Bab VIII - Permasalahan IPV6

Iljitsch van Beijnum

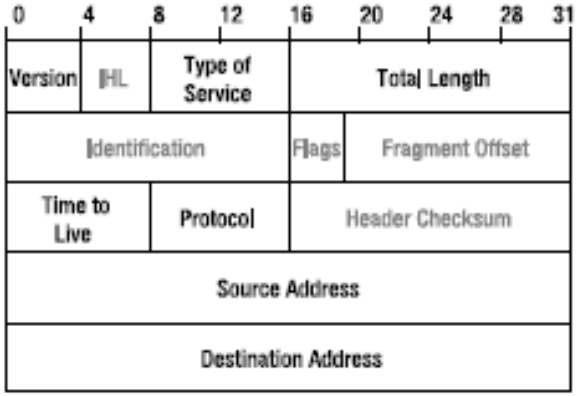
IPv6 Internals

Pada bab ini akan menjelaskan tentang internal dari IPv6, banyak dari kelebihan dan juga kekurangan yang telah dijelaskan dan anda jetahui dari IPv6. terdapat beberapa case dalam IPv6 seperti penomoran ulang dan multicast. Sangat butuh untuk belajar dan mengerti background dari spesifikasi ini sebelum mengimplementasikannya dengan baik

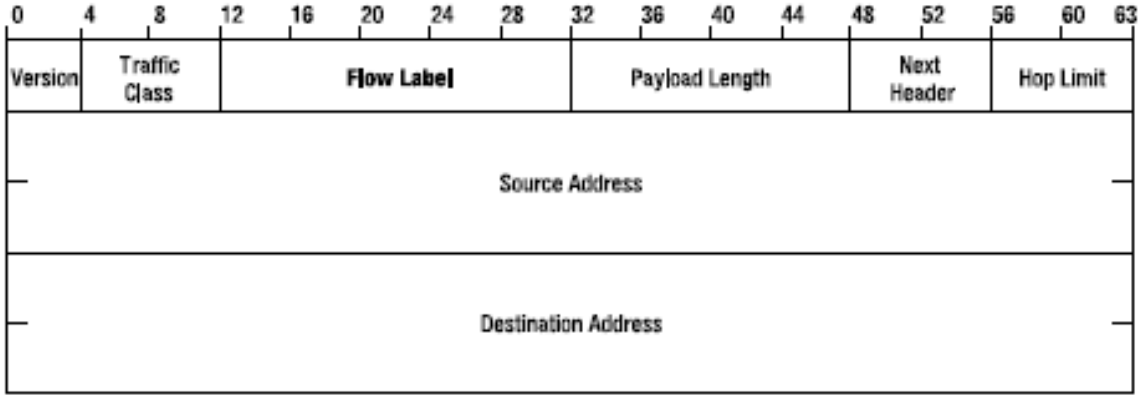
Perbedaan Antara IPv4 dan IPv6

Semua pengetahuan tentang permulaan dari IPv6 sperti header sangatlah berbeda dengan IPv4 dalam hal format. Meskipun spesifikasi dari IPv6 adalah 64 bit, IPv6 juga didesain untuk 64 bit prosesing. Untuk alasan ini IPv6 dapat membaca lebih besar memori dan sangat membantu dengan 64 bit

IPv4 Header



IPv6 Header



- Gambar diatas merupakan perbedaan dari header IPv4 dan IPv6

Model dari IPv4 header tidak merepresentasikan IPv6 header, terdapat perubahan dari IPv4 ke IPv6 :

- Versi sekarang 6 lebih tinggi dari 4
- Internet Header Length diketahui IPv6 lebih panjang 40 byte dari IPv4
- Tipe dari traffic saat ini adalah traffic class
- Flow Label terbaru dari IPv6 dengan model packet mengikuti pada stream yang sama dengan begitu memudahkan dalam mengenali paket
- Total Length pada IPv4 termasuk header, sedangkan IPv6 tidak, Payload tidak masuk pada header tetapi tersimpan pada router
- Identifikasi Flag dan Fragmentasi jika IPv4 haruslah terfragmentasi sedangkan pada IPv6 fragmentasi dilakukan sendiri pada header
- Time to live atau Hop Limit sangat cocok dengan router

- Protokol dari IPv4 diganti dengan header lanjutan dari IPv6, yang dapat dijelaskan header dari IPv4 mengikuti IPv6 header dan juga mengimplementasi untuk paket 6 TCP dan 17 UDP. Karena IPv6 memiliki length yang tetap , setiap routing danfragmentasi haruslah diimplementasikan pada header antara IPv6 header dan juga TCP
- IPv4 checksum dihapus pada IPv6
- Alamat sumber dan alamat tujuan sama pada IPv6 dan IPv4 hanya pada IPv6 terdapat 128 bit

Checksum

- Pada IPv4 dan IP header diproteksi dengan header checksum, checksum algoritma untuk IPv4, ICMP,ICMPv6,TCP,UDP memiliki model checksum yang sama
- IPv6 tidak memiliki header checksum yang berarti ketika paket error saat mentransnsmisikannya maka paket akan error dan tidak terkirim, tetapi IPv6 tetap dapat mengetahui apakah paket itu error dengan CRC (cyclic redundancy check)
- Seperti checksum akan tetapi lebih baik dalam mengkoreksi

Extension header

- Pada setiap spesial proses, IPv4 mengikuti IP header terdapat tambahan 1 atau lebih,saat ini masih belum memiliki sesuatu yang dapat memcahkannya karena paket tidak dapat diproses dengan fast path
- Karena header tetappada IPv6, hal ini tidak dapat menjadikan IP header pada IPv4, mereka hanya sama mengimplementasikan TCP dan UDP. Extension yang paling sering digunakan adalah :

- Hop by Hop Option = melihat section yang diikuti
- Routing = sama seperti routing pada IPv4
- Fragment = digunakan untuk fragmentasi
- Authentication = mengautentikasi user data pada header
- Encapsutation Security Payload = mengenkripsi user data
- Destination Option = melihat section yang mengikuti

ICMPv6

Pada IPv6 ICMP yang digunakan sama dengan ICMP pada IPv4, akan tetapi terdapat sedikit perubahan, pada IPv4 ketika tujuan tidak dapat memproses maka ICMP akan mengirim balik pesan error.

Tetapi pada IPV6 ketika tujuan tidak dapat memproses ICMPv6 akan mengembalikan paket dengan merubah besar paket sehingga lebih kecil traffic pada jaringan

- Berikut adalah tipe pesan dari ICMPv6

1. 1: Destinasi tidak terdeteksi
2. 2: paket terlalu besar
3. 3: waktu yang terlalu lama
4. 4: terdapat parameter yang bermasalah pada router
5. 128: echo request
6. 129: echo reply
7. 130: multicast menerima query
8. 131: multicast menerima laporan
9. 132: multicast selesai
10. 133: router socilicitation
11. 134 : iklan dari router
12. 135: heighbour socilicitation
13. 136: iklan neighbour
14. 137 : redirect pesan

Neighbour Discovery

Ketika pesan ingin mengirim IPv6 paket pada sistem lain yang terkoneksi pada subnet yang sama, sangatlah dibutuhkan Mac Address, Neighbour Discovery dimaksudkan untuk mengetahui Mac Address layaknya ARP pada IPv4

Setiap IPv6 sistem bergabung pada solicited node multicast grup yang hampir sama pada setiap alamat, karena solicitec grup consisten pada prefix ff02:0:0:0:0:1:ff00::/104

Karena multiple address pada IPv6 dapat dipetakan pada 1 solicited maka sistem akan menerima neighbour solicition pada check yang pertama

Neighbour Unreachability Detection

RFC 2461 juga sangat spesifik dalam prosedur dari heighbour unreachability detection, IPv6 host dan router sangat aktif dalam melakukan list neighbour reachable. Hal ini untuk melakukan list pada IPv6 sistem untuk dead neighbour, dan neighbour yang telah berganti Mac Address Windows XP, linux, Mac OS dan Free BSD semuanya akan menerima report dari IPv6 yang loses secepatnya saat setelah IPv6 di run

Stateless Address Configuration

- Satu host pada link local address dapat diproses pada 1 atau lebih alamat global IPv6 menggunakan RFC 2462
- IPv6 router akan mengirim router advertisement (RA) juga ICMP tipe 134 secara periodik
- Informasi dari RA meliputi :

1. 8 bit cur hop limit yaitu host yang memiliki data hop limit pada IPv6 paket yang terkirim
2. Managed address configuration untuk memanage dari alamat agar dapat ter set secara otomatis
3. Other statefull configuration layaknya point 2 tapi lebih ke nonaddress configuration
4. 16 bit router life time
5. 32 bit reachable time dengan nilai milisekon
6. 32 bit retrans timer dengan nilai milisekon

- Ketika nilai dikenali 0, maka dapat dikenali spesifikasi dari RA, lali host akan datang untuk step lainnya salah satunya preceding, router advertisement seperti :

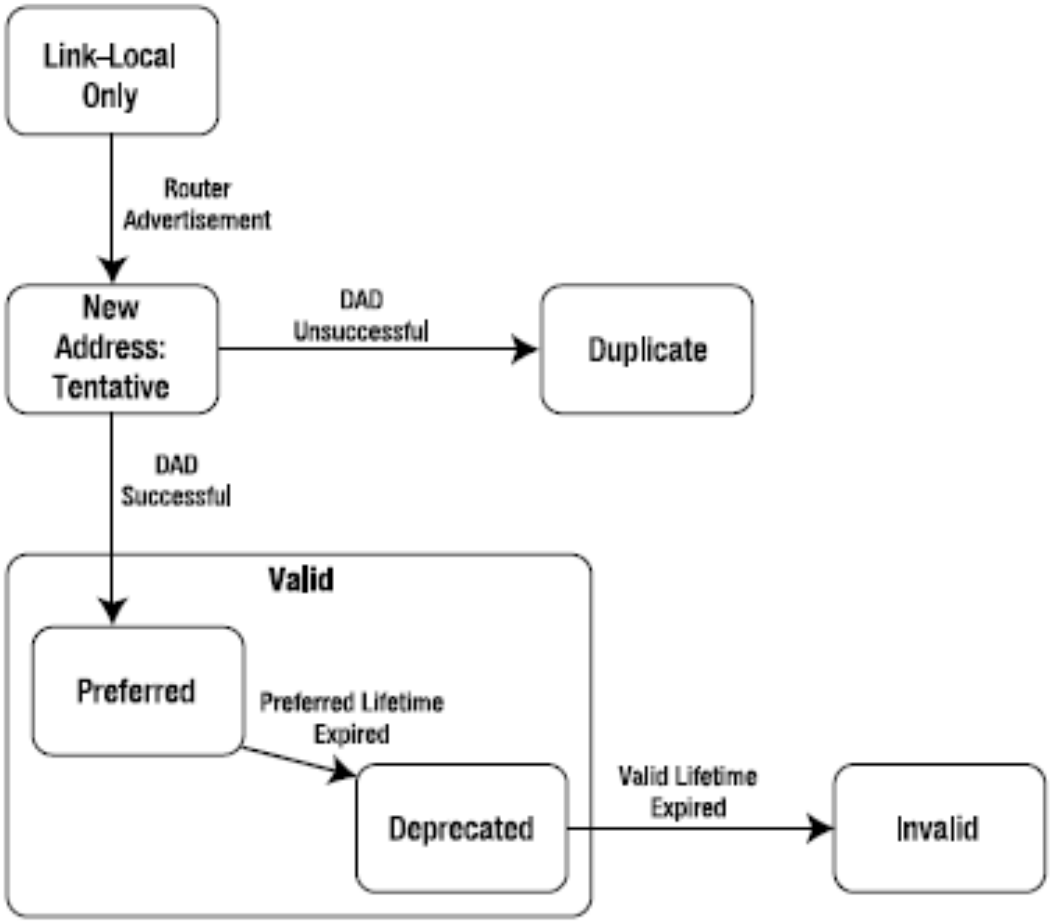
1. Source link layer address, router Mac Address
2. MTU, max besar dari paket
3. Prefix information untuk spesifikasi prefix

- Informasi prefix meliputi

1. Alamat prefix sendiri dan panjangnya
2. On-Link Flag, flag ini memberitahu prefix sedang on Link
3. Autonomous address configuration , ini memeberitahu host bahwa dapat mensetting alamat sendiri
4. 32 bit valid lifetime
5. 32 bit preferred lifetime

Mendeteksi Alamat Kembar

- Untuk menghindari situasi dimana IPv6 menggunakan alamat yang kembar, maka dapat dideteksi apakah ada kembar atau tidak, ini sangat baru dari IPv6 dan diimplementasikan dari alamat global unicast
- Jadi jika host melakukan stateless address configuration dengan EUI 64 maka DAD akan melakukan pengecekan untuk alamat link lokalnya



- Dari gambar diatas host akan memulai pada link lokal address dan DAD juga selesai pada link lokal address

- Jika DAD mengembalikan nilai 0 maka tidak ada tindakan dari DAD, dan mengikuti dari situasi yaitu :

1. Host menerima neighbour advertisement dari host lain
2. Host menerima neighbour solicitation dari host lain
3. Tidak ada jawaban

Address Lifetime

Setelah sukses dalam pengimplementsian DAD, alamat akan mengkonfigurasi stateless address autoconfiguration dapat digunakan pada preffered lifetime dari router lain

Selanjutnya digunakan alamat, valid time juga dan menghapus alamat menghapus dari interface dan juga memberhentikan session yang masih menggunakan alamat

Penomoran Ulang

Terdapat perbedaan dan valid nomor untuk router advertisement dan juga untuk setiap prefix dan membuatnya mungkin untuk 2 model, penomoran ulang sangatlah mudah dan juga sangat mungkin untuk menjalankannya sekaligus

```
!
interface Ethernet0
 ipv6 address 2001:db8:4500:17c::/64 eui-64
 ipv6 address 2001:db8:31:2::/64 eui-64
 ipv6 nd prefix 2001:db8:31:2::/64 infinite 0
!
```

- Memulai dengan alamat baru, TCP dan UDP akan melanjutkan untuk proses seperti alamat sebelumnya, seluruh komunikasi akan dimulai sebelum perubahan dan alamat lama akan dihapus

```
!
interface Ethernet0
 ipv6 nd prefix 2001:db8:31:2::/64 7200 0
!
```

- Untuk setting dari lifetime dan menghapus alamat :

```
ipv6 nd prefix 2001:db8:31:2::/64 0 0 no-autoconfig
```

- 2 jam kemudian akan dihapus secara otomatis dengan penghapusan dari router seperti berikut

```
!
interface Ethernet0
 no ipv6 address 2001:db8:31:2::/64 eui-64
 no ipv6 nd prefix 2001:db8:31:2::/64
!
```

- Anda dapat melakukan monitoring lifetime dengan netsh interface ipv6 show address

Alamat Prefix dan Router Lifetime Mismatch

- Awalnya, akan dijelaskan potensial untuk router advertisement dan prefix dengan independent lifetime dengan mengikuti permutasi :

1. RA lifetime valid
2. RA lifetime invalid
3. RA lifetime valid tetapi prefix invalid
4. RA lifetime invalid tetapi prefix valid

Address Selection

- Pilihan yang baik tetapi datang dengan masalah sendiri, seperti explicit dari support untuk multiple address pada IPv6, sistem pada aplikasi akan memilih untuk mengijinkan komunikasi dengan model RFC 3483

```
# ip6addrctl show
Prefix                    Prec Label      Use
::1/128                     50     0        0
::/0                        40     1     8892
2002::/16                   30     2        0
::/96                       20     3        0
::ffff:0.0.0.0/96           10     4        0
```

- Hal ini bekerja pada semisal dengan tujuan DNS 2001::db8:31:2::! Dan 2002:dfe0:e1e2:2::! Dengan reguler alamat ::/0 dengan 6to4
- Lalu dengan lokal sistem yang memiliki alamat 2600:9700:c0::! Dan 3ffe:9700:c0::1 maka akan dibaca pada tujuan yaitu 2001::db8:31:2::1 dan 2001::db8:31:2::1 dari kedua IP itu
- Anda dapat menghapus policy table dengan ip6addrct1 delete (prefix)
- Juga dapat menambah dengan ip6addrct1 add (prefix)

- List dibawah menunjukan default alamat policy table dibawah windows XP dan Effect dari policy entry

```
C:\>netsh
netsh>interface ipv6
netsh interface ipv6>show prefixpolicy
Querying active state...

Precedence  Label  Prefix
----------  -----  --------------------------------
         5      5  3ffe:831f::/32
        10      4  ::ffff:0:0/96
        20      3  ::/96
        30      2  2002::/16
        40      1  ::/0
        50      0  ::1/128

netsh interface ipv6>set prefixpolicy ::ffff:83.0.0.0/104 60 4
Ok.

netsh interface ipv6>show prefixpolicy
Querying active state...

Precedence  Label  Prefix
----------  -----  --------------------------------
        60      4  ::ffff:83.0.0.0/104
```

Path MTU Discovery dan Fragmentasi

- Karena paket yang memilii pesan yang besar, maka TCP akan mengakomodasikan MTU untuk memperkecilnya, bagaimanapun, protokol akan berjalan pada UDP untuk reduce dari besar packet , pada IPv4 UDP paket umumnya dengan fragment, IPv6 pada router akan melakukan fragmentasi jika dibutuhkan
- Fragment header adalah 8 byte kecuali untuk header selanjutnya akan diterima 2 fields
- Setelah menerima paket pada fragmen pertama host akan menunggu 60 detik untuk fragmen lain datang

DHCPv6

DHCPv6 merupakan IPv6 model untuk DHCP karena IPv6 memiliki stateless autoconfiguration maka DHCP akan mengambil alih part berbedsa pada IPv6 dan dikompare dengan IPv4 meski detail sangatlah berbeda tetapi DHCPv6 penggunaannya sangat sama dengan DHCP pada IPv4 yang mana bertujuan untuk :

1. Konfigurasi alamat, memberi alamat untuk tiap host
2. Non address konfigurasi, memberi info seperti DNS atau domain
3. Prefix delegation memberi prefix router

KAME DHCPv6

- KAME memiliki DHCPv6 yang diimplementasikan pada ftp.kame.net pada directory /pub/kame/misc pada kame-dhcp mengikuti dari nomor versi

```
option domain-name-servers 2001:db8:31:2::53;
option domain-name "example.com";

host router
  {
    duid 00:03:00:01:00:04:27:FE:24:9F;
    prefix 2001:db8:4700::/48 86400 259200;
  };
```

- Seluruh sistem akan bertanya untuk DNS server atau domain name dengan menerima informasi. Sistem akan matching DUID juga menerima prefix 2001:db8:4700::/48

```
interface xl0
  {
    information-only;
    script "/etc/dhcp6clientscript.sh";
  };
```

- Dhcp6c daemon akan set beberapa variabel pada script berikut

```
#!/bin/sh
echo  >/etc/resolv.conf domain $new_domain_name
echo >>/etc/resolv.conf nameserver $new_domain_name_servers
```

Linux DHCPv6

- DHCPv6 project pada sourceforge http://dhcpv6.sourceforge.net didasari dari KAME DHCPv6 dengan linux port
- Source tidak dapat dicompile pada FreeBSD dan MacOS
- Dhcp6c tidak memiliki cara untuk membuat DUID jadi perlu info DHCPv6 untuk configurasi

Cisco IOS DHCPv6

- Pada versi cosco IOS sangatlah support DHCPv6 dan router juga memiliki DHCPv6 client relay server atau kombinasi

```
!
interface Ethernet0
 ipv6 dhcp relay destination 2001:db8:31:2::547
!
```

- Terdapat router relay DHCPv6 yang membuat central DHCP server dapat berjalan untuk setiap subnet

```
!
ipv6 dhcp pool dhcpv6-pool
 prefix-delegation 2001:DB8:AA5E::/48 00030001000427FEAA5E lifetime 7200 900
 prefix-delegation 2001:DB8:246E::/48 00030001000427FE246E
 dns-server 2001:db8:31:2::53
 domain-name example.com
!
interface Ethernet0
 ipv6 dhcp server dhcpv6-pool
!
```

- DHCPv6 bekerja sangat berbeda dari IPv4 yang mana akan membalas info dari dhcpv6-pool contohnya seluruh client akan menerima DNS dan domain info

- Seluruhnya sangat baik, tapi hanya akan dimulai dengan DHCP prefix delegation client

```
!
interface Ethernet1
 ipv6 address autoconfig
 ipv6 dhcp client pd dhcpv6prefix
!
interface Ethernet2
 ipv6 address dhcpv6prefix 0:0:0:A0::/64 eui-64
!
```

- Bagaimanapun interface akan mendapat DHCPv6 client dan dikonfigurasi untuk bertanya prefix, yang mana didapat dari DHCP server yang di kombinasi prefix 0:0:0:a0::64 dan EUI-64 full address

```
2001:0db8:0006:70xx
xxxx:xxxx:xxxx:xxa0
------------------- +
2001:0db8:0006:70a0
```

IPv6 Over

- Meski protokol baik IPv6 ia juga tidak dapat melakukannya sendiri, IPv6 butuh asisten dari layer protokol yang lebih rendah untuk mendapat pajet dari sistem dan dilanjutkan
- Karena layer protokol yang lebih rendah memiliki karakteristik yang berbeda maka di atur untuk standarisasi IPv6 Over… RFC

IPv6 Over Ethernet

Ethernet memiliki sejarah panjang pada aspek protokol kecuali 1 yang memiliki perubahan dimana terdapat beberapa media seperti kabel dengan kecepatan 100,1000 atau 10000 megabit per second

Destination 48 bits	Source 48 bits	Type 16 bits	User Data 46 – 1500 bytes	FCS 32 bits

- **Multicast**

Multicast address pada IPv4 terjadi pada 24 bit dari IP multicast dengan alamat yang ada pada IETF IEEE OUI 00:00:5E atau IETF OUI dengan gruo bit 01:00:5E dengan IEEE memiliki blok dari OUI

Dengan IPv6 IETF mengadopsi strategi dengan global unik OUI ethernet multicast untuk IPv6, berikut adalah setting untuk FreeBSD dan Mac OS :

```
> netstat -ia
Name    Mtu Network       Address              Ipkts Ierrs    Opkts Oerrs  Coll
xl0    1500 <Link#1>     00:01:02:29:26:40   681428     0   169451     0     0
                         33:33:5b:81:52:75
                         33:33:00:00:00:01
                         33:33:ff:29:26:40
                         01:00:5e:00:00:01
xl0    1500 192.0.2.65/24  sequoia           154437     -   164922     -     -
                         ALL-SYSTEMS.MCAST.NET
xl0    1500 fe80:1::201 fe80:1::201:2ff:f     1359     -     2389     -     -
                         ff02:1::2:5b81:5275(refs: 1)
                         ff02:1::1          (refs: 1)
                         ff02:1::1:ff29:2640(refs: 1)
xl0    1500 2001:db8:31 2001:db8:31:2:201:2  33034     -     2866     -     -
                         ff02:1::2:5b81:5275(refs: 1)
                         ff02:1::1          (refs: 1)
                         ff02:1::1:ff29:2640(refs: 1)
```

Ethernet diatas mendengar untuk 5 Mac address

- 00:01:02:29:26:40 untuk burned MAC address
- 33:33:5b:81:52:40 dipetakan ke ff02::2:5b81:5275
- 33:33:00:00:00:01 selalu dimunculkan
- 33:33:ff:29:26:40 dipetakan ke socilited node address untuk global dan lokal link address
- 01:00:5e:00:00:01 dipetakan IPv4 untk seluruh host 224.0.0.1

- **Group membership management**

Pada IPv4 multicast router akan mengirim internet group management protokol (IGMP) secara periodik, host akan memberikan router multicast group akan mendengar multicast group dan meninggalkan pesan layaknya IGMPv2 dengan perbedaan MLD untuk IPv6 dengan part ICMPv6

- **IPv6 Over Wifi**

Wifi atau IEEE 802.11 wireless lan bekerja pada 2,4 GHz karena bekerja pada internal networking pada layer yang lebih tinggi yang berati mentransmit multicast pada speed rendah sesuai kebutuhan dari 802.11. juga dapat ditambah pada multicast paket untuk seluruh penerima dengan begitu kurang dari megabit per second akan mendapat multicast pada wireless channel

- **IPv6 Over IEEE 1394**

IEEE menampung untuk share aspek dari USB dan Ethernet, seperti USB dapat dikonekkan dengan peripehral komputer, tapi tidak seperti USB, ini juga dapat dikonekkan ke beberapa komputer secara bersamaan dengan support untuk 100,200,4000 Mbps dan juga dengan nine lead connector akan dapat 800 Mbps

Pada IEEE 1394 support dengan 3 communication mode :

1. Asynchronous Block Writes
2. Asynchronous Stream Packets
3. Isochronous Stream Packet

IP over IEEE 1394 umumnya dan IPv6 IEEE 1394 part dan sangat support dan bekerja sangat baik pada Mac OS, Windows XP

- **IP Over PPP**

Point to point protokol merupakan protokol yang digunakan untuk point to point link, dan PPP sangatlah simple yang mana dapat berjalan di protokol yang berbeda (contohnya IPv4 dan IPv6)

PPP dapat tergabung pada nifty trick sebelum paket dikirm sebelum semuanya terjadi. Link control protocol (LCP) akan bernegosiasi tentang maximum yang dapat diterima dan beberapa detail lain

Tidak juga untuk IPv6 Control Protocol, RFC2023 akan memberi IPv6 over PPP hanya specifies dengan menegosiasi untuk 32 bit dengan interface yang berbeda

```
sudo /usr/sbin/pppd /dev/tty.USA19H3b1P1.1 38400 noauth local passive persist ➥
silent ipv6 ::2005
```

The arguments are

/dev/tty.USA19H3b1P1.1: The device name for the serial interface. Under Linux, PC COM ports 1–4 are numbered `ttyS0`–`ttyS3`.

38400: The serial interface speed.

noauth: Don't ask the peer to authenticate itself (this is why we need to be root to execute `pppd`).

local: Don't use modem control lines (i.e., the connection is through a null modem).

passive: Wait for the other side to initiate the LCP session.

persist: Try to reopen the PPP session after a failure.

silent: Wait with sending LCP packets until the other end becomes active.

ipv6 ::2005: Use `0x00002005` as the identifier for the local end and an empty identifier for the remote end.

Dengan syntax tersebut PPP akan mengaktifkan IPv6 dan membuiat alamat link local , jika menjalankan IPv6 pada PPP link kemungkinan akan set up manual juga dapat menggunakan DHCPv6 prefix