

**2THEPOINT**  
Intensivkurser för IT-branschen

## IPv6 – paketnivå och nätanalys

**2THEPOINT**  
Intensivkurser för IT-branschen



*Snabbt, enkelt  
och flexibelt*

[Så jobbar vi](#) [Våra kurser](#) [Välkommen på kurs](#) [Om oss](#) [Nyheter](#)

### Välkommen

Vi utbildar inom nätverk och datakommunikation, och ger utbildning du direkt har nytta av. Snabbt, enkelt och flexibelt!

1. Välj den utbildning som intresserar dig. 2. Gör vårt test 3. Boka – gå kursen!





# Wireshark

3

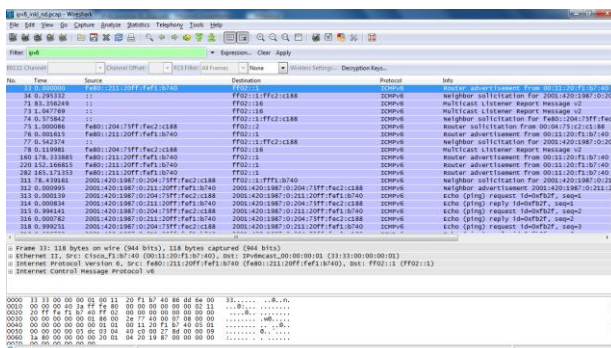
Maj 2010

COPYRIGHT 2 the point och Håkan Lindberg



# Nätverksanalyator

- Spelar in de paket som når ditt LAN-kort
- Wireshark är gratis och mycket kompetent på IPv6



4

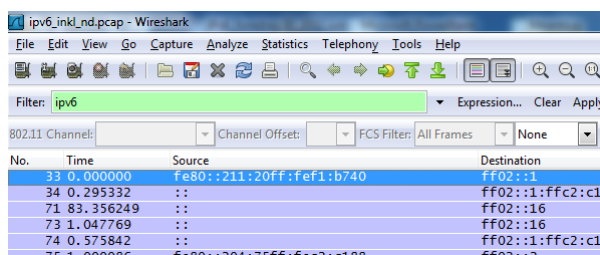
Sep 2010

COPYRIGHT 2 the point



## Filtrera ut IPv6

- Du har det förmodligen redan i nätet
- Windows Vista och 7 är "IPv6 aggresiva"



| No. | Time      | Source                   | Destination     |
|-----|-----------|--------------------------|-----------------|
| 33  | 0.000000  | fe80::211:20ff:fe11:b740 | ff02::1         |
| 34  | 0.295332  | ::                       | ff02::1:ffc2:c1 |
| 71  | 83.356249 | ::                       | ff02::16        |
| 73  | 1.047769  | ::                       | ff02::16        |
| 74  | 0.575842  | ::                       | ff02::1:ffc2:c1 |
| 75  | 1.000086  | fe80::204:75ff:fe21:c188 | ff02::1         |

5 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## Vad kommer vi se?

- Broadcast var ganska lätt. Multicast är lite krångligare
- Långa adresser
- IPv6 headern –den är enklare än i IPv4

```

* Frame 33: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
  Ethernet II, Src: Cisco_f1:b7:40 (00:11:20:f1:b7:40), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
    Destination: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
    Source: Cisco_f1:b7:40 (00:11:20:f1:b7:40)
    Type: IPv6 (0x86dd)
  Internet Protocol Version 6, Src: fe80::211:20ff:fe11:b740 (fe80::211:20ff:fe11:b740), dst: ff02::1 (ff02::1)
    0110 .... = Version: 6
    .... 1110 0000 .... = Traffic class: 0x000000e0
    .... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 64
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source: fe80::211:20ff:fe11:b740 (fe80::211:20ff:fe11:b740)
    [Source SA MAC: Cisco_f1:b7:40 (00:11:20:f1:b7:40)]
    Destination: ff02::1 (ff02::1)
  Internet Control Message Protocol v6
  
```

6 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## Ett inspelat IPv6 paket

```

Frame 33: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Epoch Time: 1174484957.727202000 seconds
[Time delta from previous captured frame: 2.891573000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 87.253234000 seconds]
Frame Number: 33
Frame Length: 118 bytes (944 bits)
Capture Length: 118 bytes (944 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ipv6:icmpv6]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp | | icmpv6]
Ethernet II, Src: Cisco_f1:b7:40 (00:11:20:f1:b7:40), Dst: IPv6multicast_00:00:00:01 (33:33:00:00:00:01)
Destination: IPv6multicast_00:00:00:01 (33:33:00:00:00:01)
Address: IPv6multicast_00:00:00:01 (33:33:00:00:00:01)
....1.... = IG bit: Group address (multicast/broadcast)
....1.... = LG bit: Locally administered address (this is NOT the factory default)
Source: Cisco_f1:b7:40 (00:11:20:f1:b7:40)
Address: Cisco_f1:b7:40 (00:11:20:f1:b7:40)
....0.... = IG bit: Individual address (unicast)
....0.... = LG bit: Globally unique address (factory default)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::211:20ff:fe1:b740 (fe80::211:20ff:fe1:b740), Dst: ff02::1 (ff02::1)
0110... = Version: 6
[0110... = This field makes the filter "ip version == 6" possible: 6]
....11100000... = Traffic class: 0x00000000
....111000... = Differentiated Services Field: Class Selector 7 (0x00000038)
....0... = ECN-Capable Transport (ECT): Not set
....0... = ECN-CE: Not set
....00000000000000000000 = Flowlabel: 0x00000000
Payload length: 64
Next header: ICMPv6 (0x3a)
Hop limit: 255
Source: fe80::211:20ff:fe1:b740 (fe80::211:20ff:fe1:b740)
[Source SA MAC: Cisco_f1:b7:40 (00:11:20:f1:b7:40)]
Destination: ff02::1 (ff02::1)

Internet Control Message Protocol v6
Type: 134 (Router advertisement)
Code: 0
Checksum: 0x2e77 [correct]
Cur hop limit: 64
Flags: 0x00
0... = Not managed
0... = Not other
0... = Not Home Agent
0... = Router preference: Medium
...0... = Not Proxied
Router lifetime: 1800
Reachable time: 0
Retrans timer: 0
ICMPv6 Option (Source link-layer address)
Type: Source link-layer address (1)
Length: 8
Link-layer address: 00:11:20:f1:b7:40
ICMPv6 Option (MTU)
Type: MTU (5)
Length: 8
MTU: 1500
ICMPv6 Option (Prefix information)
Type: Prefix information (3)
Length: 32
Prefix Length: 64
Flags: 0x00
1... = On-link flag(L): Set
1... = Autonomous address-configuration flag(A): Set
000000 = Reserved: 0
Valid lifetime: 2592000
Preferred lifetime: 604800
Reserved
Prefix: 2001:420:1987::

```

7

Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## Adressering

Ethernet II

Src: Cisco\_f1:b7:40 (**00:11:20:f1:b7:40**),

Dst: IPv6multicast (**33:33:00:00:00:01**)

Internet Protocol Version 6,

Src: fe80::211:20ff:fe1:b740 (**fe80::211:20ff:fe1:b740**),

Dst: **ff02::1 (ff02::1)**

Internet Control Message Protocol v6

Type: 134 (Router advertisement)

8

Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

**2THEPOINT**  
Intensivkurser för IT-branschen

# Multicast

Ethernet II

Src: Cisco\_f1:b7:40 (00:11:20:f1:b7:40),

Dst: IPv6multicast (**33:33:00:00:00:01**)

Internet Protocol Version 6,

Src: fe80::211:20ff:fef1:b740 (fe80::211:20ff:fef1:b740),

Dst: **ff02::1 (ff02::1)**

Internet Control Message Protocol v6

Type: 134 (Router advertisement)

9

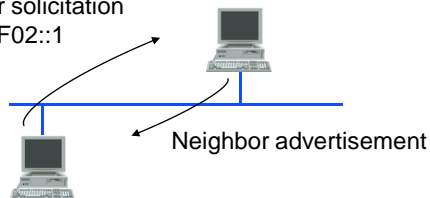
Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

# Multicast

Neighbor solicitation  
D-IP = FF02::1



10

Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## Multicast

- Broadcast är helt borta ut IPv6. Multicast med olika scope ersätter

|          |         |         |           |
|----------|---------|---------|-----------|
| 8 bitar  | 4 bitar | 4 bitar | 112 bitar |
| 11111111 | flags   | scope   | Group id  |

### scope:

|   |                          |
|---|--------------------------|
| 1 | node-local scope         |
| 2 | link-local scope         |
| 5 | site-local scope         |
| 8 | organization-local scope |
| E | global scope             |

11 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
 Intensivkurser för IT-branschen

## ICMPv6 är likt IPv4 med tillägg

| Typ | ICMP-meddelande               |
|-----|-------------------------------|
| 1   | Destination Unreachable       |
| 2   | <b>Packet Too Big</b>         |
| 3   | Time Exceeded                 |
| 4   | Parameter Problem             |
| 128 | Echo                          |
| 129 | Echo Reply                    |
| 133 | <b>Router Solicitation</b>    |
| 134 | <b>Router Advertisement</b>   |
| 135 | <b>Neighbor Solicitation</b>  |
| 136 | <b>Neighbor Advertisement</b> |
| 137 | <b>Redirect</b>               |

12

COPYRIGHT 2 the point

**2THEPOINT**  
 Intensivkurser för IT-branschen

**2THEPOINT**  
 Intensivkurser för IT-branschen

## IPv6 nivå

Internet Protocol Version 6

**Version:** 6  
**Traffic class:** 0x000000e0  
**Flowlabel:** 0x00000000  
**Payload length:** 64  
**Hop limit:** 255  
**Source:** fe80::211:20ff:fef1:b740  
**Destination:** ff02::1

I

Ganska likt IPv4 men nya namn.  
 Tagit bort fragmenteringsfunkt,  
 Ingen info om headerlängd.  
 Ingen checksumma.

| 6                   | Trafikklass | "Flow Label" |             |           |
|---------------------|-------------|--------------|-------------|-----------|
| Längd på nyttolast  |             |              | Next Header | Hop Limit |
| IP avsändare (S-IP) |             |              |             |           |
| IP mottagare (D-IP) |             |              |             |           |

13 Sep 2010

**2THEPOINT**  
 Intensivkurser för IT-branschen

## Router advertisement

Internet Control Message Protocol v6

**Type: 134 (Router advertisement)**

Code: 0

Checksum: 0x2e77 [correct]

Cur hop limit: 64 /från router till alla noder/

Flags: 0x00

0... .. = Not managed /Om 1 så ska DHCP anv/

.0... .. = Not other /1= hämta mer än adress via DHCP/

..0... .. = Not Home Agent

...0 0... = Router preference: Medium /fler kan finnas,  
 tre nivåer har definierats/

.... 0.. = Not Proxied

Router lifetime: 1800 /som default router/

Reachable time: 0 /tid i ms för ND unreachable/

Retrans timer: 0 /tid i ms för ND soliciation/

ICMPv6 Option (Source link-layer address)

Type: Source link-layer address (1)

Length: 8

Link-layer address: 00:11:20:f1:b7:40

ICMPv6 Option (MTU)

Type: MTU (5)

Length: 8

MTU: 1500

ICMPv6 Option (Prefix information)

Type: Prefix information (3)

Length: 32

Prefix Length: 64

Flags: 0xc0

1... .. = On-link flag(L): Set /Delar länknivå/

.1... .. = Autonomous address-configuration flag(A): Set /SLAAC/

..00 0000 = Reserved: 0

Valid lifetime: 2592000 /anv prefix hur länge? 30 dagar/

Preferred lifetime: 604800 /JfrDHCP, får anv längre, 7 dgr/

Reserved

Prefix: 2001:420:1987::

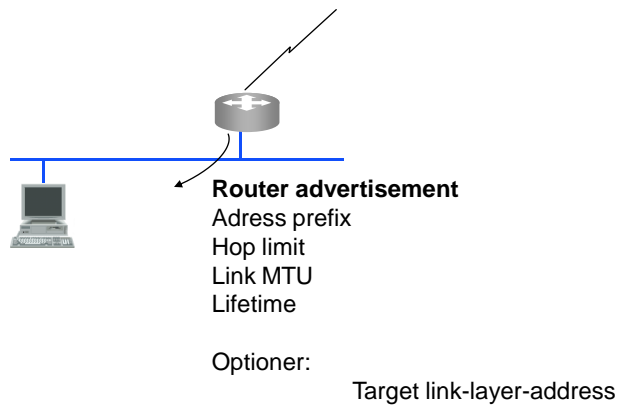
14 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
 Intensivkurser för IT-branschen

**2THEPOINT**  
 Intensivkurser för IT-branschen

## Router advertisement, RA

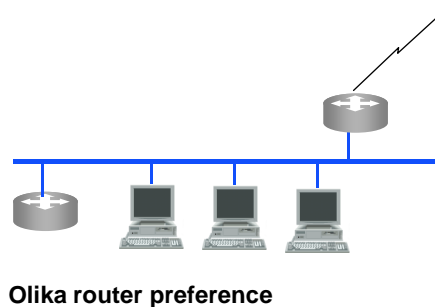


15 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## Ny möjlighet: bättre hantering av många routrar



16 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen



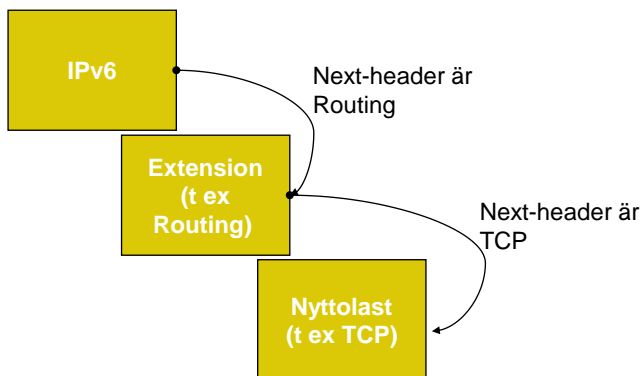
# Neighbor Discovery

- Kommando: netsh interface ipv6 show neighbors

```

Internetadress ----- Fysisk adress Typ ----- Gränssnitt 14: Trådlös nätverksanslutning ----- Internetadress -----
ff02::2 Permanent Permanent Internetadress Fysisk adress Typ -----
ff02::16 Permanent Permanent 00-00-00-00-00-00 Inte Atkomlig Gränssnitt 17: Teredo Tunneling P
ff02::1b Permanent Permanent fe80::5ef6:127.0.0.1
ff02::1c Permanent Permanent Internetadress Fysisk adress Typ -----
ff02::112 Permanent Permanent ff02::2 Internetadress -----
ff02::113 Permanent Permanent ff02::16 33-33-00-00-00-02 Permanent ff02::16
ff02::11f02:aeff2 Permanent Permanent ff02::1c 33-33-00-00-00-0c Permanent ff02::12
ff02::11ff1a:9808 Permanent Permanent ff02::1e 33-33-00-00-00-16 Permanent ff02::1e
ff02::11ff2f:1ca6 Permanent Permanent ff02::112 33-33-00-01-00-02 Permanent ff02::112
ff02::11ff2e:9883 Permanent Permanent ff02::1133 33-33-00-01-00-03 Permanent ff02::112
ff02::11ff3b:34db Permanent Permanent Gränssnitt 11: Anslutning till lokalt nätverk ----- Gränssnitt 15: Bluetooth-nätverk -----
ff02::11ff44:7816 Permanent Permanent Permanent ff02::2 Internetadress -----
ff02::11ff41:cb41 Permanent Permanent Permanent ff02::16
ff02::11ff50:4aa4 Permanent Permanent Permanent ff02::1b
ff02::11ff60:2a26 Permanent Permanent 2001:2:3:4::1 Inte Atkomlig Inte Atkomlig ff02::12
ff02::11ff61:4a00 Permanent Permanent 2001:2:3:4::12 Inte Atkomlig Inte Atkomlig ff02::112
ff02::11ff69:b182 Permanent Permanent fe80::9da:801:bc00:bac5 Fösladress ff02::1b
ff02::11ff6c:1091 Permanent Permanent ff02::11 33-33-00-00-00-01 Permanent ff02::113
ff02::11ff72:73c Permanent Permanent ff02::12 33-33-00-00-00-02 Permanent ff02::1ff02:aeff2
ff02::11ff80:45ab Permanent Permanent ff02::1c 33-33-00-00-00-0c Permanent ff02::11ff93:368c
ff02::11ff91:ae50a Permanent Permanent ff02::16 33-33-00-00-00-16 Permanent ff02::11ff1e:9808
ff02::11ff9a:1077c Permanent Permanent ff02::1b 33-33-00-00-00-1b Permanent ff02::11ff2f:1ca6
ff02::11ff98:9556 Permanent Permanent ff02::112 33-33-00-01-00-02 Permanent ff02::11ff2e:9883
ff02::11ffa2:90db Permanent Permanent ff02::11f00:1 33-33-ff-00-00-01 Permanent ff02::11ff3b:34db
ff02::11ffa9:9318 Permanent Permanent ff02::11ff00:2 33-33-ff-00-00-02 Permanent ff02::11ff44:7816
ff02::11ffab:674a Permanent Permanent ff02::11ff27:1ca6 33-33-ff-27-1c-a6 Permanent ff02::11ff41:cb41
ff02::11ffab:78ff Permanent Permanent ff02::11ffab:674a 33-33-ff-ab-67-4a Permanent ff02::11ff44:9d36
ff02::11ffab:8532 Permanent Permanent ff02::11ffab:78ff 33-33-ff-ab-78-ff Permanent ff02::11ff50:4aa4
ff02::11ffae:d0 Permanent Permanent ff02::11ff02:5095 33-33-ff-b2-50-95 Permanent ff02::11ff60:2a26
ff02::11fdb3:5955 Permanent Permanent ff02::11ff61:7a8 33-33-ff-b3-7a-8 Permanent ff02::11ff63:4a00
ff02::11fdb3:a408 Permanent Permanent ff02::11ff22:5296 33-33-ff-c2-52-96 Permanent ff02::11ff69:b182
ff02::11fcc4:4902 Permanent Permanent ff02::11ffca:2036 33-33-ff-c4-20-36 Permanent ff02::11ff6c:1091
ff02::11fcc8:953b Permanent Permanent ff02::11fffa:d7b4 33-33-ff-ca-d7-b4 Permanent ff02::11ff72:73c
ff02::11fd04:3242 Permanent Permanent ff02::11fffa:5028 33-33-ff-fa-50-28 Permanent ff02::11ff80:45ab
ff02::11fd0b:30a3 Permanent Permanent ff02::1c 33-33-00-00-00-0c Permanent ff02::11ff8a:3255
ff02::11fd01:967f Permanent Permanent Gränssnitt 24: Isatap.(B32E47FC-3061-4536-918A-72F8F2657A7) -----
ff02::11fd03:9922 Permanent Permanent Permanent ff02::11ff91:ae50a
ff02::11fd04:9898 Permanent Permanent Permanent ff02::11ff9a:1077c
ff02::11fd03:b7a8 Permanent Permanent Permanent ff02::11ff98:9556
ff02::11fd04:1b96 Permanent Permanent Permanent ff02::11ffa2:90db
ff02::11fd07:fd2a Permanent Permanent Permanent ff02::11ffa9:9318
ff02::11ff50:2036 Permanent Permanent Permanent ff02::11ffab:674a
ff02::11ff59:1208e Permanent Permanent Permanent ff02::11ffab:78ff
ff02::11ff5a:d7b4 Permanent Permanent Permanent ff02::11ffab:8532
ff02::11ff5c:480d Permanent Permanent Permanent ff02::11ffae:d0
ff02::11ff5f:9e28 Permanent Permanent Permanent ff02::11fdb3:5955
      
```

# En kedja av headers



## Några utmaningar förutom två protokoll i sig:

- Större organisationer och Internetoperatörer har ofta små trix för sig:
  - Option 82 i DHCP
  - Inställningar ARP cache
  - Wake on LAN
  - Gratuitous ARP används på smarta sätt
  - Virtuella maskiner och interface ID
  - Sammanslagning av interface resp. VLAN

19 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
 Intensivkurser för IT-branschen

## IP-miljön idag kan vara otroligt komplex

- Konsult hos kund. Använder kundens system och skrivare
- Kör kundens affärssystem ”i molnet”
  - Lappar ihop det för att kunna skriva ut från affärssystemet
- Drar ibland igång ett VPN mot konsultföretaget (hemmanätet)
  - Vad är default gateway?
  - Hur ska utskriften hanteras (broadcast)?

20 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
 Intensivkurser för IT-branschen

## Sammanfattning

- Wireshark är klart att köra och kan lära oss om IPv6. Verkytet behövs för felsökning
- Vi behöver lära om en del!
- En del fiffiga saker funkar inte...

21 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen

## När ska man starta med IPv6?

Det finns inga egentliga fördelar med att vänta

- Ta med IPv6 vid inköp och nya avtal
- Adressbristproblemet kommer att göra ont någonstans
  - **Det finns inget problemfritt alternativ!**
- ISOC:s undersökning 2009
  - Under 10 % av de tillfrågade kan tänka sig att lämna tillbaka sina egna adresser

22 Sep 2010

COPYRIGHT 2 the point

**2THEPOINT**  
Intensivkurser för IT-branschen



Tack för mig!

[hakan.lindberg@b3it.se](mailto:hakan.lindberg@b3it.se)