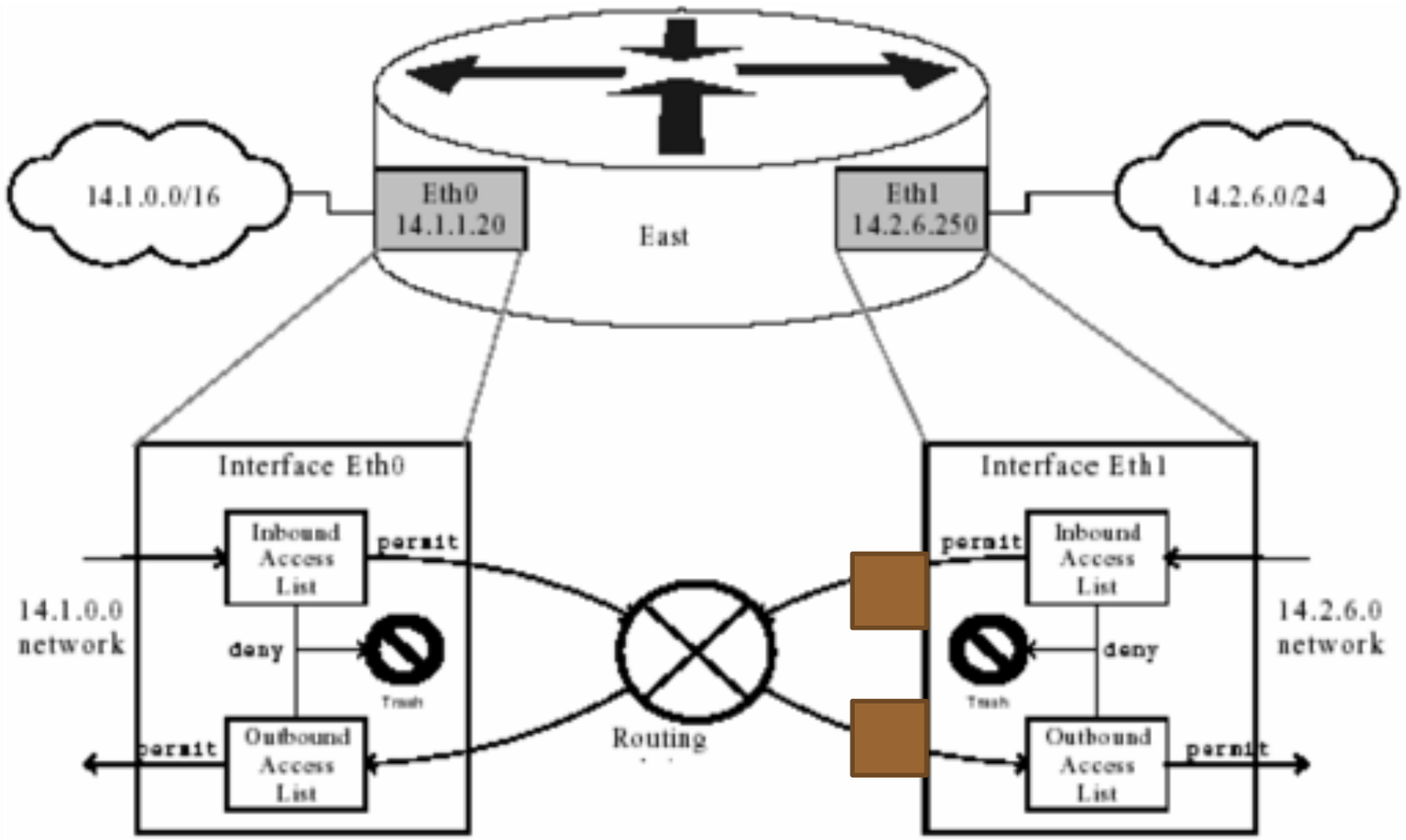
Conceptual Model for Access Lists on Interfaces

Smerovače s NAT a filtrovaním



Smerovače s filtrovaním paketov

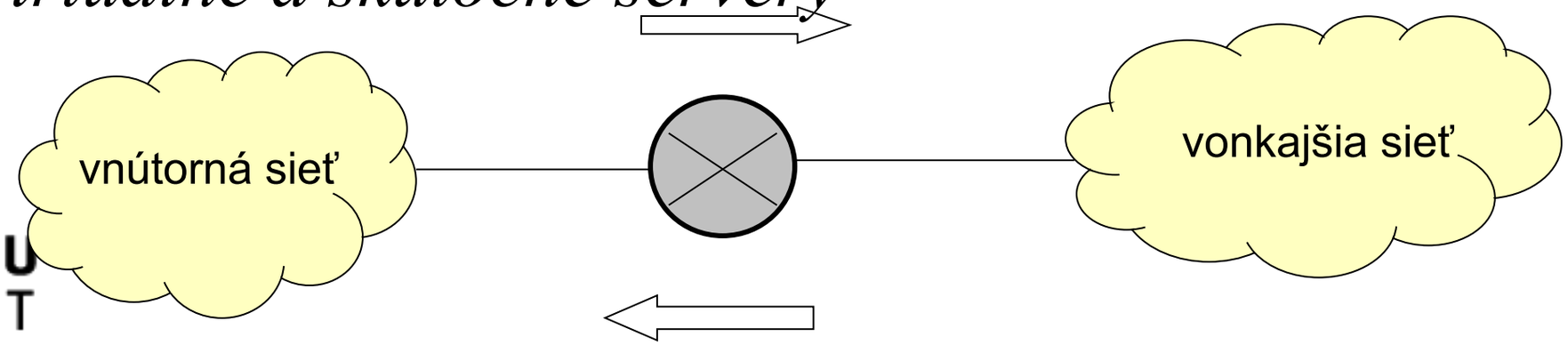
- Vytvorenie filtra
  - definovanie pravidiel (access-list)
  - aktivovanie filtra na konkrétnom rozhraní smerovača a určenie smeru filtrácie



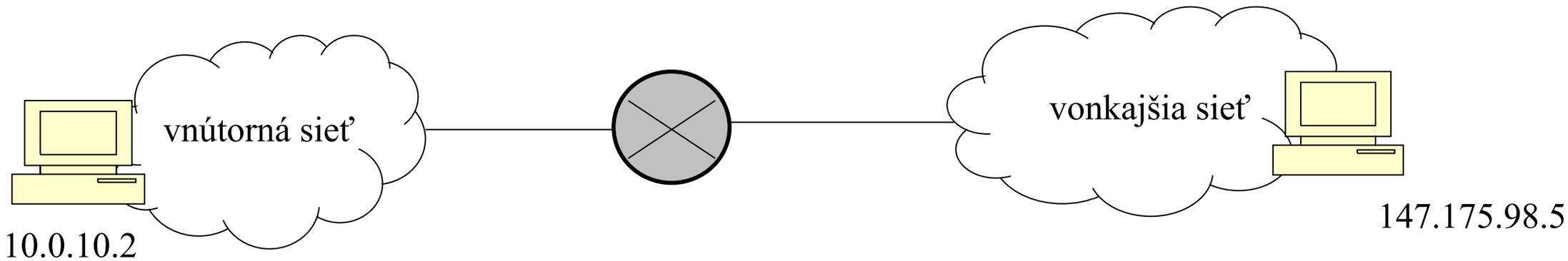
Conceptual Model for Access Lists on Interfaces

Niektoré typy NAT

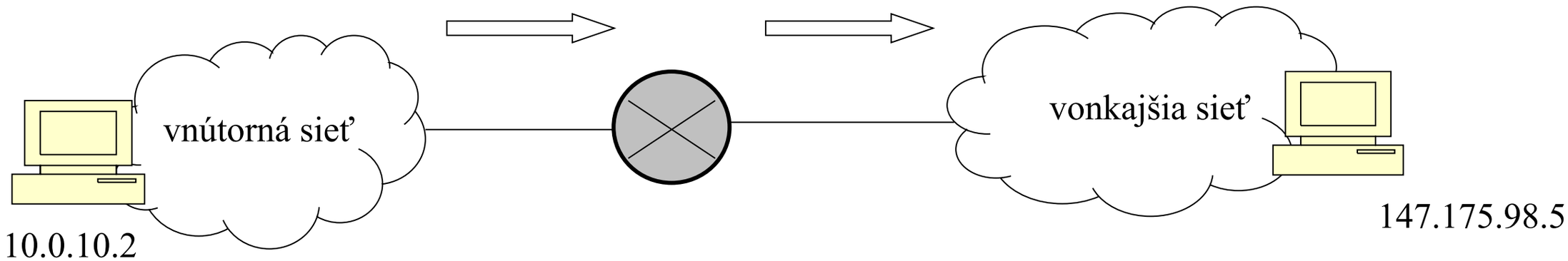
- jednosmerný NAT (jednoduchý, tradičný – unidirectional, traditional, outbound)
  - komunikácia z vnútornej siete
  - preklad zdrojových adries
  - ďalšie zmeny v IP pakete
- rozšírený NAT (overloaded, port-based, PAT, NAPT)
- *rozloženie výkonu (TCP load distribution)*
  - *virtuálne a skutočné servery*



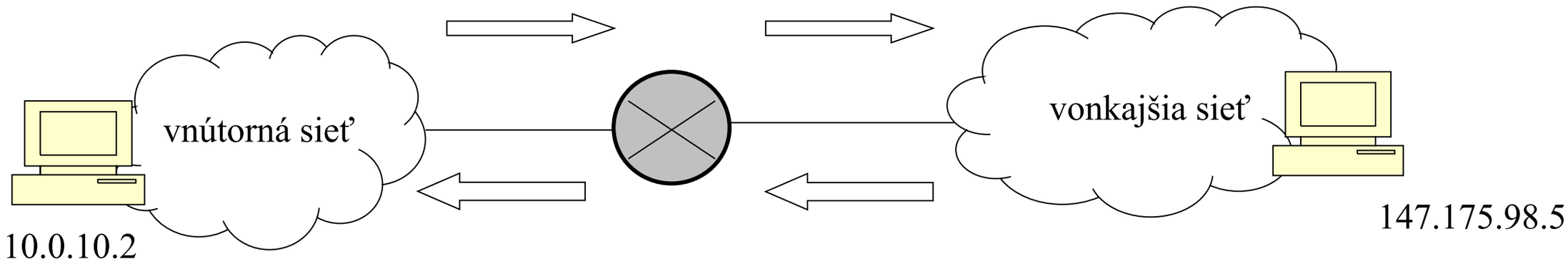
Smerovače s NAT



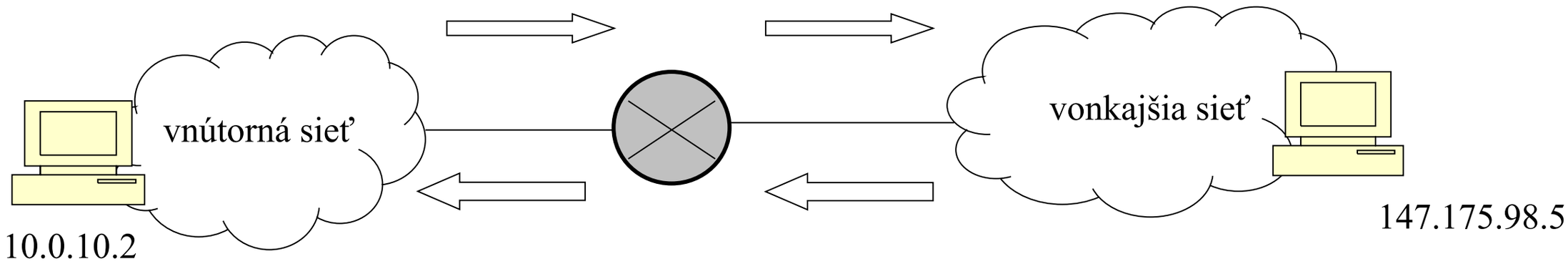
Smerovače s NAT



Smerovače s NAT



Smerovače s NAT

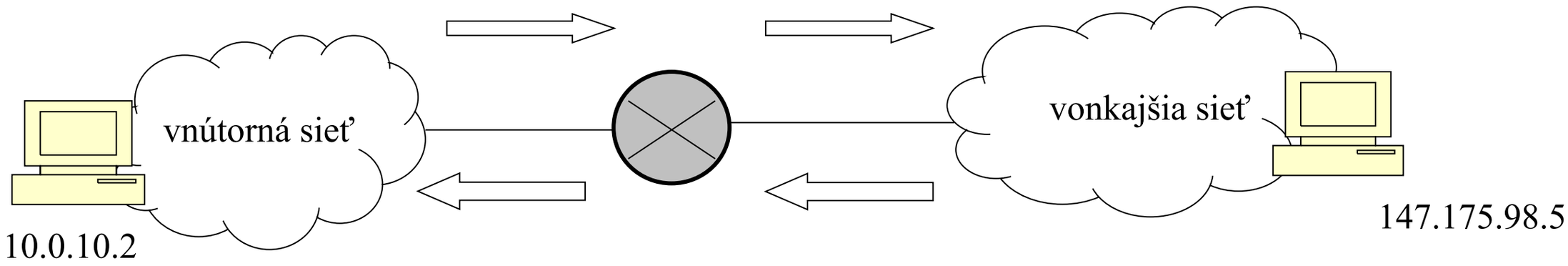


S-IP	D-IP
10.0.10.2	147.175.98.5

⇨

S-IP	D-IP
130.30.30.2	147.175.98.5

Smerovače s NAT



S-IP	D-IP
10.0.10.2	147.175.98.5

⇒

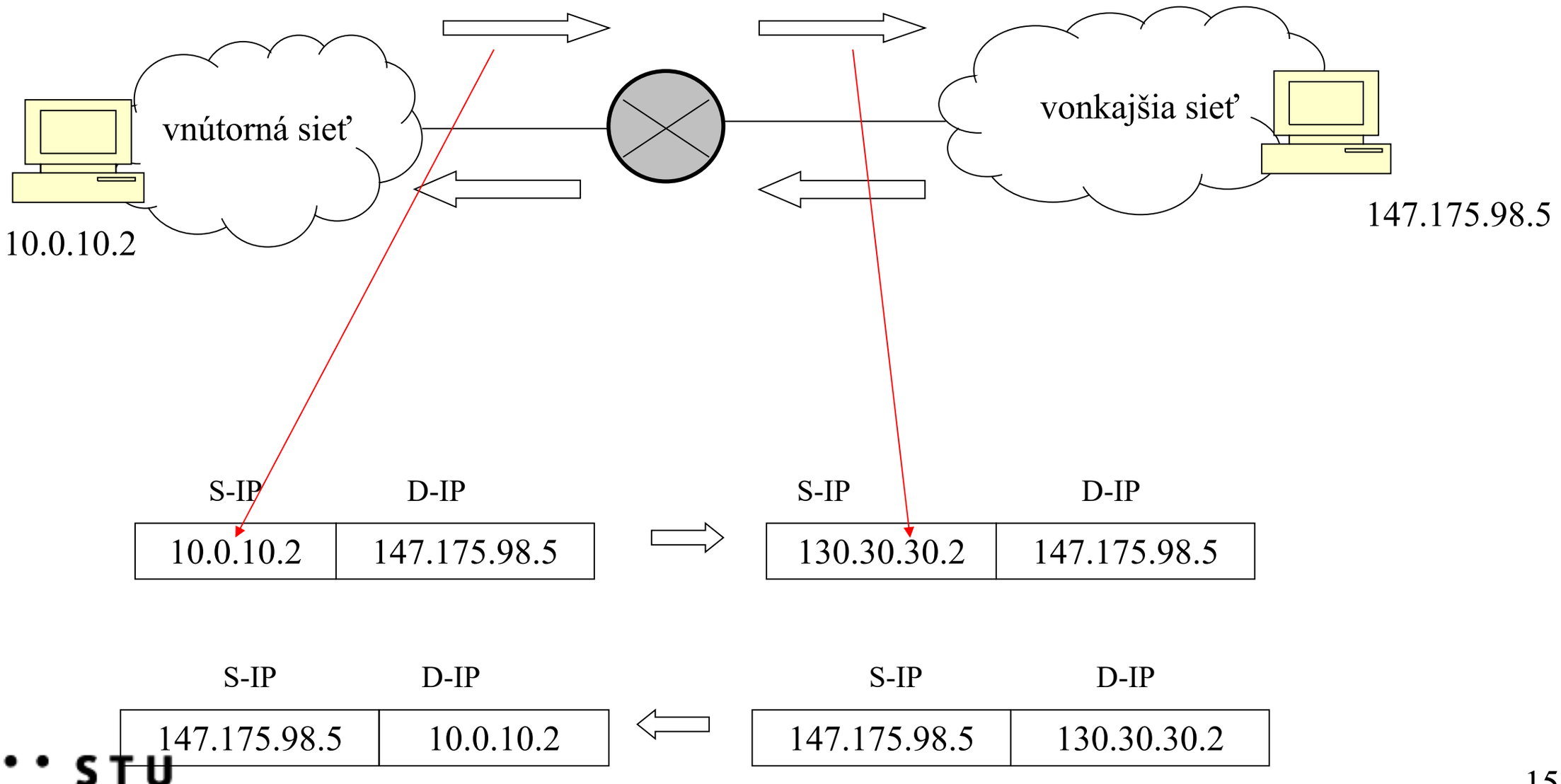
S-IP	D-IP
130.30.30.2	147.175.98.5

S-IP	D-IP
147.175.98.5	10.0.10.2

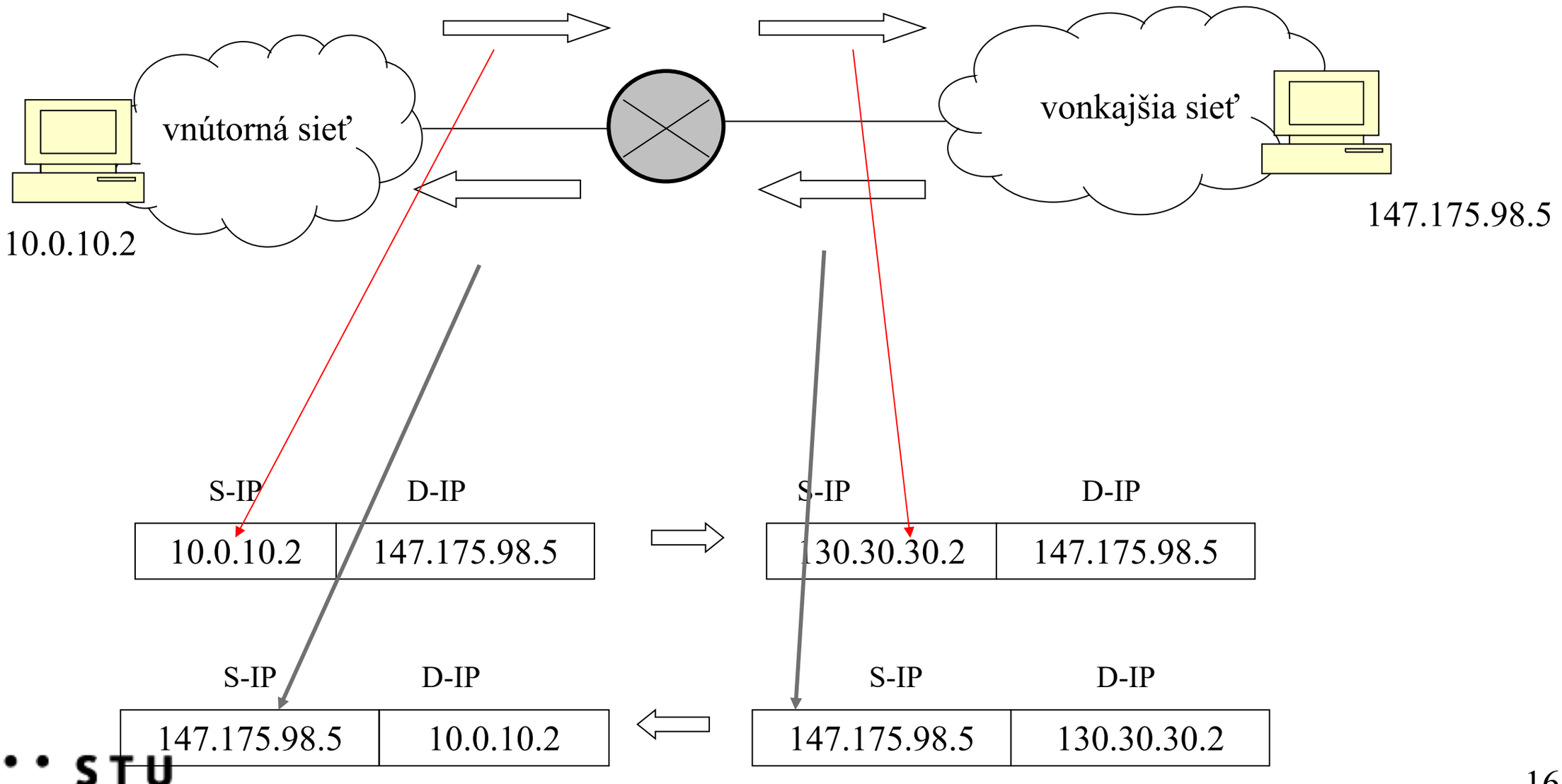
⇐

S-IP	D-IP
147.175.98.5	130.30.30.2

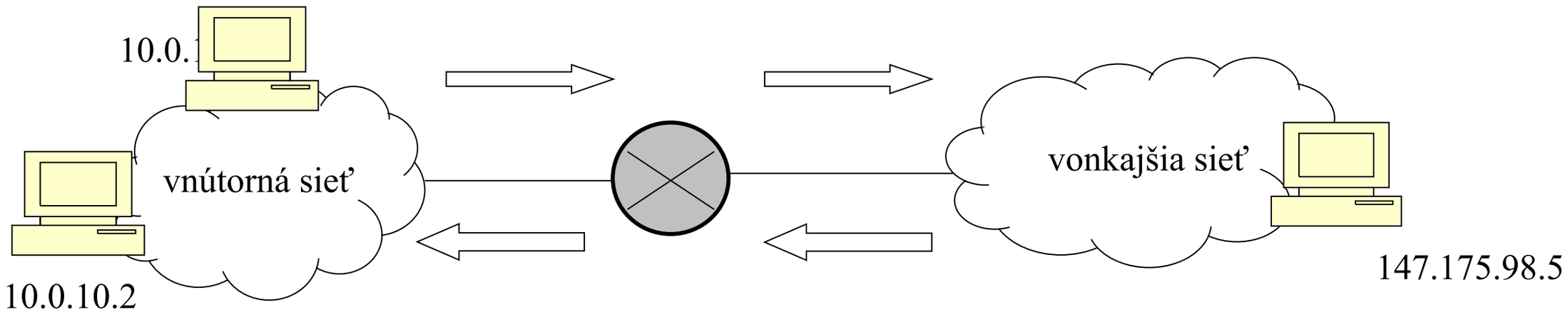
Smerovače s NAT



Smerovače s NAT



Smerovače s NAT



S-IP	D-IP
10.0.10.2	147.175.98.5

S-IP	D-IP
130.30.30.2	147.175.98.5

S-IP	D-IP
10.0.10.3	147.175.98.5

S-IP	D-IP
130.30.30.3	147.175.98.5

S-IP	D-IP
147.175.98.5	10.0.10.2

S-IP	D-IP
147.175.98.5	130.30.30.2

S-IP	D-IP
147.175.98.5	10.0.10.3

S-IP	D-IP
147.175.98.5	130.30.30.3

Jednosmerný statický NAT

Konfigurovanie

– NAT tabuľka

ip nat inside source static 10.0.0.2 130.30.30.2

ip nat inside source static 10.0.0.3 130.30.30.3

– rozhranie

interface ethernet 0

ip nat inside

interface serial 1

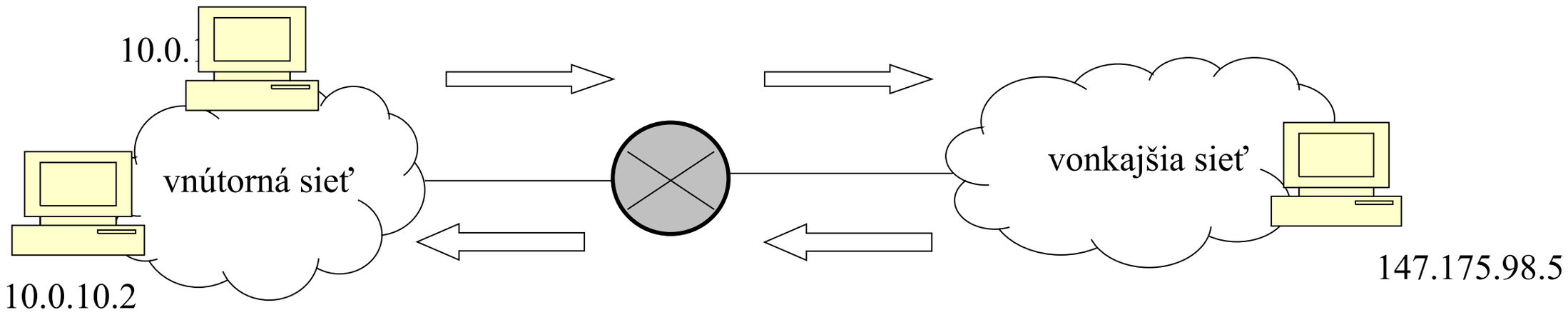
ip nat outside

Jednosmerný dynamický NAT

Konfigurovanie

- určiť rozsah IP adries, ktoré sa budú alokovať
  - **ip nat pool** <meno> <zač. IP> <kon. IP> **network** <sieť. maska>
- určiť s ACL vnútorné IP adresy, ktoré sa budú transformovať
  - **access-list** <No.> **permit** <IP adresa> <maska>
- prepojiť ACL s rozsahom adries
  - **ip nat inside source list** <No.> **pool** <meno>
- určiť rozhranie “inside” a “outside”
  - **interface** ethernet 0
  - **ip nat inside**
  - **interface** serial 1
  - **ip nat outside**

Smerovače s NAT



S-IP	D-IP
10.0.10.2	147.175.98.5

⇒

S-IP	D-IP
130.30.30.2	147.175.98.5

S-IP	D-IP
10.0.10.3	147.175.98.5

⇒

S-IP	D-IP
130.30.30.2	147.175.98.5

S-IP	D-IP
147.175.98.5	10.0.10.2

⇐ ????

S-IP	D-IP
147.175.98.5	130.30.30.2

S-IP	D-IP
147.175.98.5	10.0.10.3

⇐ ????

S-IP	D-IP
147.175.98.5	130.30.30.3

Rozšírený NAT

(overloaded, port-based, PAT, NAPT)

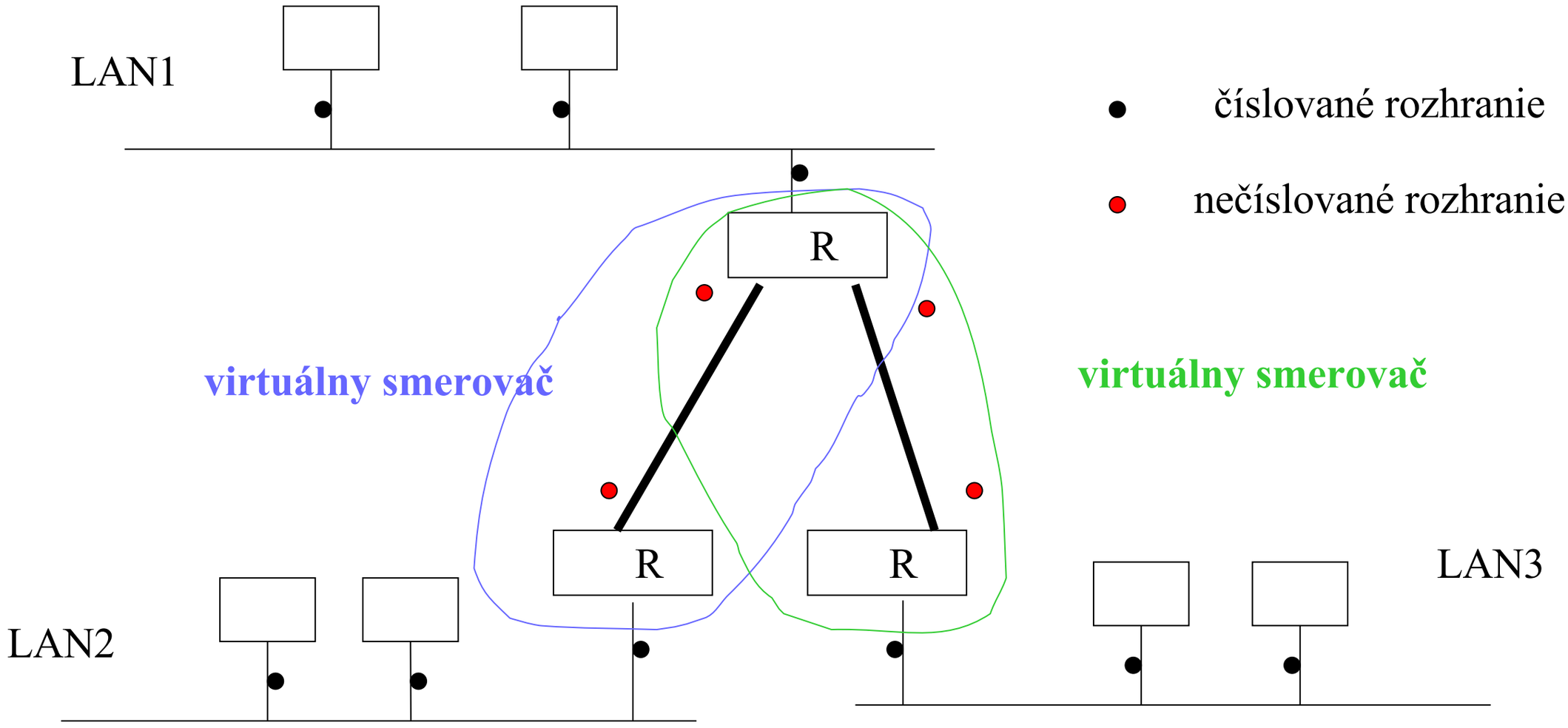
- transformácia portov
- menší počet (aj jedna) verejných IP adries

Vnútorná IP adresa : port	Preklad vnútornej IP adresy : port	Vonkajšia IP adresa : port
10.2.5.3 : 1750	168.20.2.8 : 1750	147.175.98.30 : 53
10.2.5.4 : 1750	168.20.2.8 : 1486	147.175.98.30 : 53
10.2.5.2 : 1650	168.20.2.8 : 1650	147.175.98.30 : 53

Nečíslované sieťové rozhranie

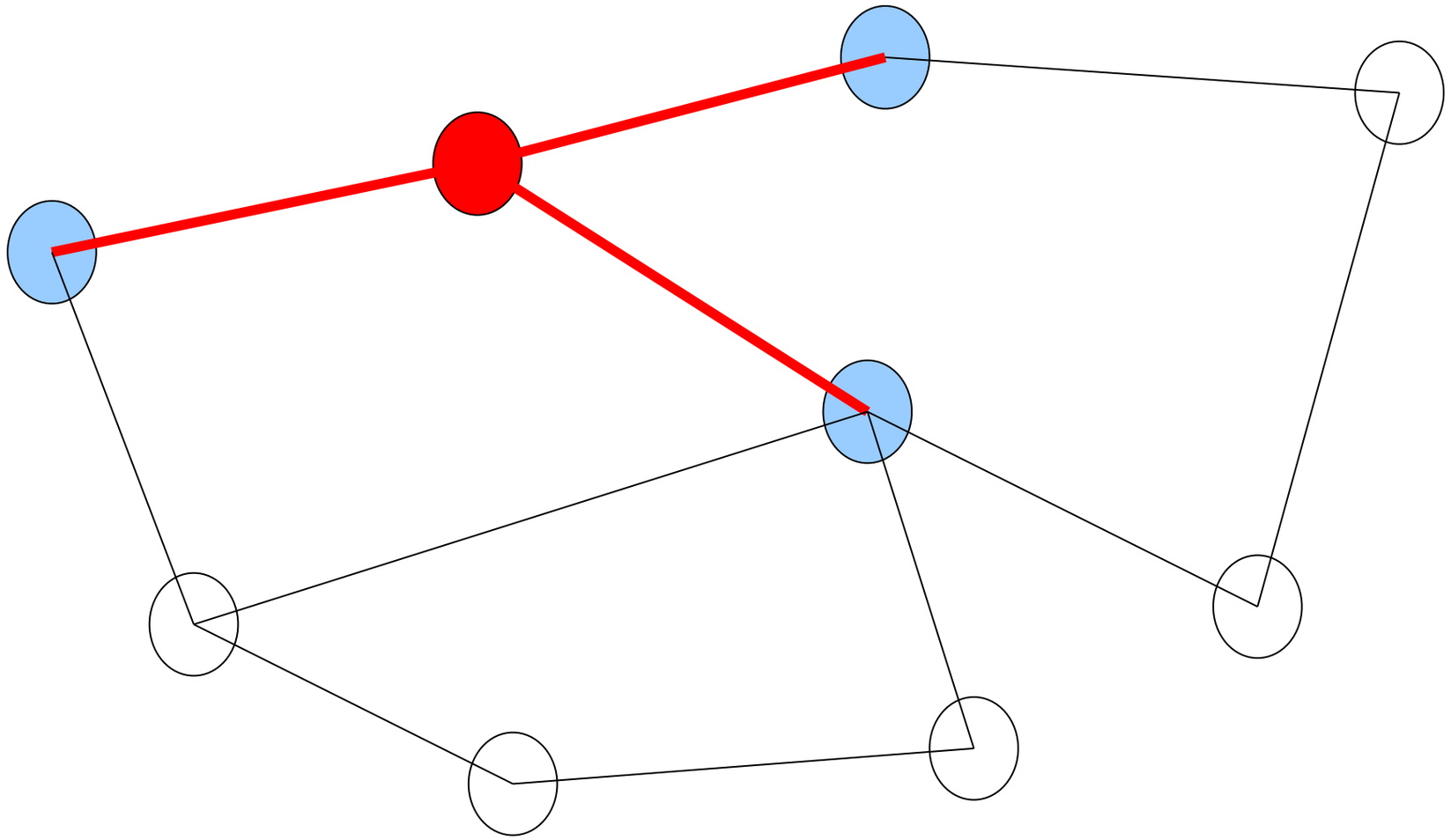
Nečíslované sieťové rozhranie (unnumbered interface)

– dvojbodové spojenia nemusia mať IP adresy



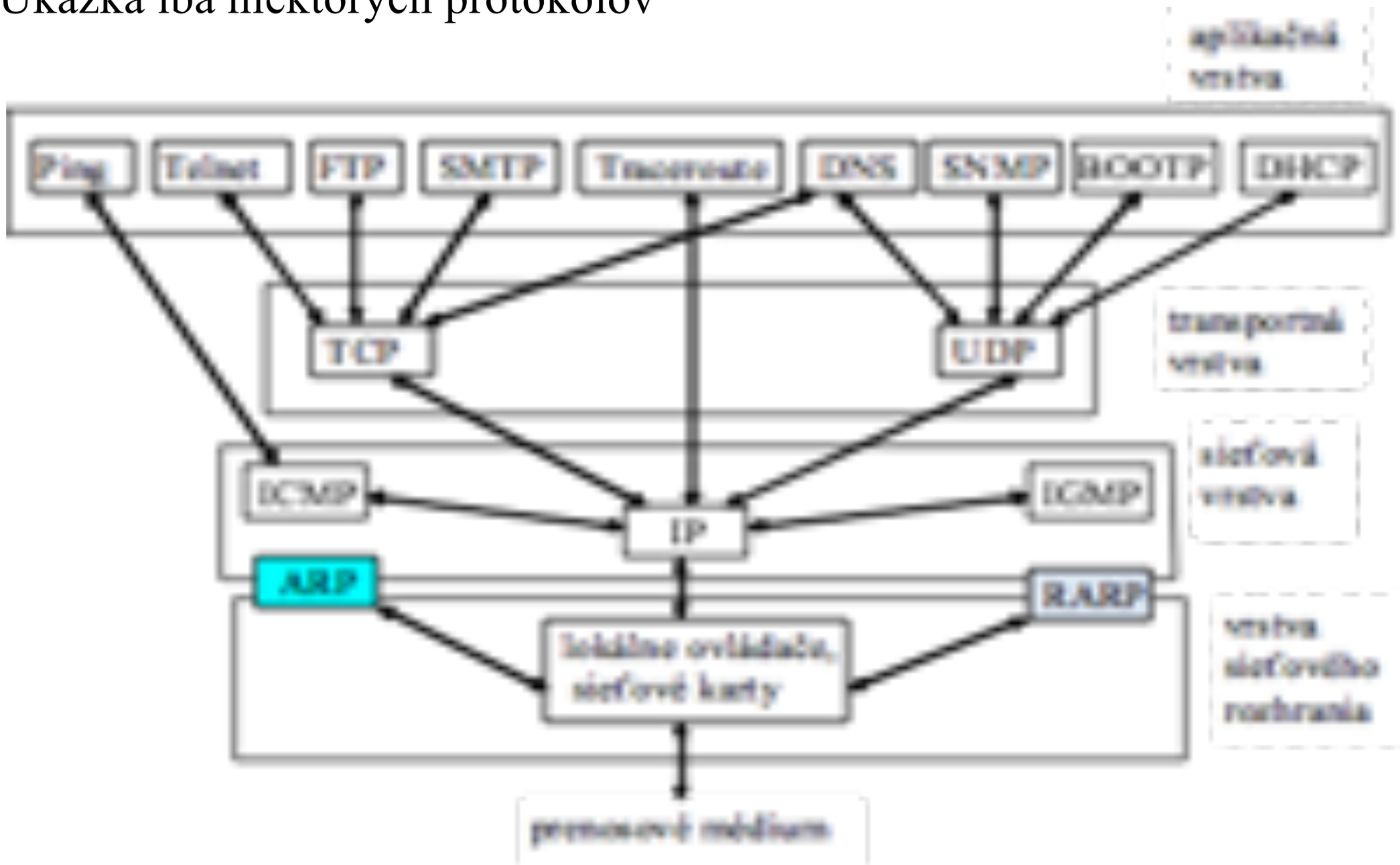
Linková vrstva

“Pohľad vrstiev” na topológiu siete
dátová vrstva



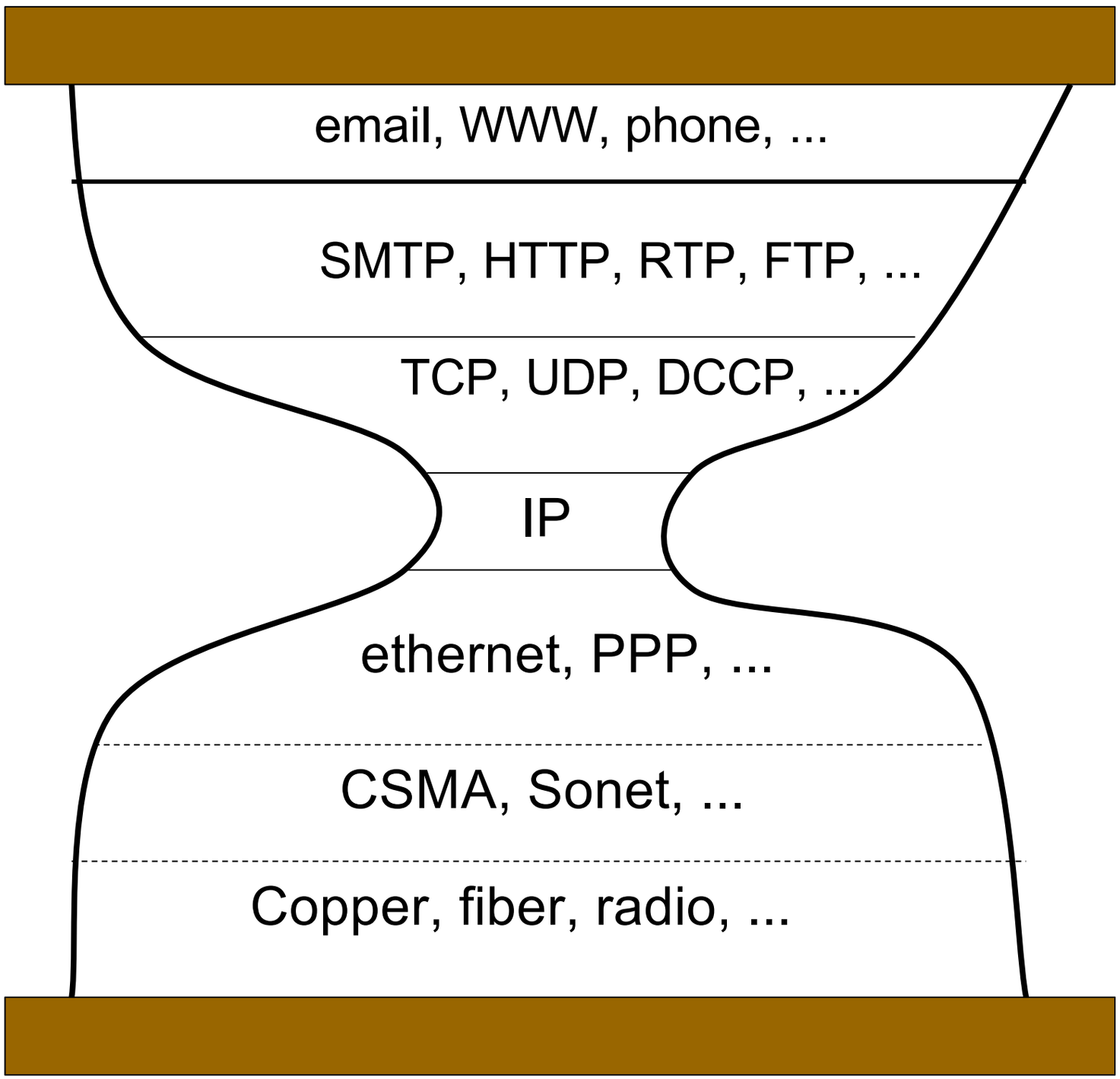
Protokolový zásobník TCP/IP

Ukážka iba niektorých protokolov



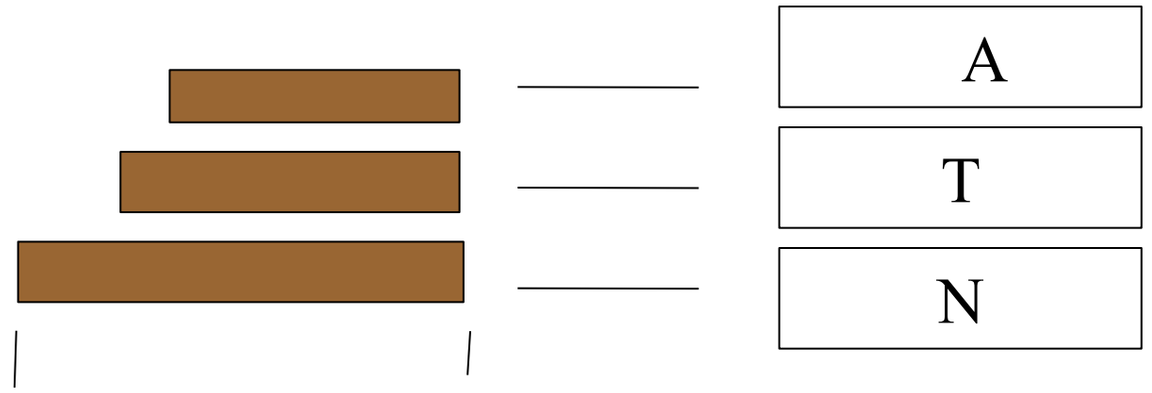
The Internet Hourglass

Presented by Steve Deering at London IETF plenary session



Sieť Ethernet – rámce

Typy rámcov:

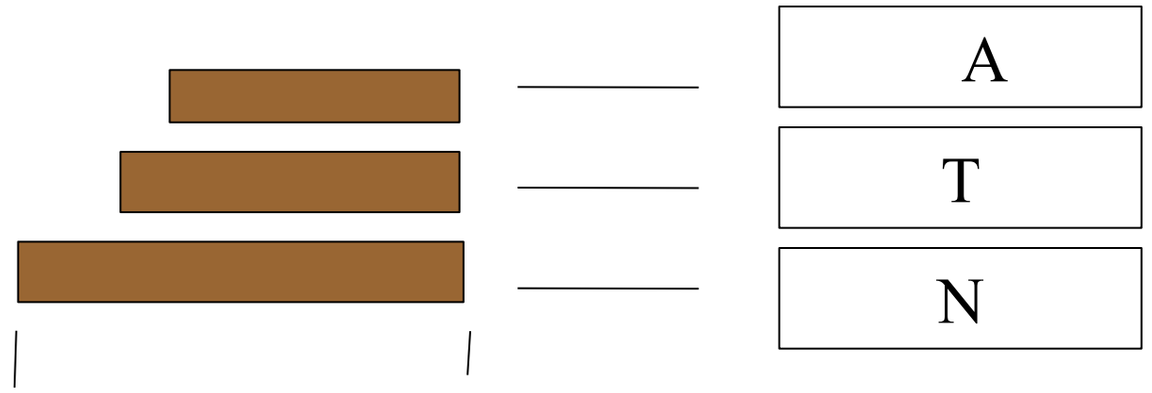


- Ethernet II

preamble	DA	SA	Type	Data	Pad	FCS
8B	6B	6B	2B	46 – 1500B		4B

Sieť Ethernet – rámce

Typy rámcov:



❑ Ethernet II

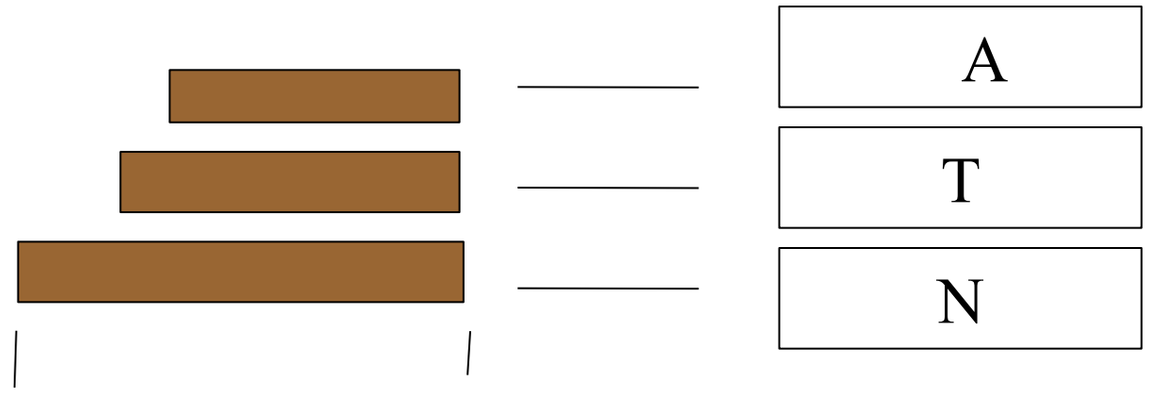
preamble	DA	SA	Type	Data	Pad	FCS
8 B	6 B	6 B	2 B	46-1500 B		4 B

❑ IEEE 802.3

preamble	SFD	DA	SA	Length	Data	Pad	FCS
7 B	1 B	6 B	6 B	2 B	46-1500 B		4 B

Sieť Ethernet – rámce

Typy rámcov:



❑ Ethernet II

preamble	DA	SA	Type	Data	Pad	FCS
8 B	6 B	6 B	2 B	46-1500 B		4 B

❑ IEEE 802.3

preamble	SFD	DA	SA	Length	Data	Pad	FCS
7 B	1 B	6 B	6 B	2 B	46-1500 B		4 B

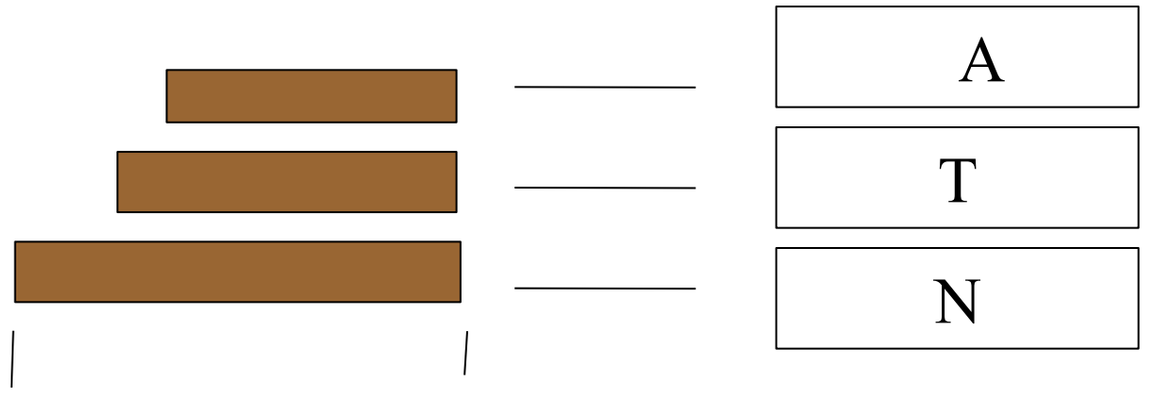
LLC (802.2)

SNAP

"raw“

Sieť Ethernet – rámce

Typy rámcov:



❑ Ethernet II

preamble	DA	SA	Type	Data	Pad	FCS
8 B	6 B	6 B	2 B	46-1500 B		4 B

❑ IEEE 802.3

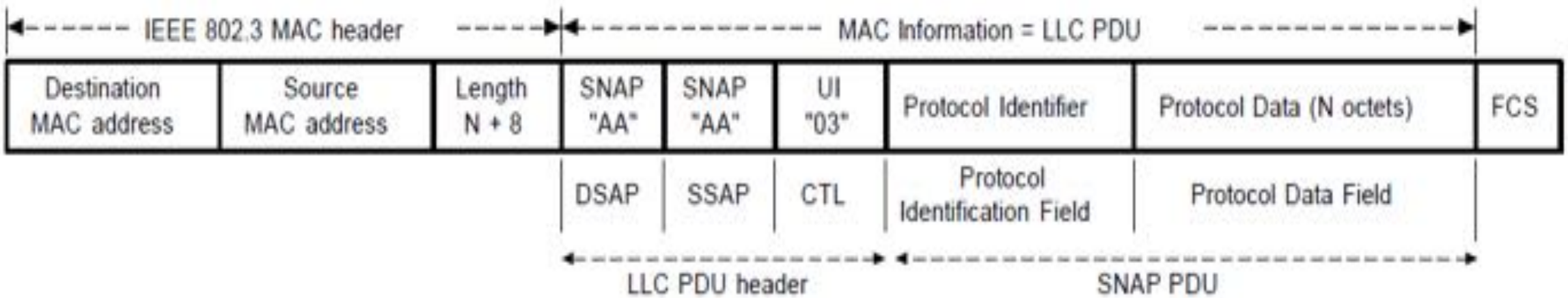
preamble	SFD	DA	SA	Length	Data	Pad	FCS
7 B	1 B	6 B	6 B	2 B	46-1500 B		4 B

LLC (802.2)

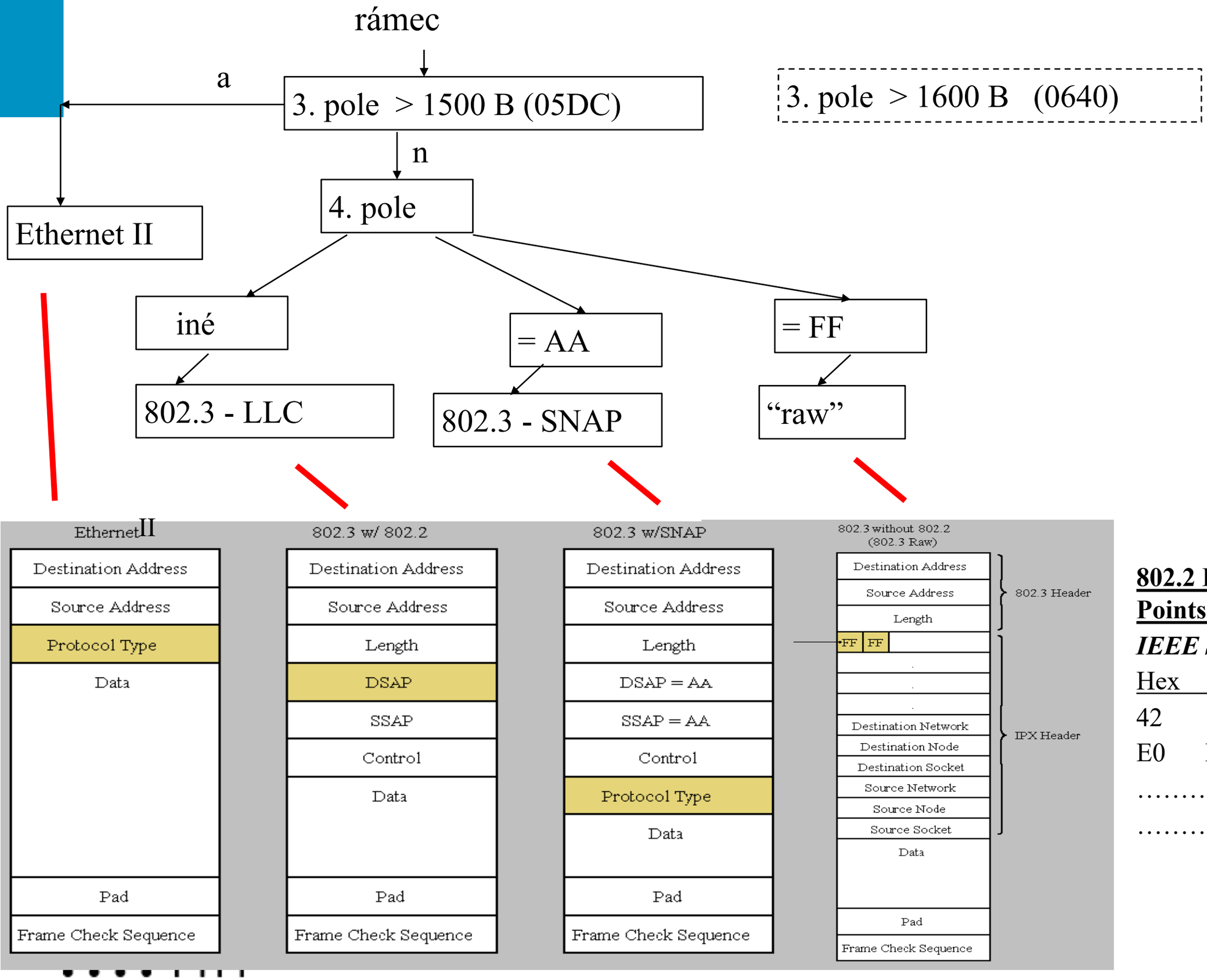
SNAP

"raw“

SNAP PDU v MAC rámci IEEE 802.3



Sieť Ethernet - rámce



802.2 LLC Service Access Points (SAPs)

IEEE SAPs

Hex	Function
42	BPDU
E0	IPX
.....	
.....	

No.	Time	Source	Destination	Protocol	Src port	Dst port	length	Info
1	0.000000	3Com_a4:e4:8c	Broadcast	ARP			60	Who has 147.175.98.147? Tell 147.175.98.1
2	0.466750	Standard_05:51:2b	Broadcast	ARP			60	Who has 147.175.98.116? Tell 147.175.98.30
3	1.002145	147.175.98.238	147.175.98.1	NBNS	netbios-	netbios-	92	Name query NB ENIGMA<20>
4	1.003246	147.175.98.1	147.175.98.238	NBNS	netbios-	netbios-	104	Name query response NB 147.175.98.232
5	1.003585	Western0_d7:80:c2	Broadcast	ARP			42	Who has [illegible]
6	1.004018	3Com_13:97:df	Western0_d7:80:c2	ARP			60	147.175.98.232 is at 00:04:76:13:97:df
7	1.004053	147.175.98.238	147.175.98.232	TCP	omnivisi	netbios-	62	omnivision > netbios-ssn [SYN] Seq=0 Win=16384 Le
8	1.004726	147.175.98.232	147.175.98.238	TCP	netbios-	omnivisi	62	netbios-ssn > omnivision [SYN, ACK] Seq=0 Ack=1 W
9	1.004839	147.175.98.238	147.175.98.232	TCP	omnivisi	netbios-	54	omnivision > netbios-ssn [ACK] Seq=1 Ack=1 Win=17
10	1.004930	147.175.98.238	147.175.98.232	NBSS	omnivisi	netbios-	126	Session request, to ENIGMA<20> from AA-DO4PZ2V1P0
11	1.005817	147.175.98.232	147.175.98.238	NBSS	netbios-	omnivisi	60	Positive session response

```
Frame 5 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Western0_d7:80:c2 (00:00:c0:d7:80:c2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Western0_d7:80:c2 (00:00:c0:d7:80:c2)
    Sender IP address: 147.175.98.238 (147.175.98.238)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 147.175.98.232 (147.175.98.232)
```

```
0000  ff ff ff ff ff ff 00 00  c0 d7 80 c2 08 06 00 01   ........ ........
0010  08 00 06 04 00 01 00 00  c0 d7 80 c2 93 af 62 ee   ........ ......b.
0020  00 00 00 00 00 00 93 af  62 e8                     ........ b.
```

File Edit View Go Capture Analyze Statistics Help

Filter: • Expression... Clear Apply

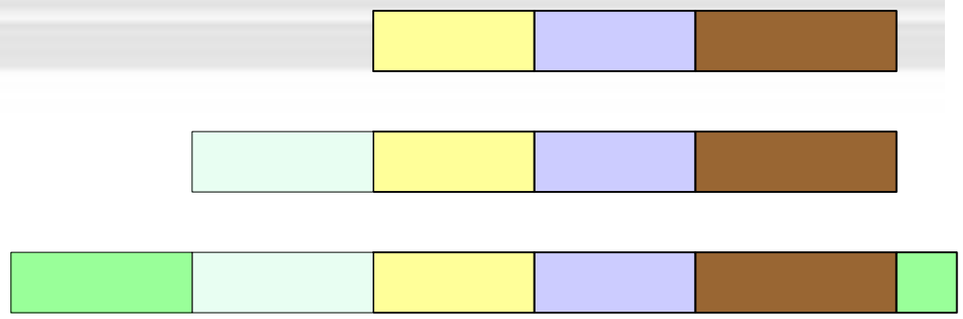
No.	Time	Source	Destination	Protocol	Src port	Dst port	Length	Info
1	0.000000	3Com_a4:e4:8c	Broadcast	ARP			60	who has 147.175.98.147? Tell 147.175.98.1
2	0.466750	Standard_05:51:2b	Broadcast	ARP			60	who has 147.175.98.116? Tell 147.175.98.90
3	1.002145	147.175.98.238	147.175.98.1	NBNS	netbios-	netbios-	92	Name query NB ENIGMA<20>
4	1.003246	147.175.98.1	147.175.98.238	NBNS	netbios-	netbios-	104	Name query response NB 147.175.98.232
5	1.003385	Western0_d7:80:c2	Broadcast	ARP			42	who has 147.175.98.232? Tell 147.175.98.238
6	1.004018	3Com_11:97:df	Western0_d7:80:c2	ARP			60	147.175.98.232 is at 00:04:76:11:97:df
7	1.004053	147.175.98.238	147.175.98.232	TCP	omnivisi	netbios-	62	omnivision > netbios-ssn [SYN] Seq=0 Win=16384 Len=0 MSS=
8	1.004726	147.175.98.232	147.175.98.238	TCP	netbios-	omnivisi	62	netbios-ssn > omnivision [SYN, ACK] Seq=0 Ack=1 Win=65535
9	1.004839	147.175.98.238	147.175.98.232	TCP	omnivisi	netbios-	54	omnivision > netbios-ssn [ACK] Seq=1 Ack=1 Win=17520 Len=
10	1.004930	147.175.98.238	147.175.98.232	NBSS	omnivisi	netbios-	126	Session request, to ENIGMA<20> from AA-DDAPZ2V1PGSV<00>
11	1.005817	147.175.98.232	147.175.98.238	NBSS	netbios-	omnivisi	60	Positive session response

- Frame 6 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: 3Com_11:97:df (00:04:76:11:97:df), Dst: Western0_d7:80:c2 (00:00:c0:d7:80:c2)
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (0x0001)
  - Protocol type: IP (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (0x0002)
  - Sender MAC address: 3Com_11:97:df (00:04:76:11:97:df)
  - Sender IP address: 147.175.98.232 (147.175.98.232)
  - Target MAC address: Western0_d7:80:c2 (00:00:c0:d7:80:c2)
  - Target IP address: 147.175.98.238 (147.175.98.238)

```
0000  00 00 c0 d7 80 c2 00 04  76 11 97 df 08 06 00 01   ........ v.......
0010  08 00 06 04 00 02 00 04  76 11 97 df 93 af 62 e8   ........ v.....b.
0020  00 00 c0 d7 80 c2 93 af  62 ee 00 00 00 00 00 00   ........ b.......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0x56c83203
2	0.001653	192.168.1.1	192.168.1.3	DHCP	DHCP ACK - Transaction ID 0x56c83203
3	15.710976	192.168.1.3	195.80.171.4	DNS	Standard query A cisco.netacad.net
4	15.728807	195.80.171.4	192.168.1.3	DNS	Standard query response A 128.107.229.50
5	15.736346	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
6	15.928457	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
7	16.732516	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
8	16.925467	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
9	17.732481	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
10	17.925010	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
11	18.732460	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
12	18.923814	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
13	20.723404	D-Link_fa:94:63	HewlettP_06:e0:93	ARP	Who has 192.168.1.3? Tell 192.168.1.1
14	20.723424	HewlettP_06:e0:93	D-Link_fa:94:63	ARP	192.168.1.3 is at 00:14:38:06:e0:93
15	29.999418	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0xa64ef4b1

- Frame 1 (342 bytes on wire, 342 bytes captured)
- Ethernet II, Src: HewlettP_06:e0:93 (00:14:38:06:e0:93), Dst: D-Link_fa:94:63 (00:0d:88:fa:94:63)
- Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol



11100011…01101010

E3……..6A

```
0000  00 0d 88 fa 94 63 00 14  38 06 e0 93 08 00 45 00   .....c.. 8.....E.
0010  01 48 71 9c 00 00 80 11  44 b4 c0 a8 01 03 c0 a8   .Hq..... D.......
0020  01 01 00 44 00 43 01 34  65 ac 01 01 06 00 56 c8   ...D.C.4 e.....V.
0030  32 03 00 00 00 00 c0 a8  01 03 00 00 00 00 00 00   2....... ........
```

• • • • FIN

Apply a display filter ... <⌘/>

Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1062…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2	0.000065	fe80::22cf…	ff02::1:ff…	ICMPv6	86	Neighbor Solicitation for fe80::20b:82ff:fe5d:4550 from 20:cf:30:e4:f2:bc
3	0.327113	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.164.205? Tell 147.175.144.1
4	0.327115	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.145.47? Tell 147.175.144.1
5	0.327116	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.145.190? Tell 147.175.144.1
6	0.327117	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.144.202? Tell 147.175.144.1
7	0.327118	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.144.219? Tell 147.175.144.1
8	0.327120	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.145.238? Tell 147.175.144.1
9	0.327121	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.144.112? Tell 147.175.144.1
10	0.327122	Flextron_b…	Broadcast	ARP	60	Who has 147.175.144.1? Tell 147.175.145.64
11	0.342508	AsustekC_6…	Broadcast	ARP	60	Who has 10.91.223.1? Tell 10.91.0.1
12	0.913268	fe80::ca07…	ff02::1:2	DHCPv6	207	Request XID: 0x90f685 CID: 000300090585c8671039485d IAA: fda3:5c73:a65c::7e9

```
▸ Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▾ Ethernet II, Src: Cisco_66:72:34 (84:b8:02:66:72:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Cisco_66:72:34 (84:b8:02:66:72:34)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000040fc1462
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Cisco_66:72:34 (84:b8:02:66:72:34)
    Sender IP address: 147.175.144.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 147.175.144.205
```

```
0000  ff ff ff ff ff ff 84 b8  02 66 72 34 08 06 00 01   ........ .fr4....
0010  08 00 06 04 00 01 84 b8  02 66 72 34 93 af 90 01   ........ .fr4....
0020  00 00 00 00 00 00 93 af  90 cd 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  40 fc 14 62              ........ @..b
```

Opcode (arp.opcode), 2 bytes

Packets: 2080 · Displayed: 2080 (100.0%)

Profile: Default

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1503	20.473852	147.175.14…	213.163.97…	ICMP	70	Destination unreachable (Port unreachable)

```
▸ Frame 1503: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▾ Ethernet II, Src: Apple_10:49:e0 (ac:87:a3:10:49:e0), Dst: Cisco_66:72:34 (84:b8:02:66:72:34)
  ▸ Destination: Cisco_66:72:34 (84:b8:02:66:72:34)
  ▸ Source: Apple_10:49:e0 (ac:87:a3:10:49:e0)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 147.175.145.224, Dst: 213.163.97.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xac04 (44036)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 147.175.145.224
    Destination: 213.163.97.104
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  84 b8 02 66 72 34 ac 87  a3 10 49 e0 08 00 45 00   ...fr4.. ..I...E.
0010  00 38 ac 04 00 00 40 01  00 00 93 af 91 e0 d5 a3   .8....@. ........
0020  61 68 03 03 d3 ac 00 00  00 00 45 00 01 bc 00 00   ah...... ..E.....
0030  40 00 37 11 e5 8c d5 a3  61 68 93 af 91 e0 13 e3   @.7..... ah......
0040  13 c4 01 a9 00 00                                 ......
```

Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1492	20.465193	13.107.6.1…	147.175.14…	TCP	1434	443 → 60446 [ACK] Seq=4105 Ack=218 Win=262656 Len=1368 TSval=2382096171 TSecr=1049717156 [TCP segment of a reasse…
1493	20.465194	13.107.6.1…	147.175.14…	TLSv1.2	247	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
1494	20.465271	147.175.14…	13.107.6.1…	TCP	66	60446 → 443 [ACK] Seq=218 Ack=2737 Win=128576 Len=0 TSval=1049717168 TSecr=2382096171
1495	20.465272	147.175.14…	13.107.6.1…	TCP	66	60446 → 443 [ACK] Seq=218 Ack=5473 Win=125856 Len=0 TSval=1049717168 TSecr=2382096171
1496	20.465272	147.175.14…	13.107.6.1…	TCP	66	60446 → 443 [ACK] Seq=218 Ack=5654 Win=125664 Len=0 TSval=1049717168 TSecr=2382096171
1497	20.465353	147.175.14…	13.107.6.1…	TCP	66	[TCP Window Update] 60446 → 443 [ACK] Seq=218 Ack=5654 Win=131072 Len=0 TSval=1049717168 TSecr=2382096171
1498	20.470444	Cisco_66:7…	Broadcast	ARP	60	Who has 147.175.145.223? Tell 147.175.144.1
1499	20.472749	147.175.14…	13.107.6.1…	TLSv1.2	141	Client Key Exchange
1500	20.472777	147.175.14…	13.107.6.1…	TLSv1.2	72	Change Cipher Spec
1501	20.472795	147.175.14…	13.107.6.1…	TLSv1.2	111	Encrypted Handshake Message
1502	20.473982	213.163.97…	147.175.14…	SIP	459	Request: OPTIONS sip:100@147.175.145.224 |
1503	20.473952	147.175.14…	213.163.97…	ICMP	70	Destination unreachable (Port unreachable)

▸ Frame 1494: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▾ Ethernet II, Src: Apple_18:49:e0 (ac:87:a3:18:49:e0), Dst: Cisco_66:72:34 (84:b8:02:66:72:34)
  ▸ Destination: Cisco_66:72:34 (84:b8:02:66:72:34)
  ▸ Source: Apple_18:49:e0 (ac:87:a3:18:49:e0)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 147.175.145.224, Dst: 13.107.6.151
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x4b4b (19275)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 147.175.145.224
    Destination: 13.107.6.151
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]

```
0000  84 b8 02 66 72 34 ac 87  a3 18 49 e0 08 00 45 00   ...fr4.. ..I...E.
0010  00 34 4b 4b 40 00 40 06  00 00 93 af 91 e0 0d 6b   .4KK@.@. .......k
0020  06 97 ec 3e 01 bb d0 24  d2 a0 e6 7d 65 a0 80 10   .......$ ...}e...
0030  01 b2 39 b0 00 00 01 01  08 0a 3e 91 69 b0 0d fb   ..9..... ..>.i...
0040  e7 2b                                             .+
```

Source hardware address (eth.src), 6 bytes — Packets: 2080 · Displayed: 2080 (100.0%) · Dropped: 0 (0.0%) — Profile: Default

Stop capturing packets

No.	Time	Source	Destination	Protocol	Length	Info
1250	19.071179	fe80::fc98…	ff02::c	SSDP	181	M-SEARCH * HTTP/1.1
1329	19.489090	147.175.14…	66.102.1.1…	STUN	90	Binding Request
1332	19.512595	66.102.1.1…	147.175.14…	STUN	74	Binding Success Response XOR-MAPPED-ADDRESS: 147.175.145.224:54113
1397	19.993818	fe80::468:…	ff02::1:3	LLMNR	86	Standard query 0x34c8 ABOY PC-203
1398	19.994149	147.175.14…	224.0.0.252	LLMNR	66	Standard query 0x34c8 ABOY PC-203
1399	19.997183	10.92.0.2	10.92.255.…	NBNS	92	Name query NB WORKGROUP<1e>
1403	20.010391	fe80::1062…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
1415	20.103333	fe80::468:…	ff02::1:3	LLMNR	86	Standard query 0x34c8 ABOY PC-203
1416	20.103360	147.175.14…	224.0.0.252	LLMNR	66	Standard query 0x34c8 ABOY PC-203
1420	20.135714	fe80::8987…	ff02::1:3	LLMNR	84	Standard query 0x8240 A wpad
1422	20.135884	147.175.14…	224.0.0.252	LLMNR	64	Standard query 0x8240 A wpad
1426	20.156098	147.175.14…	147.175.14…	NBNS	92	Name query NB WPAD<00>

```
▸ Frame 1399: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
▾ Ethernet II, Src: HewlettP_a7:f4:67 (00:0c:82:a7:f4:67), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: HewlettP_a7:f4:67 (00:0c:82:a7:f4:67)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.92.0.2, Dst: 10.92.255.255
▾ User Datagram Protocol, Src Port: 137, Dst Port: 137
    Source Port: 137
    Destination Port: 137
    Length: 58
    Checksum: 0xa12b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
▸ NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff 00 0c  82 a7 f4 67 08 00 45 00   ........ ...g..E.
0010  00 4e 32 e4 00 00 80 11  f3 01 0a 5c 00 02 0a 5c   .N2..... ...\...\
0020  ff ff 00 89 00 89 00 3a  a1 2b c5 06 01 10 00 01   .......: .+......
0030  00 00 00 00 00 00 20 46  48 45 50 46 43 45 4c 45   ...... F HEPFCELE
0040  48 46 43 45 50 46 46 46  41 43 41 43 41 43 41 43   HFCEPFFF ACACACAC
0050  41 43 41 43 41 42 4f 00  00 20 00 01              ACACABO. . ..
```

Stop capturing packets

stp

Expression…

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
2	2.005383	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
3	4.009585	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
4	6.014086	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
5	8.019261	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
6	10.024018	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
7	12.030370	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
8	14.033632	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
9	16.038664	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
10	18.043307	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
11	20.048408	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004
12	22.052808	Cisco_87:8…	Spanning-t…	STP	60	Conf. Root = 32768/100/00:1c:0e:87:70:00 Cost = 4 Port = 0x8004

▾ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 24, 2007 15:55:55.413456000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1193234155.413456000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 60 bytes (480 bits)
  Capture Length: 60 bytes (480 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:llc:stp]
  [Coloring Rule Name: Broadcast]
  [Coloring Rule String: eth[0] & 1]
▸ IEEE 802.3 Ethernet
▾ Logical-Link Control
  ▸ DSAP: Spanning Tree BPDU (0x42)
  ▸ SSAP: Spanning Tree BPDU (0x42)
  ▸ Control field: U, func=UI (0x03)

```
0000  01 80 c2 00 00 00 00 1c  0e 87 85 04 00 26 42 42   ........ .....&BB
0010  03 00 00 00 00 00 00 64  00 1c 0e 87 70 00 00 00   .......d ....p...
0020  00 04 00 64 00 1c 0e 87  85 00 00 04 01 00 14 00   ...d.... ........
0030  02 00 0f 00 00 00 00 00  00 00 00 00               ........ ....
```

Packets: 98 · Displayed: 98 (100.0%) · Load time: 0:0.1

Profile: Default

bootp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.25…	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.…	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.25…	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.…	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

```
▸ Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits)
▾ Ethernet II, Src: Grandstr_01:fc:42 (00:0b:82:01:fc:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Grandstr_01:fc:42 (00:0b:82:01:fc:42)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▾ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 280
    Checksum: 0x591f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▸ Bootstrap Protocol (Discover)
```

```
0000  ff ff ff ff ff ff 00 0b  82 01 fc 42 08 00 45 00   ........ ...B..E.
0010  01 2c a8 36 00 00 fa 11  17 8b 00 00 00 00 ff ff   .,.6.... ........
0020  ff ff 00 44 00 43 01 18  59 1f 01 01 06 00 00 00   ...D.C.. Y.......
0030  3d 1d 00 00 00 00 00 00  00 00 00 00 00 00 00 00   =....... ........
0040  00 00 00 00 00 00 00 0b  82 01 fc 42 00 00 00 00   ........ ...B....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

http

Capture options

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2210	23.360371	147.175.14…	147.175.1…	HTTP	672	GET / HTTP/1.1
2307	23.714984	147.175.1…	147.175.14…	HTTP	1332	HTTP/1.1 200 OK (text/html)
2327	23.875527	147.175.14…	147.175.1…	HTTP	570	GET /new/web_css/normalize.min.css HTTP/1.1
2330	23.876343	147.175.1…	147.175.14…	HTTP	958	HTTP/1.1 200 OK (text/css)
2342	23.884978	147.175.14…	147.175.1…	HTTP	697	GET /css/bootstrap.min.css HTTP/1.1
2470	23.888387	147.175.1…	147.175.14…	HTTP	539	HTTP/1.1 200 OK (text/css)
2487	23.894436	147.175.14…	147.175.1…	HTTP	585	GET /new/web_css/bootstrap-theme.min.css HTTP/1.1
2510	23.895751	147.175.1…	147.175.14…	HTTP	330	HTTP/1.1 200 OK (text/css)
2531	23.902089	147.175.14…	147.175.1…	HTTP	700	GET /css/font-awesome.min.css HTTP/1.1
2550	23.903340	147.175.1…	147.175.14…	HTTP	548	HTTP/1.1 200 OK (text/css)
2574	23.910286	147.175.14…	147.175.1…	HTTP	578	GET /new/web_css/flickity.min.css HTTP/1.1
2577	23.910965	147.175.1…	147.175.14…	HTTP	1150	HTTP/1.1 200 OK (text/css)

▸ Frame 2210: 672 bytes on wire (5376 bits), 672 bytes captured (5376 bits) on interface 0

▾ Ethernet II, Src: Apple_18:49:e0 (ac:87:a3:18:49:e0), Dst: Cisco_66:72:34 (84:b8:02:66:72:34)

▸ Destination: Cisco_66:72:34 (84:b8:02:66:72:34)

▸ Source: Apple_18:49:e0 (ac:87:a3:18:49:e0)

Type: IPv4 (0x0800)

▸ Internet Protocol Version 4, Src: 147.175.145.224, Dst: 147.175.1.34

▸ Transmission Control Protocol, Src Port: 62296, Dst Port: 80, Seq: 1, Ack: 1, Len: 606

▸ Hypertext Transfer Protocol

```
0000  84 b8 02 66 72 34 ac 87  a3 18 49 e0 08 00 45 00   ...fr4.. ..I...E.
0010  02 92 dd 72 40 00 40 06  00 00 93 af 91 e0 93 af   ...r@.@. ........
0020  01 22 f3 58 00 50 64 52  7b fd c6 c8 8d ee 80 18   ."·X·PdR {.......
0030  10 00 bc f9 00 00 01 01  08 0a 3e e8 d2 06 0c 38   ........ ..>....8
0040  2f 38 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   /8GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 66 69 69 74   ..Host:  www.flit
0060  2e 73 74 75 62 61 2e 73  6b 0d 0a 41 63 63 65 70   .stuba.s k..Accep
0070  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c 61 70 70   t: text/ html,app
0080  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d 6c 2b 78   lication /xhtml+x
0090  6d 6c 2c 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   ml,appli cation/x
00a0  6d 6c 3b 71 3d 30 2e 39  2c 2a 2f 2a 3b 71 3d 30   ml;q=0.9 ,*/*;q=0
00b0  2e 38 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   .8..Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
```

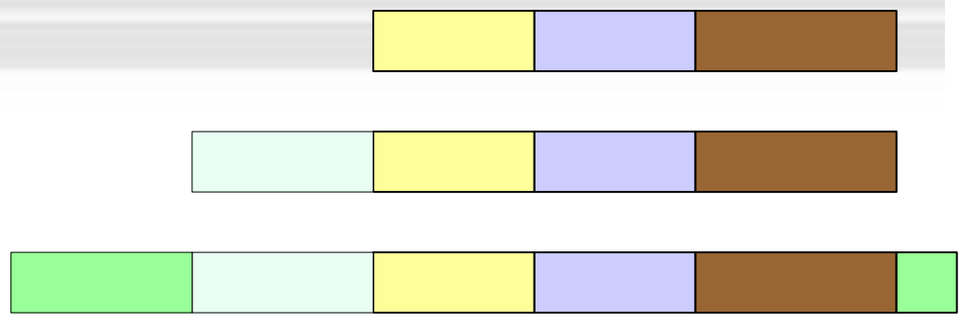
wireshark_en0_20170825083630_x8vn9C

Packets: 6362 · Displayed: 108 (1.7%)

Profile: Default

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0x56c83203
2	0.001653	192.168.1.1	192.168.1.3	DHCP	DHCP ACK - Transaction ID 0x56c83203
3	15.710976	192.168.1.3	195.80.171.4	DNS	Standard query A cisco.netacad.net
4	15.728807	195.80.171.4	192.168.1.3	DNS	Standard query response A 128.107.229.50
5	15.736346	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
6	15.928457	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
7	16.732516	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
8	16.925467	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
9	17.732481	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
10	17.925010	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
11	18.732460	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
12	18.923814	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
13	20.723404	D-Link_fa:94:63	HewlettP_06:e0:93	ARP	Who has 192.168.1.3? Tell 192.168.1.1
14	20.723424	HewlettP_06:e0:93	D-Link_fa:94:63	ARP	192.168.1.3 is at 00:14:38:06:e0:93
15	29.999418	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0xa64ef4b1

- Frame 1 (342 bytes on wire, 342 bytes captured)
- Ethernet II, Src: HewlettP_06:e0:93 (00:14:38:06:e0:93), Dst: D-Link_fa:94:63 (00:0d:88:fa:94:63)
- Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol



11100011…01101010

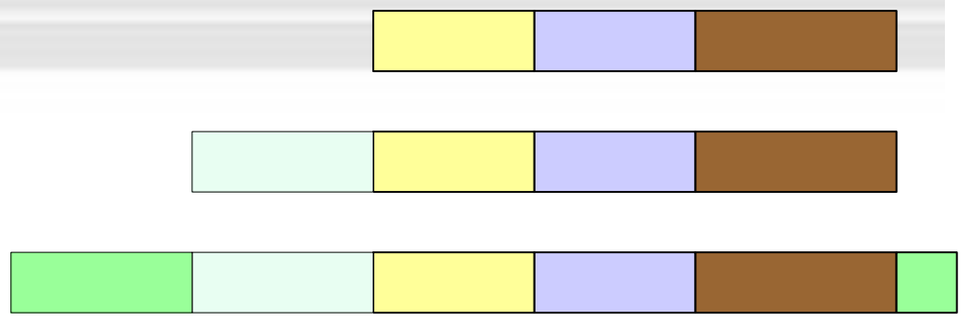
E3……..6A

```
0000  00 0d 88 fa 94 63 00 14  38 06 e0 93 08 00 45 00   .....c.. 8.....E.
0010  01 48 71 9c 00 00 80 11  44 b4 c0 a8 01 03 c0 a8   .Hq..... D.......
0020  01 01 00 44 00 43 01 34  65 ac 01 01 06 00 56 c8   ...D.C.4 e.....V.
0030  32 03 00 00 00 00 c0 a8  01 03 00 00 00 00 00 00   2....... ........
```

• • • • FIN

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0x56c83203
2	0.001653	192.168.1.1	192.168.1.3	DHCP	DHCP ACK - Transaction ID 0x56c83203
3	15.710976	192.168.1.3	195.80.171.4	DNS	Standard query A cisco.netacad.net
4	15.728807	195.80.171.4	192.168.1.3	DNS	Standard query response A 128.107.229.50
5	15.736346	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
6	15.928457	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
7	16.732516	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
8	16.925467	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
9	17.732481	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
10	17.925010	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
11	18.732460	192.168.1.3	128.107.229.50	ICMP	Echo (ping) request
12	18.923814	128.107.229.50	192.168.1.3	ICMP	Echo (ping) reply
13	20.723404	D-Link_fa:94:63	HewlettP_06:e0:93	ARP	Who has 192.168.1.3? Tell 192.168.1.1
14	20.723424	HewlettP_06:e0:93	D-Link_fa:94:63	ARP	192.168.1.3 is at 00:14:38:06:e0:93
15	29.999418	192.168.1.3	192.168.1.1	DHCP	DHCP Request - Transaction ID 0xa64ef4b1

- Frame 1 (342 bytes on wire, 342 bytes captured)
- Ethernet II, Src: HewlettP_06:e0:93 (00:14:38:06:e0:93), Dst: D-Link_fa:94:63 (00:0d:88:fa:94:63)
- Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol



11100011…01101010

E3……..6A

```
0000  00 0d 88 fa 94 63 00 14  38 06 e0 93 08 00 45 00   .....c.. 8.....E.
0010  01 48 71 9c 00 00 80 11  44 b4 c0 a8 01 03 c0 a8   .Hq..... D.......
0020  01 01 00 44 00 43 01 34  65 ac 01 01 06 00 56 c8   ...D.C.4 e.....V.
0030  32 03 00 00 00 00 c0 a8  01 03 00 00 00 00 00 00   2....... ........
```

• • • • FIN

eth4.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
18	6.791664	147.175.99.30	147.175.98.238	DNS	Standard query response PTR Golem.dcs.elf.stuba.sk
19	7.539818	147.175.98.238	147.175.99.30	DNS	Standard query A Golem.dcs.elf.stuba.sk
20	7.542592	147.175.99.30	147.175.98.238	DNS	Standard query response A 147.175.98.28
21	7.589601	147.175.98.238	209.11.45.139	TCP	crrprotocol > http [SYN] Seq=0 Win=16384 Len=0 MSS=1
22	7.687735	209.11.45.139	147.175.98.238	TCP	http > crrprotocol [SYN, ACK] Seq=0 Ack=1 Win=5840 L
23	7.687844	147.175.98.238	209.11.45.139	TCP	crrprotocol > http [ACK] Seq=1 Ack=1 Win=16560 Len=0
24	7.688471	147.175.98.238	209.11.45.139	HTTP	GET /heartbeat?program=weather&partner=CAST1202&id=E
25	7.711885	Standard_05:51:2b	Broadcast	ARP	Who has 147.175.98.72? Tell 147.175.98.30
26	7.787027	209.11.45.139	147.175.98.238	TCP	http > crrprotocol [ACK] Seq=1 Ack=312 Win=6432 Len=
27	7.789080	209.11.45.139	147.175.98.238	HTTP	HTTP/1.1 200 OK (text/plain)
28	7.789103	209.11.45.139	147.175.98.238	TCP	http > crrprotocol [FIN, ACK] Seq=406 Ack=312 Win=64
29	7.789173	147.175.98.238	209.11.45.139	TCP	crrprotocol > http [ACK] Seq=312 Ack=407 Win=16155 L
30	7.790671	147.175.98.238	209.11.45.139	TCP	crrprotocol > http [FIN, ACK] Seq=312 Ack=407 Win=16

```
⊞ Frame 21 (62 bytes on wire, 62 bytes captured)
⊟ Ethernet II, Src: WesternD_d7:80:c2 (00:00:c0:d7:80:c2), Dst: 3Com_a4:e4:8c (00:04:76:a4:e4:8c)
  ⊞ Destination: 3Com_a4:e4:8c (00:04:76:a4:e4:8c)
  ⊞ Source: WesternD_d7:80:c2 (00:00:c0:d7:80:c2)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 147.175.98.238 (147.175.98.238), Dst: 209.11.45.139 (209.11.45.139)
⊞ Transmission Control Protocol, Src Port: crrprotocol (1096), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 04 76 a4 e4 8c 00 00  c0 d7 80 c2 08 00 45 00   ..v..... ......E.
0010  00 30 07 1d 40 00 80 06  fe 76 93 af 62 ee d1 0b   .0..@... .v..b...
0020  2d 8b 04 48 00 50 71 54  67 27 00 00 00 00 70 02   -..H.PqT g'....p.
0030  40 00 70 d7 00 00 02 04  05 b4 01 01 04 02        @.p..... ......
```

Type (eth.type), 2 bytes | Packets: 162 Displayed: 162 Marked: 0 | Profile: Default

start | Total Commander 6.0... | Microsoft PowerPoint ... | eth4.pcap - Wireshark | untitled - Paint | 11:18 PM

eth7.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
60	15.473200	30098000.0004757fb302	30098000.ffffffffffff	IPX SAP	General Response
61	15.532689	3Com_a4:e4:8c	Broadcast	ARP	who has 147.175.98.200? Tell 147.175.98.1
62	15.639916	00000000.5254ab148b15	00000000.ffffffffffff	IPX SAP	General Query
63	15.813403	3Com_13:97:df	NETBIOS-	SMB_NETL	Query for PDC from ENIGMA
64	15.830688	147.175.98.232	147.175.98.255	NBNS	Name query NB CA&0<1c>
65	16.581787	147.175.98.232	147.175.98.255	NBNS	Name query NB CA&0<1c>
66	17.332795	147.175.98.232	147.175.98.255	NBNS	Name query NB CA&0<1c>
67	17.754417	Standard_05:51:2b	Broadcast	ARP	who has 147.175.98.3? Tell 147.175.98.30
68	19.056341	Standard_05:51:2b	Broadcast	ARP	who has 147.175.98.78? Tell 147.175.98.30
69	20.466129	3Com_a4:e4:8c	Broadcast	ARP	who has 147.175.98.5? Tell 147.175.98.1
70	21.650566	3Com_c6:b8:1f	Broadcast	ARP	who has 147.175.98.40? Tell 147.175.98.224
71	22.205575	3Com_a4:e4:8c	Broadcast	ARP	who has 147.175.98.110? Tell 147.175.98.1
72	22.989780	3Com_a4:e4:8c	Broadcast	ARP	who has 147.175.98.142? Tell 147.175.98.1

```
⊞ Frame 63 (207 bytes on wire, 207 bytes captured)
⊟ IEEE 802.3 Ethernet
  ⊞ Destination: NETBIOS- (03:00:00:00:00:01)
  ⊞ Source: 3Com_13:97:df (00:04:76:13:97:df)
    Length: 193
⊟ Logical-Link Control
    DSAP: NetBIOS (0xf0)
    IG Bit: Individual
    SSAP: NetBIOS (0xf0)
    CR Bit: Command
  ⊞ Control field: U, func=UI (0x03)
⊞ NetBIOS
```

```
0000  03 00 00 00 00 01 00 04  76 13 97 df 00 c1 f0 f0   ........ v.......
0010  03 2c 00 ff ef 08 00 00  00 00 00 00 00 43 41 26   ........ .....CA&
0020  4f 20 20 20 20 20 20 20  20 20 20 20 1c 45 4e 49   O            .ENI
0030  47 4d 41 20 20 20 20 20  20 20 20 20 00 ff 53 4d   GMA          ..SM
0040  42 25 00 00 00 00 18 04  00 00 00 00 00 00 00 00   B%...... ........
0050  00 00 00 00 00 00 00 ff  fe 00 00 00 00 11 00 00   ........ ........
0060  36 00 02 00 00 00 00 00  02 00 00 00 00 00 00 00   6....... ........
0070  00 00 5c 00 36 00 5c 00  03 00 01 00 00 00 02 00   ..\.6.\. ........
0080  4d 00 5c 4d 41 49 4c 53  4c 4f 54 5c 4e 45 54 5c   M.\MAILS LOT\NET\
0090  4e 45 54 4c 4f 47 4f 4e  00 07 00 45 4e 49 47 4d   NETLOGON ...ENIGM
00a0  41 00 5c 4d 41 49 4c 53  4c 4f 54 5c 4e 45 54 5c   A.\MAILS LOT\NET\
```

DSAP - 7 Most Significant Bits only (0x..0x0), 1 b... Packets: 377 Displayed: 377 Marked: 0 Profile: Default

start | Total Commander 6.0... | Microsoft PowerPoint ... | eth7.pcap - Wireshark | untitled - Paint | 11:24 PM

No.	Time	Source	Destination	Protocol	S port	D port	Length	Info
35	2.503287	d0:67:e5:a4:5d:aa	CDP/VTP/DTP/PAgP/UDLD	CDP			112	Device ID: CN0F14WF2829
36	2.525909	147.175.145.174	255.255.255.255	UDP	17500	17500	186	Source port: 17500 Dest
37	2.528711	147.175.145.174	255.255.255.255	UDP	17500	17500	186	Source port: 17500 Dest
38	2.528844	147.175.145.174	255.255.255.255	UDP	17500	17500	186	Source port: 17500 Dest
39	2.528995	147.175.145.174	147.175.145.255	UDP	17500	17500	186	Source port: 17500 Dest
40	2.529103	147.175.145.174	255.255.255.255	UDP	17500	17500	186	Source port: 17500 Dest
41	2.598268	3Com_a4:e4:8c	Broadcast	ARP			60	who has 147.175.98.207?
42	2.611220	3Com_a4:e4:8c	Broadcast	ARP			60	who has 147.175.98.27?
43	2.613161	fe80::1d63:c087:690d:	ff02::c	SSDP	56226	ssdp	208	M-SEARCH * HTTP/1.1
44	2.621696	147.175.145.197	224.0.0.2	IGMP			60	v2 Leave Group 239.255.
45	2.622252	192.168.0.254	239.255.67.250	IGMP			60	v2 Membership Query /
46	2.623323	147.175.145.73	239.255.67.250	IGMP			60	v2 Membership Report /
47	2.767357	Cisco_e5:ae:11	Spanning-tree-(for-br	STP			60	Conf. TC + Root = 32769,
48	2.787335	fe80::403:5c43:2646:1	ff02::1:2	DHCPv6	dhcpv6	dhcpv6	148	Solicit
49	2.814400	Intel_ad:a2:a7	Broadcast	ARP			60	who has 147.175.145.136?

```
⊞ Frame 35 (112 bytes on wire, 112 bytes captured)
⊞ IEEE 802.3 Ethernet
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊞ Control field: U, func=UI (0x03)
    Organization Code: Cisco (0x00000c)
    PID: CDP (0x2000)
⊞ Cisco Discovery Protocol
```

```
0000  01 00 0c cc cc cc d0 67  e5 a4 5d aa 00 62 00 48   .......g ..]..b.H
0010  03 00 00 0c 20 00 02 b4  ac 5f 00 01 00 10 43 4e   .... ..  ._....CN
0020  30 46 31 34 57 46 32 38  32 39 38 32 39 45 30 30   0F14WF28 29829E00
0030  39 33 41 30 37 00 06 00  0b 50 43 54 37 30 32 34   93A07... .PCT7024
0040  00 03 00 0c 47 69 31 2f  30 2f 32 33 00 04 00 08   ....Gi1/ 0/23....
0050  00 00 00 01 00 05 00 0b  34 2e 32 2e 30 2e 34 00   ........ 4.2.0.4.
0060  02 00 11 00 00 00 01 01  01 cc 00 04 93 af 90 09   ........ ........
```

eth2.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	30098000.0004[illegible]	30098000.ffffffffffff	IPX RIP	Response
2	0.000016	30098000.0004[illegible]	30098000.ffffffffffff	IPX RIP	Response

```
Frame 1 (446 bytes on wire, 446 bytes captured)
IEEE 802.3 Ethernet Raw
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: 3Com_a4:e4:8c (00:04:76:a4:e4:8c)
  Length: 432
Internetwork Packet exchange
  Checksum: 0xffff
  Length: 432 bytes
  Transport Control: 0 hops
  Packet Type: RIP (0x01)
  Destination Network: 30098000 (0x30098000)
  Destination Node: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination Socket: RIP (0x0453)
  Source Network: 30098000 (0x30098000)
  Source Node: 3Com_a4:e4:8c (00:04:76:a4:e4:8c)
  Source Socket: RIP (0x0453)
IPX Routing Information Protocol
```

```
0000  ff ff ff ff ff ff 00 04  76 a4 e4 8c 01 b0 ff ff   ........ v.......
0010  01 b0 00 01 30 09 80 00  ff ff ff ff ff ff 04 53   ....0... .......S
0020  30 09 80 00 00 04 76 a4  e4 8c 04 53 00 02 00 00   0.....v. ...S....
0030  00 80 00 03 00 04 00 00  00 01 00 02 00 02 00 00   ........ ........
0040  00 82 00 04 00 05 00 00  00 02 00 03 00 04 00 00   ........ ........
0050  00 03 00 03 00 04 e0 12  60 00 00 02 00 02 00 00   ........ `.......
0060  00 85 00 04 00 05 00 00  00 05 00 03 00 04 0d 14   ........ ........
0070  71 75 00 03 00 04 00 00  00 86 00 04 00 05 e0 12   qu...... ........
0080  61 60 00 02 00 02 00 00  00 87 00 04 00 05 00 00   a`...... ........
0090  00 88 00 04 00 05 00 11  10 62 00 02 00 03 00 00   ........ .b......
00a0  00 09 00 06 00 06 00 13  00 09 00 04 00 05 20 12   ........ ...... .
```

Checksum (ipx.checksum), 2 bytes | Packets: 2 Displayed: 2 Marked: 0 | Profile: Default

start | Total Commander 6.0... | Microsoft PowerPoint ... | eth2.pcap - Wireshark | untitled - Paint | 11:27 PM

Zhrnutie prednášky

- Dokončenie IP Subnetting/NAPT
- Linková vrstva:
  - Formát Ethernet rámca
  - Analýza rámcov

STU FIIT

Čo nás čaká na budúcej prednáške

– Fyzická vrstva

STU
FIIT