IPv6 – Autokonfigurace a falešné směrovače

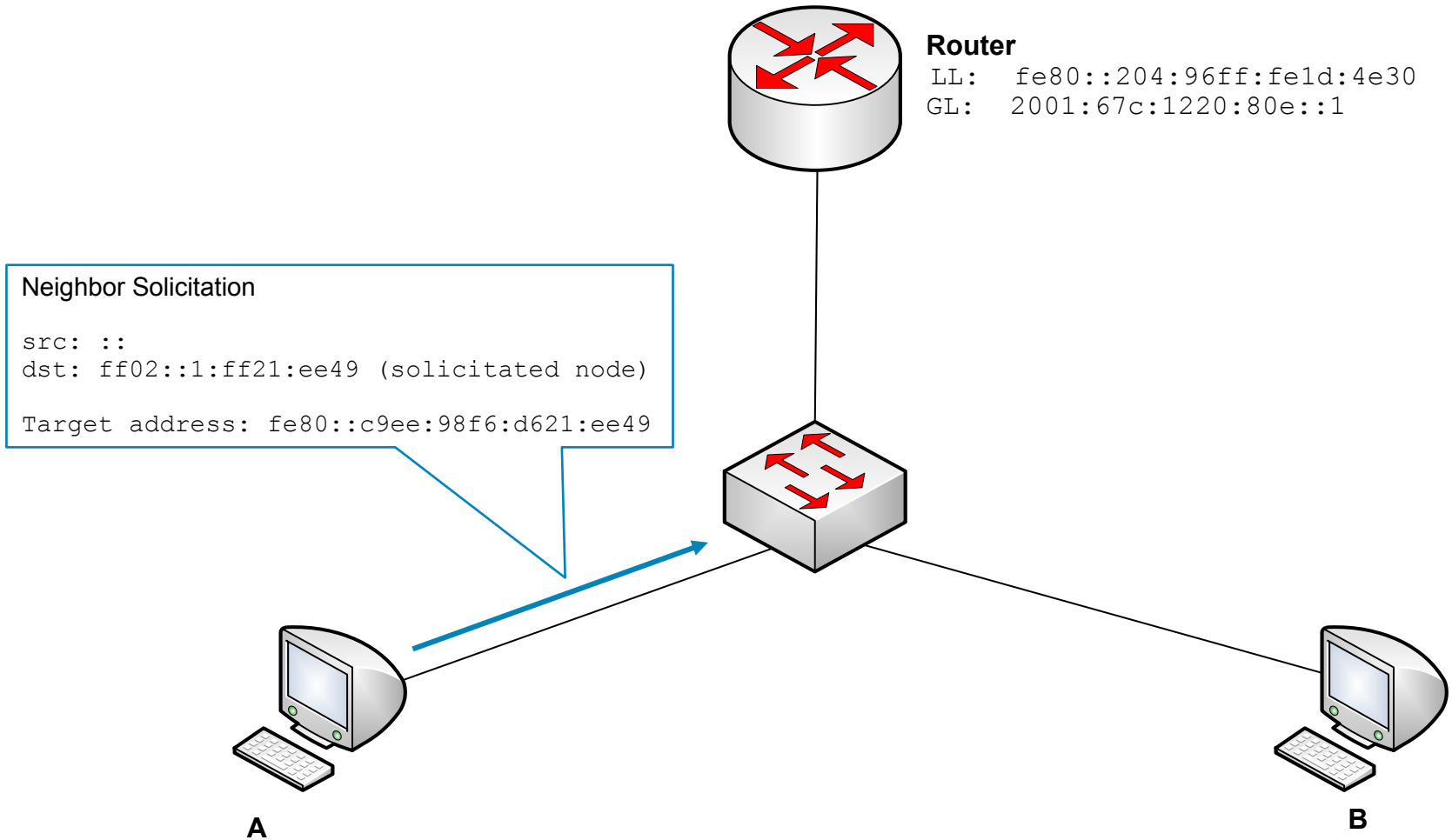
Matěj Grégr
Vysoké učení technické v Brně, Fakulta informačních technologií
igregr@fit.vutbr.cz

UPOL 2013

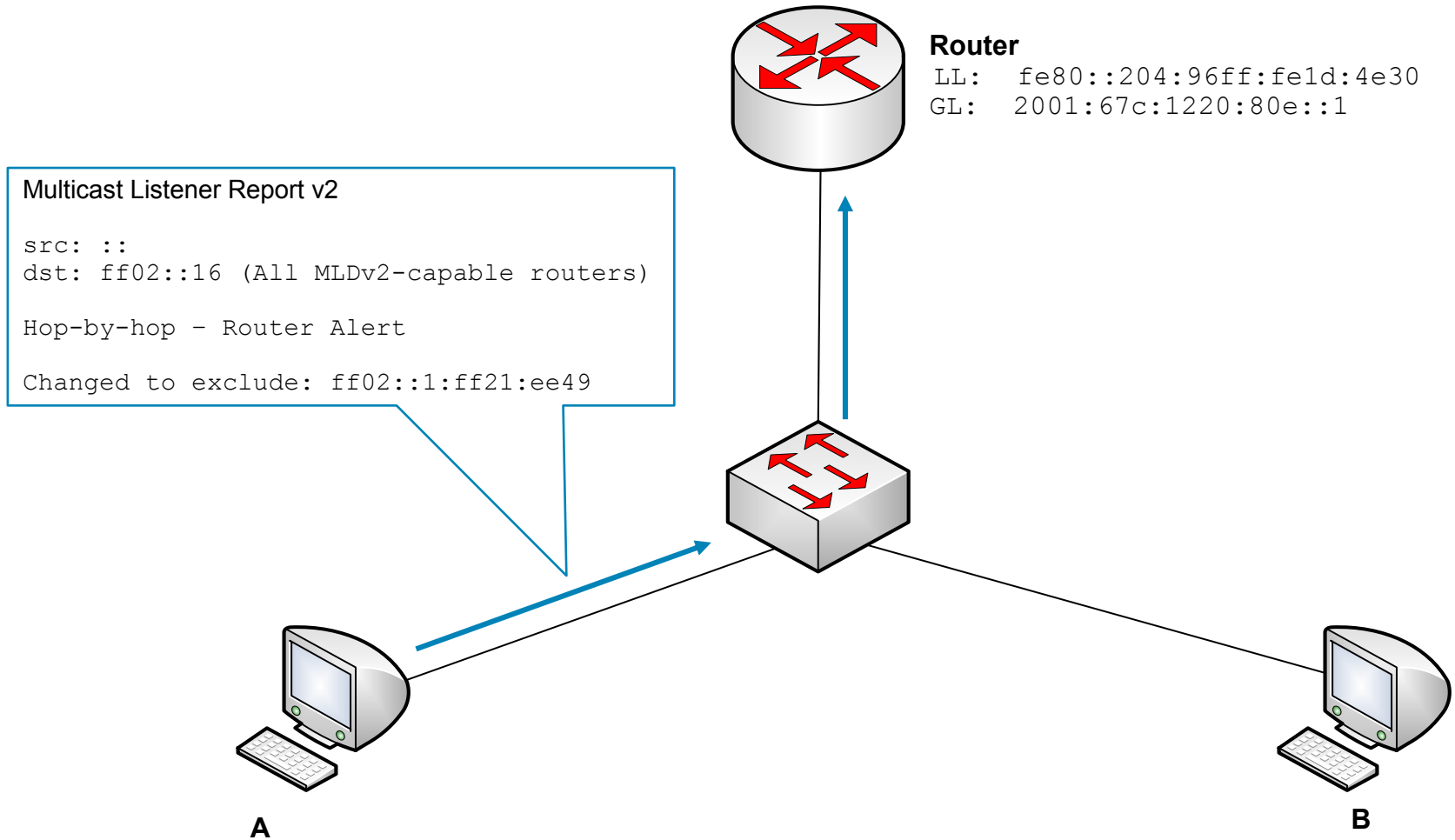
Konfigurace adres

- Snaha o plug-and-play konfiguraci
- 1984: RARP
- 1985: BOOTP
- 1993: DHCP + DHCP Options
- 1996: IPv6 Stateless Address Autoconfiguration
- 2003: DHCPv6
- 2010: Router Advertisement Options for DNS Configuration

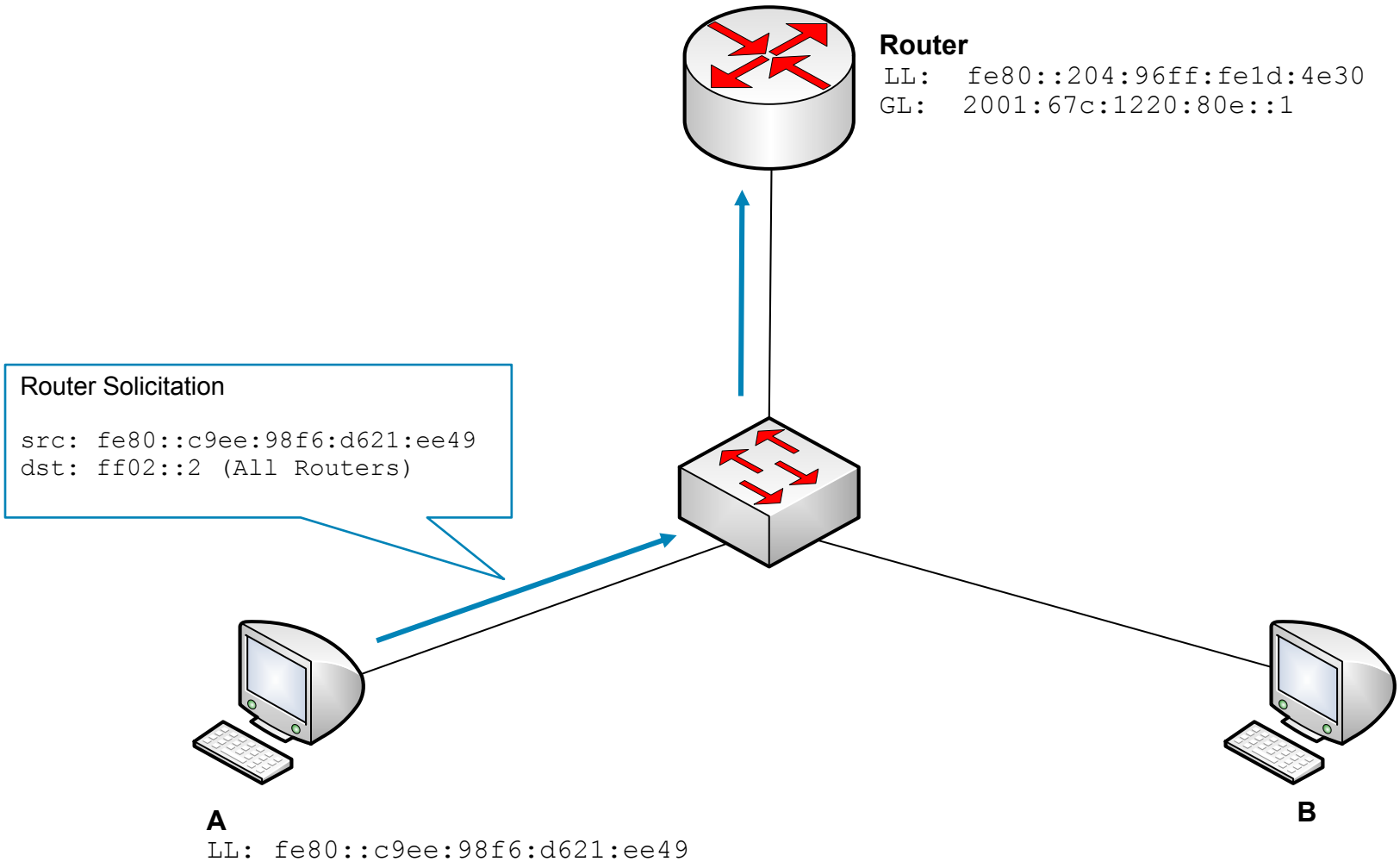
Link local adresa



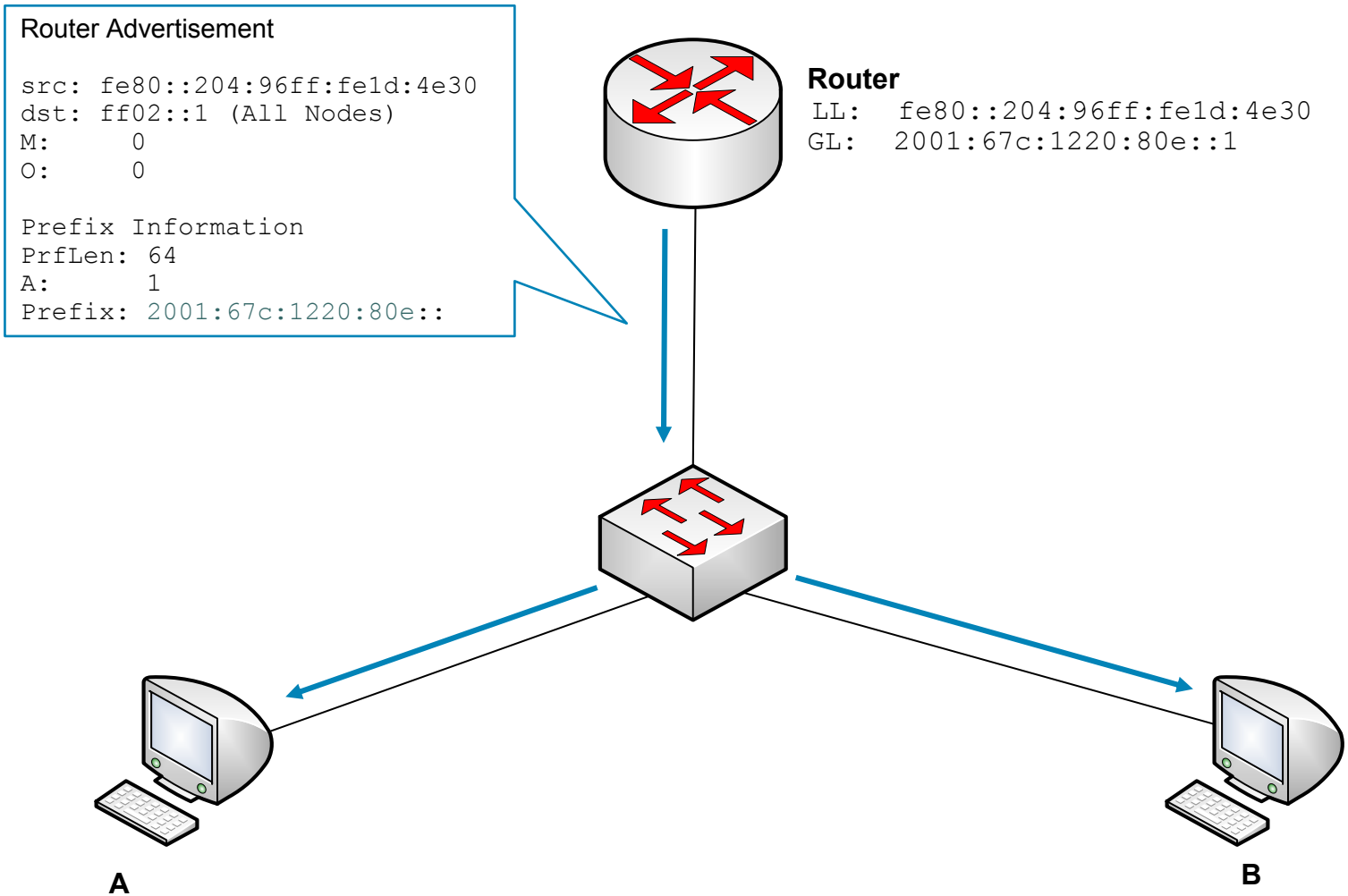
MLD Report


Router
LL: fe80::204:96ff:fe1d:4e30
GL: 2001:67c:1220:80e::1
Multicast Listener Report v2
src: ::
dst: ff02::16 (All MLDv2-capable routers)
Hop-by-hop – Router Alert
Changed to exclude: ff02::1:ff21:ee49
A
LL: fe80::c9ee:98f6:d621:ee49 [TENT]
B

Globální adresa



Globální adresa



Směrování

```
C:\Users\igregr\route -6 print
IPv6 Route Table
===========================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    266 ::/0                     fe80::204:96ff:fe1d:4e30
  1    306 ::1/128                  On-link
 10     18 2001:67c:1220:80e::/64   On-link
```

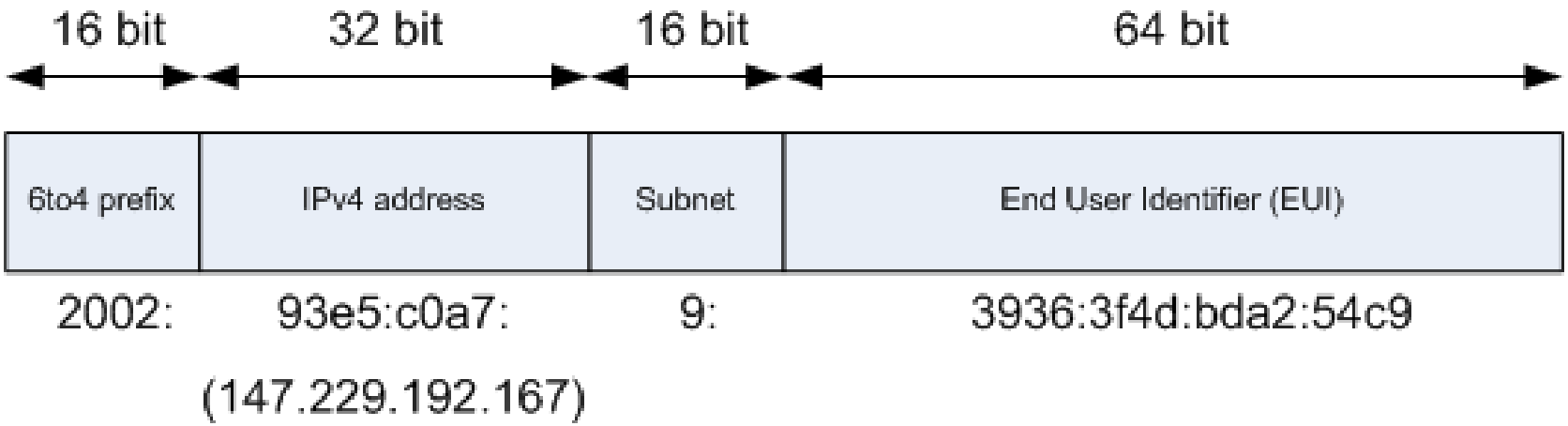
IPv6 SLAAC – poznámky

- Samotný SLAAC nestačí – chybí DNS
  - IPv4 DNS
  - DHCPv6
  - RDNSS

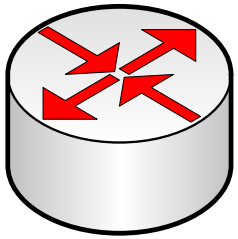
- Problematičtí klienti:
  - Android – chybí podpora DHCPv6, RDNSS
  - Windows Vista, 7, 8, Phone 8 – chybí podpora RDNSS
  - Windows XP – chybí podpora DHCPv6, RDNSS
  - Windows Phone 7.5 – chybí podpora IPv6
  - MAC OS < 10.7 – chybí DHCPv6

6to4

- Definováno v RFC 3056, RFC 3058
- Potřebuje veřejnou IPv4 adresu
- Rezervován prefix `2002::/16`

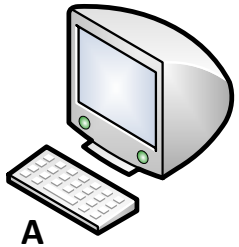


6to4

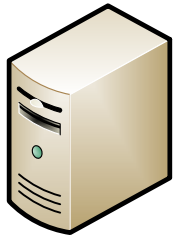


6to4 relay (6to4.nic.cz)
IPv4: 192.88.99.1
IPv6: 2001:1488:800:400::151

IPv4
src: 147.229.192.167
dst: 192.88.99.1
IPv6
src: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
dst: 2a00:1450:400b:c02::93
TCP
HTTP

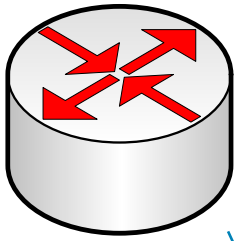


A
IPv4: 147.229.192.167
6to4: 2002:93e5:c0a7::3936:3f4d:bda2:53c9

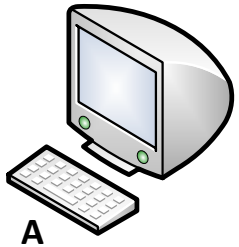


ipv6.google.com
IPv6: 2a00:1450:400b:c02::93

6to4

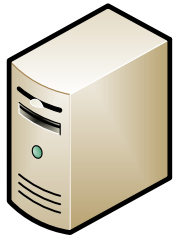


6to4 relay (6to4.nic.cz)
IPv4: 192.88.99.1
IPv6: 2001:1488:800:400::151



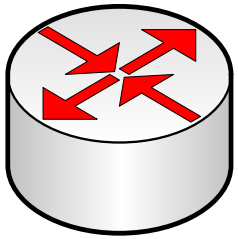
IPv6
src: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
dst: 2a00:1450:400b:c02::93
TCP
HTTP

A
IPv4: 147.229.192.167
6to4: 2002:93e5:c0a7::3936:3f4d:bda2:53c9

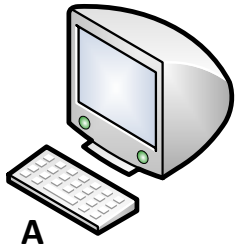


ipv6.google.com
IPv6: 2a00:1450:400b:c02::93

6to4

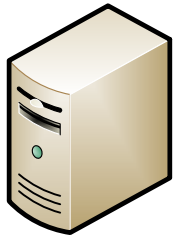


6to4 relay (6to4.nic.cz)
IPv4: 192.88.99.1
IPv6: 2001:1488:800:400::151



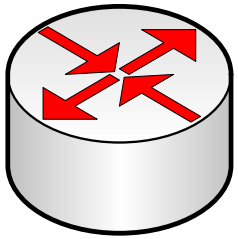
IPv6
src: 2a00:1450:400b:c02::93
dst: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
TCP
HTTP

A
IPv4: 147.229.192.167
6to4: 2002:93e5:c0a7::3936:3f4d:bda2:53c9



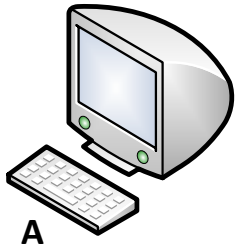
ipv6.google.com
IPv6: 2a00:1450:400b:c02::93

6to4

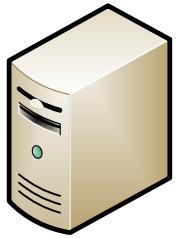


6to4 relay (6to4.nic.cz)
IPv4: 192.88.99.1
IPv6: 2001:1488:800:400::151

IPv4
src: 192.88.99.1
dst: 147.229.192.167
IPv6
src: 2a00:1450:400b:c02::93
dst: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
TCP
HTTP



A
IPv4: 147.229.192.167
6to4: 2002:93e5:c0a7::3936:3f4d:bda2:53c9

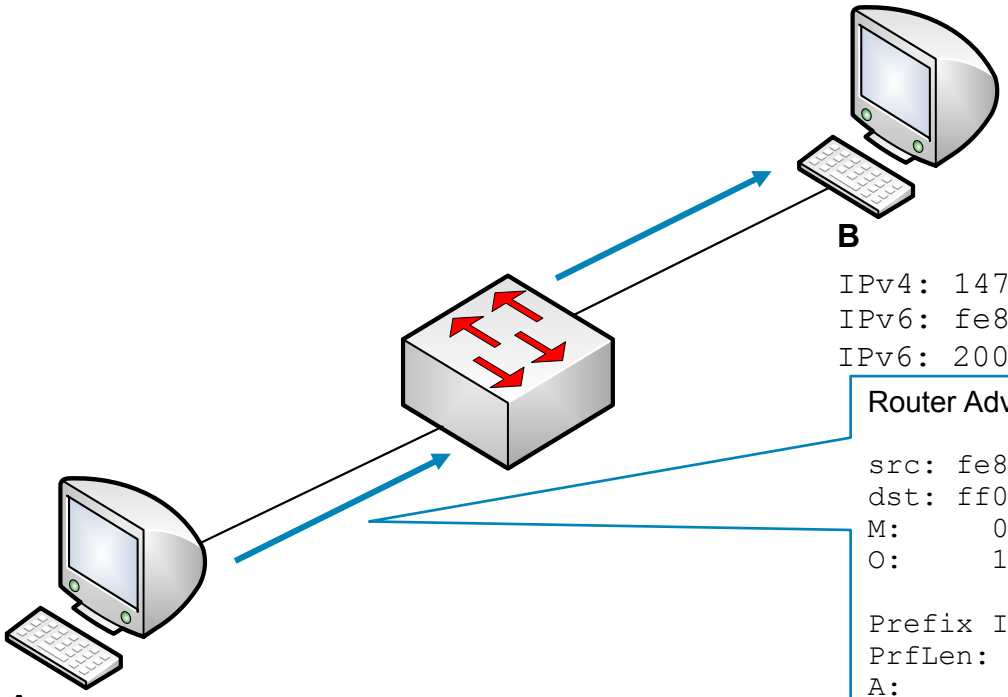


ipv6.google.com
IPv6: 2a00:1450:400b:c02::93

Windows a Internet Connection Sharing

- Sdílení Ethernet – WiFi
- Veřejná IPv4 adresa
  - Možnost ustanovení 6to4 tunelu
- 6to4 + ICS
  - OS se rád podělí o svou IPv6 konektivitu
  - Rozhraní, na kterém je ICS konfigurováno nemusí být aktivní

6to4 směrovač v IPv4 síti



B

```
IPv4: 147.229.192.150
IPv6: fe80::6154:dd83:f558:23ce
IPv6: 2002:93e5:c0a7::2cb1:6d33:57bf:cace
```

Router Advertisement

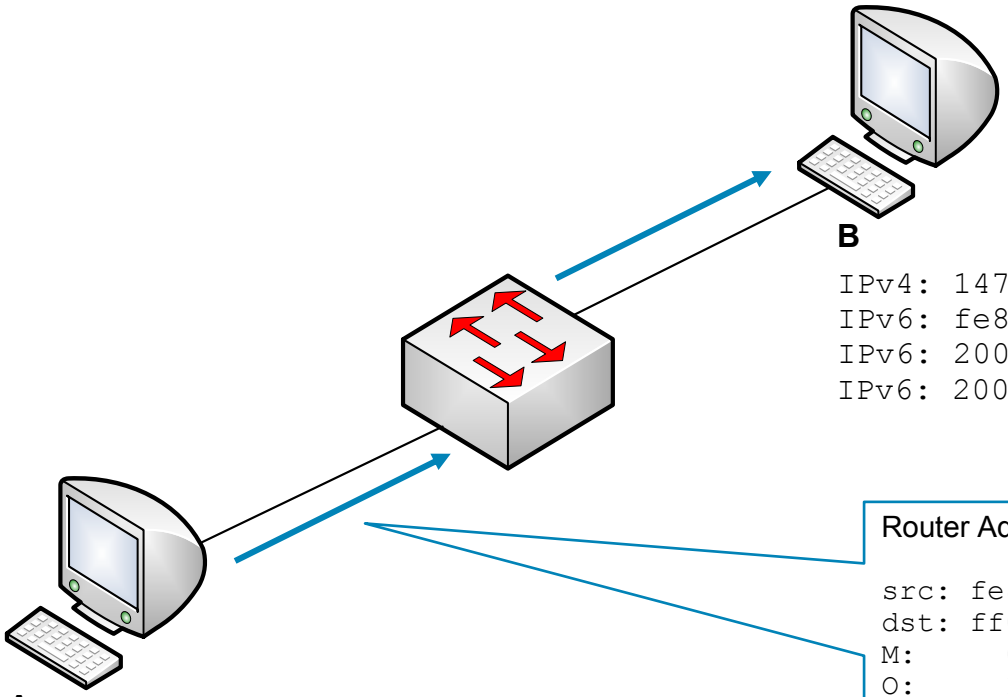
```
src: fe80::c9ee:98f6:d621:ee49
dst: ff02::1 (All Nodes)
M:     0
O:     1

Prefix Information
PrfLen: 64
A:      1
Prefix: 2002:93e5:c0a7::
```

A

```
IPv4: 147.229.192.167
IPv6: fe80::c9ee:98f6:d621:ee49
IPv6: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
```

6to4 směrovač v IPv6 síti



B

```
IPv4: 147.229.192.150
IPv6: fe80::6154:dd83:f558:23ce
IPv6: 2001:67c:1220:80e:2cb1:6d33:57bf:cace
IPv6: 2002:93e5:c0a7::2cb1:6d33:57bf:cace
```

A

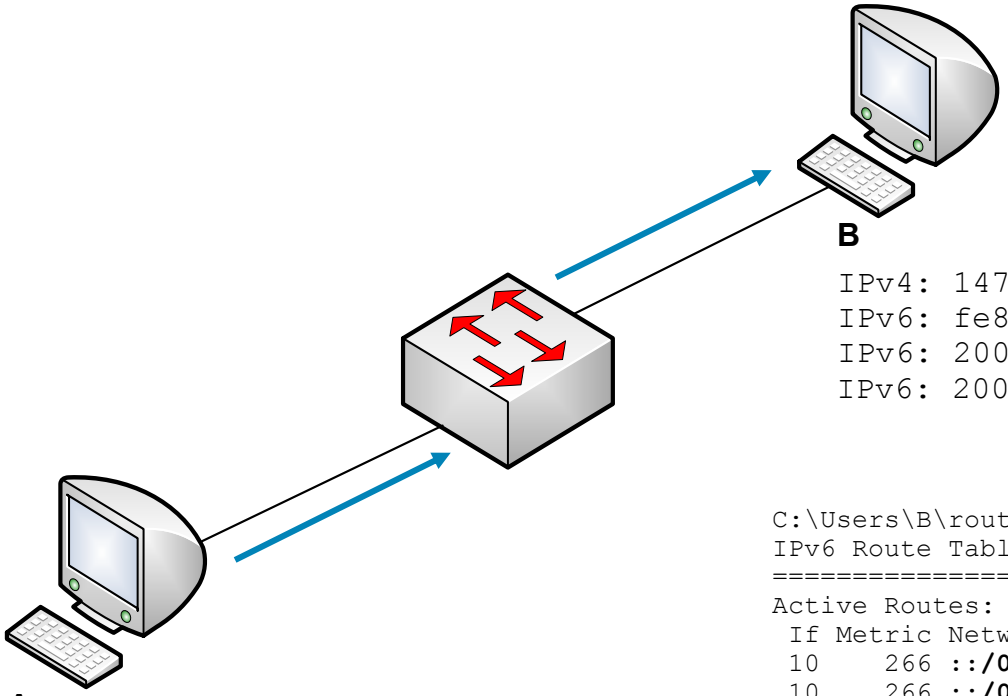
```
IPv4: 147.229.192.167
IPv6: fe80::c9ee:98f6:d621:ee49
IPv6: 2001:67c:1220:80e:d4a3:cd1b:bac:942b
IPv6: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
```

Router Advertisement

```
src: fe80::c9ee:98f6:d621:ee49
dst: ff02::1 (All Nodes)
M:     0
O:     1

Prefix Information
PrfLen: 64
A:      1
Prefix: 2002:93e5:c0a7::
```

6to4 směrovač v IPv6 síti



B

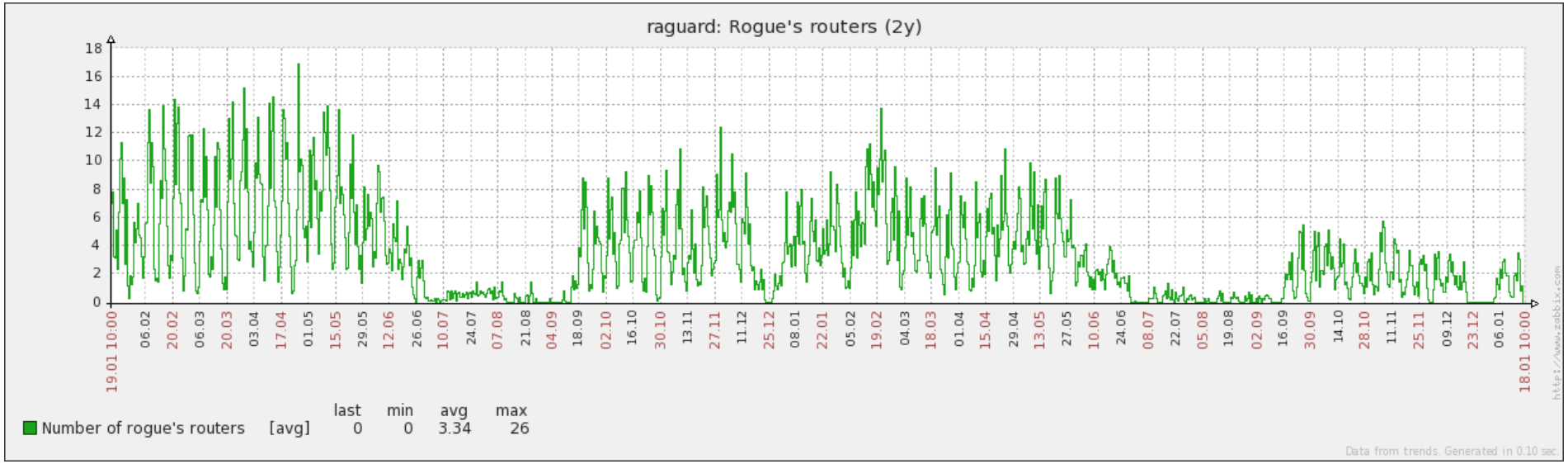
```
IPv4: 147.229.192.150
IPv6: fe80::6154:dd83:f558:23ce
IPv6: 2001:67c:1220:80e:2cb1:6d33:57bf:cace
IPv6: 2002:93e5:c0a7::2cb1:6d33:57bf:cace
```

A

```
IPv4: 147.229.192.167
IPv6: fe80::c9ee:98f6:d621:ee49
IPv6: 2001:67c:1220:80e:d4a3:cd1b:bac:942b
IPv6: 2002:93e5:c0a7::3936:3f4d:bda2:53c9
```

```
C:\Users\B\route -6 print
IPv6 Route Table
===========================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    266 ::/0                     fe80::204:96ff:fe1d:4e30
 10    266 ::/0                     fe80::c9ee:98f6:d621:ee49
  1    306 ::1/128                  On-link
 10     18 2001:67c:1220:80e::/64   On-link
```

Počet falešných směrovačů



Windows 7 – update

- Windows 7 – Update 2750841
- Před přiřazením adres 6to4 – kontrola zda se lze připojit na relay
- 6to4 + ICS – disabled by default
- Změna preferování IPv6/IPv4
  - Kontrola pomocí Network Connectivity Status Indicator
- Omezení RA flood – max. 100 záznamů ve směrovací tabulce

Obrana?

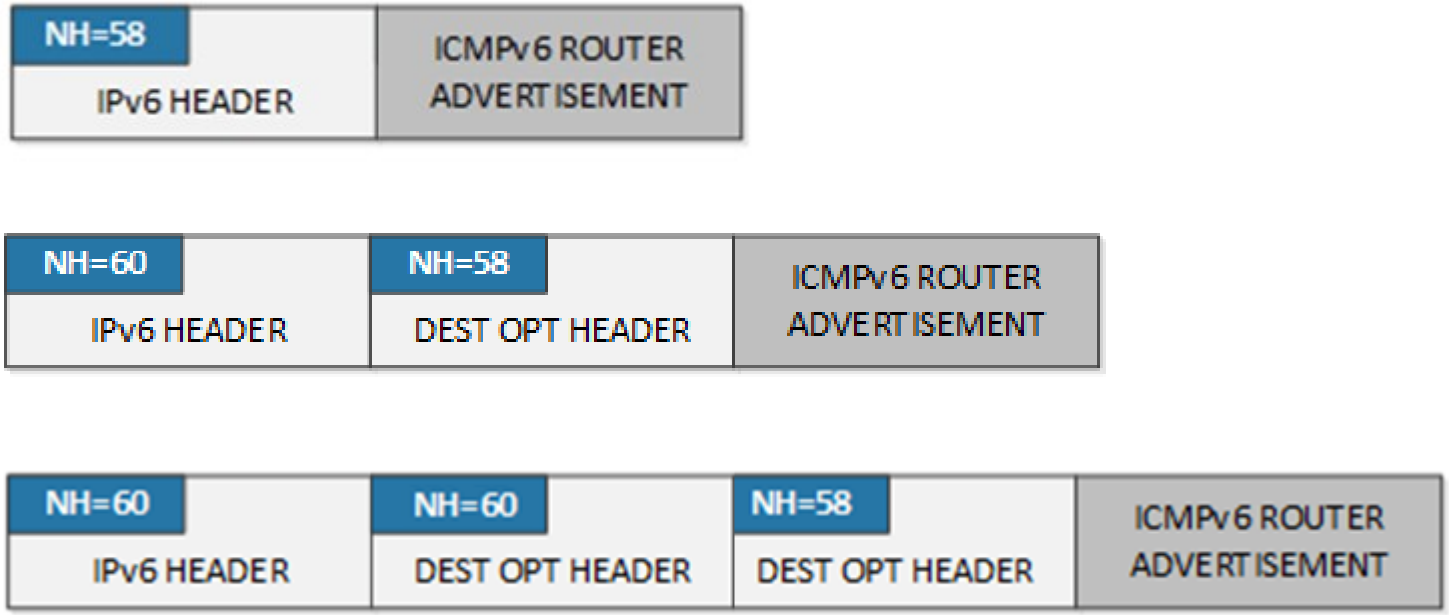
- SeND (RFC 3971, March 2005)
  - Podepisuje NS/NA zprávy
  - Potřebuje PKI
    - Jak nastavit certifikát klientovi?
  - Vlastní typ adresy, nekompatibilní s:
    - Manuální IPv6, EUI-64, Privacy extension
- RA-Guard, PACL (RFC 6105, February 2011), DHCPv6 snooping
  - Zahazuje falešné zprávy RA (RA snooping)
- SAVI (draft-ietf-savi-*)
  - Komplexní řešení – DHCPv6, RA, kontrola podvržení adresy
  - Podobné jako ND Inspection (Cisco/HP)
- Monitorovací nástroj – odregistrace
- Vysoká priorita u RA zpráv

Monitorovací software

- Ramond
  - http://ramond.sourceforge.net/
  - http://www.root.cz/clanky/ramond-past-na-falesne-ipv6-smerovace
- Ndwatch
  - http://www.fit.vutbr.cz/~lampa/ipv6/
- Rafixd
  - http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/
  - Linux port: https://github.com/strattg/rafixd
- Ndpmon
  - http://ndpmon.sourceforge.net/
- Vlastní řešení např. pomocí Scapy
  - http://www.secdev.org/projects/scapy/

Bypassing RA guard

- Rozšířené hlavičky!

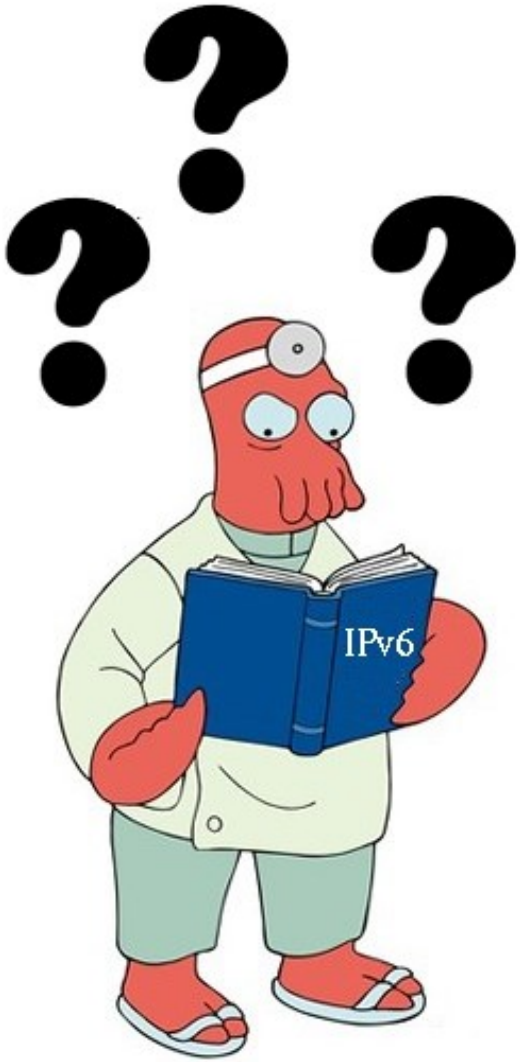


- http://6lab.cz/article/rogue-router-advertisement-attack/

Shrnutí

- Rozdílný způsob adresace
- Monitorování IPv6 provozu je nutnost
- Problém podpory u zařízeních – RDNSS, DHCPv6
- Chybějící implementace RA Guard, ND snooping

- http://6lab.cz


IPv6