



*The Internet is for Everyone.*

*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

Presentation to Hong Kong Science and Technology Parks

3 June 2011

# **IPv6 Deployment**

## **The Unavoidable Step for Present and Future**

Warren Kwok  
IPv6 Working Group  
Internet Society Hong Kong



*The Internet is for Everyone.*

*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

## **Why care IPv6 ?**

# Why need IPv6

---

## Survival of the Internet

- IPv4 already exhausted,  $2^{32}$  or 4.3 billion
- IPv6 is 128 bit, address space  $2^{128}$
- All devices need IP address

## Other benefits

- IPv6 eliminates NAT  
facilitate new services and applications that require end-to-end connectivity
- In IPv6, host has a unique public address

# Devices need IPv6 address

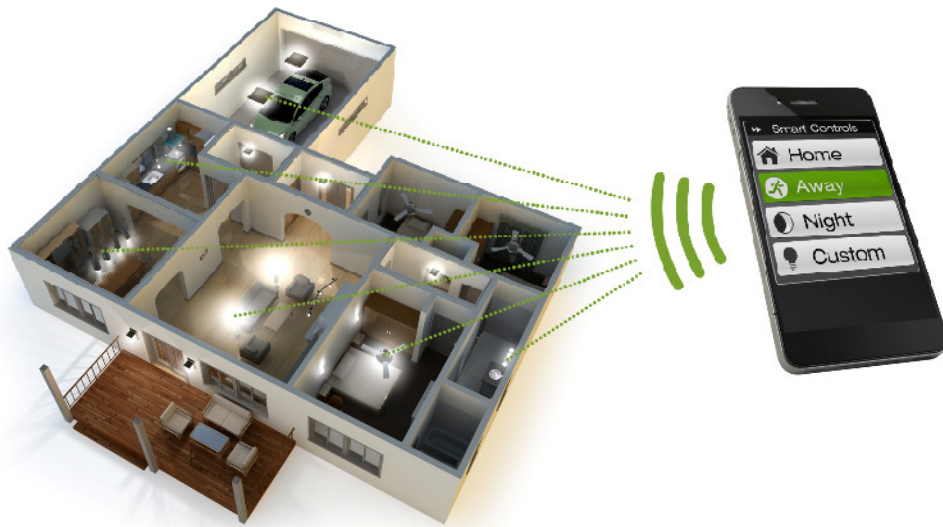
Billion devices need IPv6 an address

Rice cooker, water boiler, DVD player, TV and radio, refrigerator, air-conditioner, washing machine, microwave oven, door camera and many more



# IPv6 on every light bulb

---



## An application in IPv6 Home

- Lighting controlled by smartphones, TV or PC
- Use licence-exempted frequency band
- Energy saving
- Cost saving

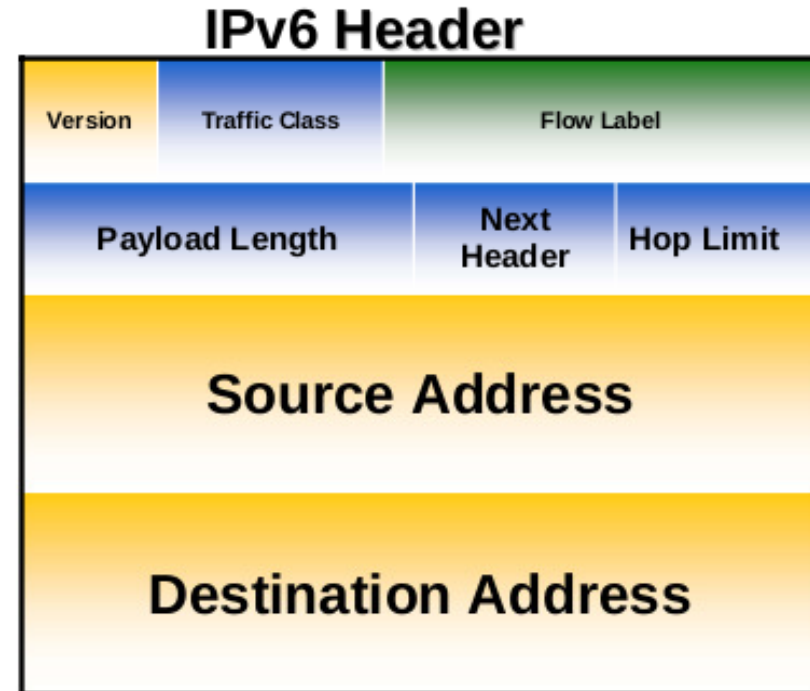
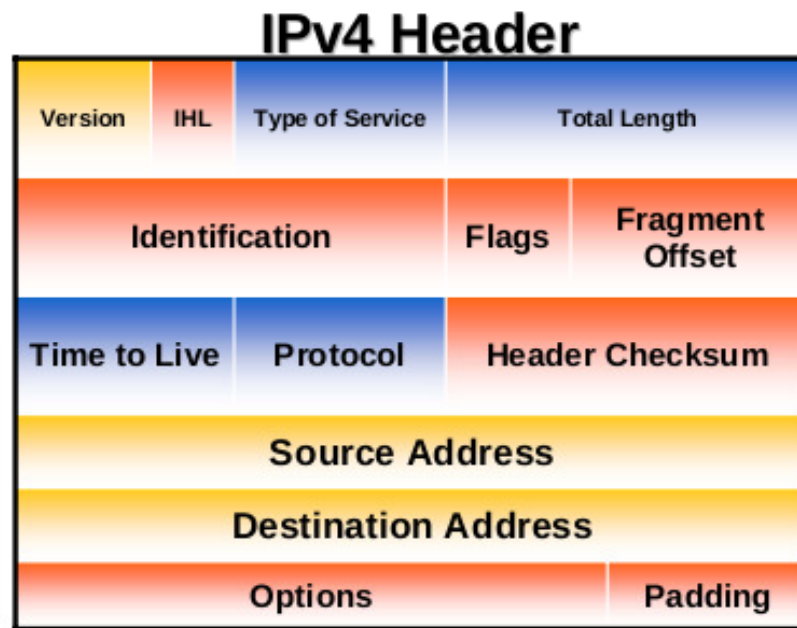
# Other benefits of IPv6





---

- 1. Efficient header
- 2. Efficient routing, each ISP advertise a /32 route
- 3. No fragmentation in router, only source perform fragmentation by extension header
- 1+2+3 = faster internet speed than IPv4
- Easy renumbering when changing ISP

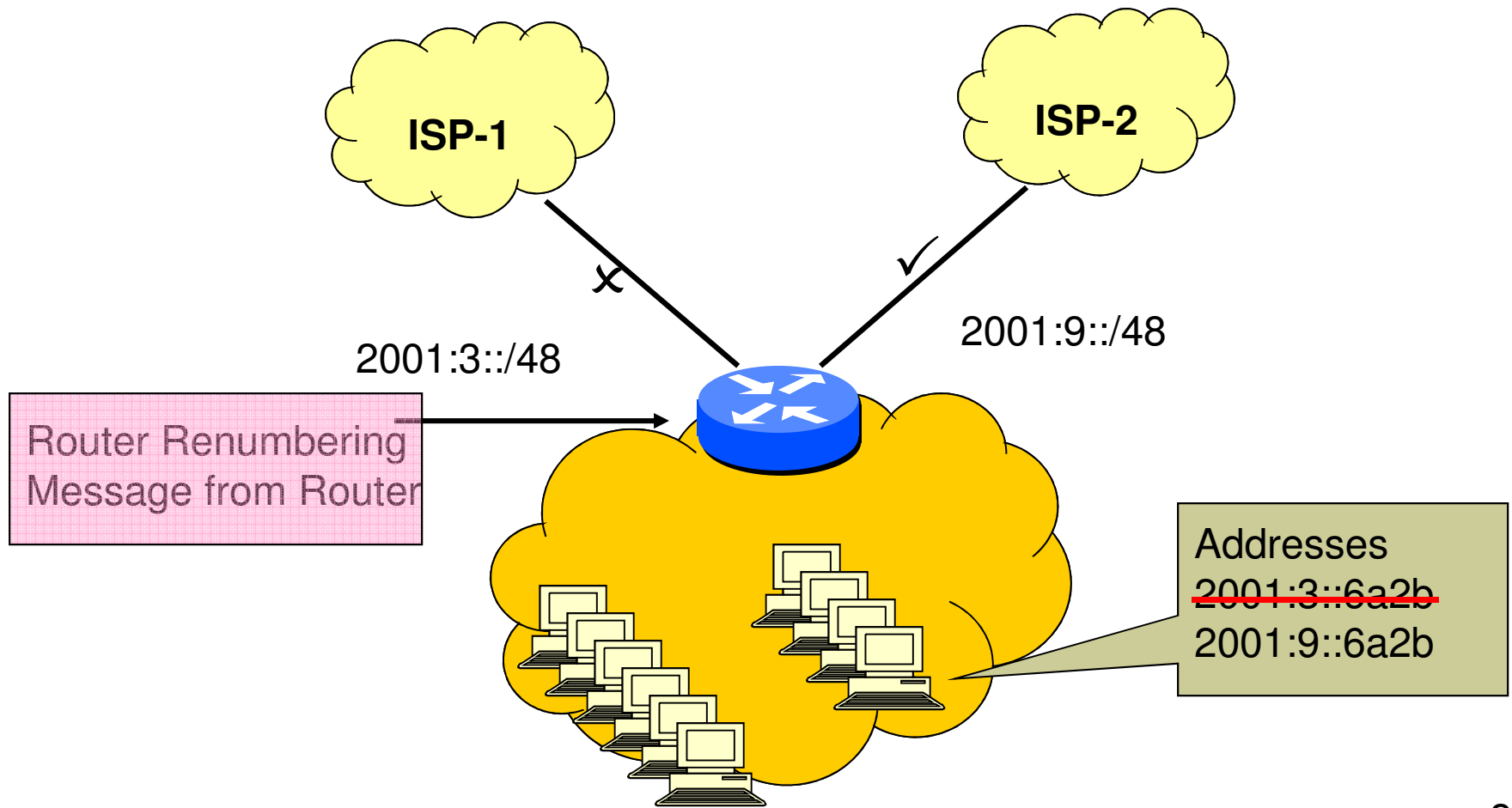
All are not as important as large address space !

# IPv6 vs IPv4 Header



- Legend**
-  - Field's name kept from IPv4 to IPv6
  -  - Fields not kept in IPv6
  -  - Name & position changed in IPv6
  -  - New field in IPv6

# Site Renumbering



# Easy Renumbering of IPv6 Hosts

---

- Aided by Router Renumbering Message
- Add a new prefix to the Router
- Reduce the lifetime of the old prefix
- As nodes depreciate the old prefix the new prefix will start to be used for new connections
- Smooth transition without break when changing ISP



*The Internet is for Everyone.*

*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

# Status of Development

# Present Status of Deployment

---

- ISPs offer IPv6 to corporate customers over Dedicated Internet Access (DIA) lines and data center customers
- A few ISPs offer IPv6 for home broadband
- Already started up in mobile broadband
- Residential v6 can not take off due to :
  - lack of CPE (v6 ADSL modem, v6 home router, v6 cable modem)
  - Windows 7 not widely deployed by home users

# US Government Mandate

---

- June 2008 – IPv6 in Federal backbone networks – complied already
- Oct 2012 - all public facing servers of Federal on native IPv6, no interim tunneling solutions is allowed
- Oct 2014 - internal systems/clients on IPv6
- Each agency appoints a transition manager to report progress

# What OS support IPv6

---

## Supported:

- Win7, Win2008 Server, MACOSX, Linux, BSD
- Win7 and 2008 Server with Teredo and 6to4 tunnels
- Mobile – Nokia Symbian (long time ago)  
iPhone OS 4.0, Android 2.2

## Windows XP

- IPv6 on SP2, installed but not enabled
  - no DHCPv6 client, no PPPv6 client,
  - auto tunnels, Teredo and 6to4



*The Internet is for Everyone.*  
*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

# IPv4 NAT Troubles

# IPv6 Internet without NAT

---

- NAT save IP address but break end-to-end connectivity (VoIP, IPSEC VPN, P2P)
- One way connection
  - ✓ NATed hosts -> Internet, ✗ Internet -> NATed hosts
- NAT not scalable

## Whereas

- IPv6 restore end-to-end visibility
- Enable end-to-end security
- Enable innovation service and application
- Trace compromised hosts and infected PCs

# NAT Issue in mobile broadband

---

- NATed address 10.x.y.z is assigned
- One routable IP address has 65536 ports max
- Google Map on Smartphone takes up more than 30 ports (next diagram will show)
- If all ports utilized, users wait until some ports released by other users on the same NAT!
- NAT keep alive message every 30 sec drain up your battery very fast !

# Ports usage by Google Map

The screenshot shows a Windows desktop environment. In the foreground, a Google Map browser window is open, displaying a map of Hong Kong. In the background, a command prompt window titled 'C:\WINDOWS\system32\cmd.exe' displays a list of network connections. The connections are all established to various IP addresses and ports, demonstrating the high number of concurrent connections used by Google Maps.

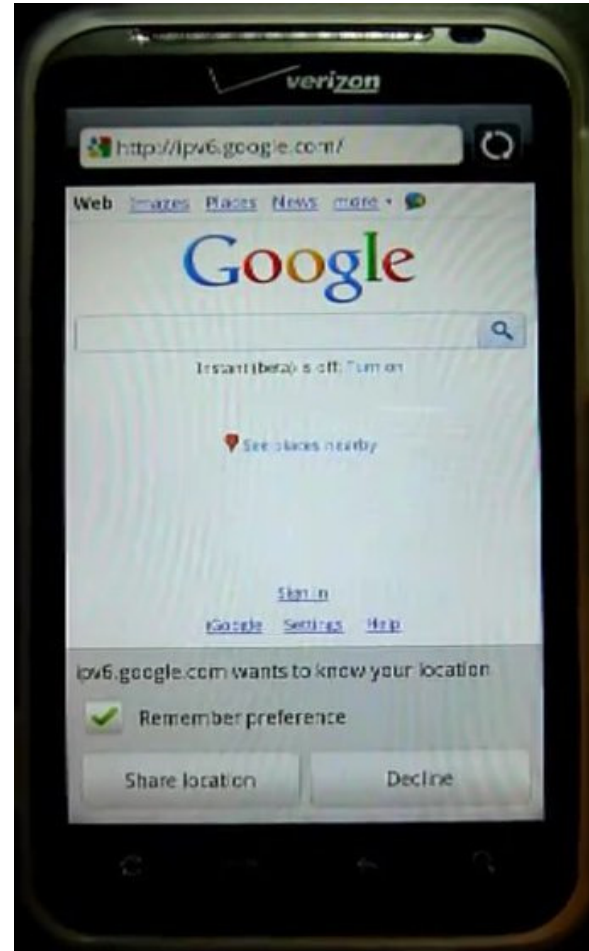
Protocol	Local IP:Port	Remote IP:Port	Status
TCP	127.0.0.1:14147	0.0.0.0:0	LISTENING
TCP	127.0.0.1:19872	127.0.0.1:1104	ESTABLISHED
TCP	192.168.1.102:139	0.0.0.0:0	LISTENING
TCP	192.168.1.102:1105	208.43.202.54:443	CLOSE_WAIT
TCP	192.168.1.102:1109	174.36.30.47:80	ESTABLISHED
TCP	192.168.1.102:1113	74.125.71.106:80	ESTABLISHED
TCP	192.168.1.102:1114	74.125.71.106:443	ESTABLISHED
TCP	192.168.1.102:1115	74.125.71.106:80	ESTABLISHED
TCP	192.168.1.102:1116	74.125.71.106:80	ESTABLISHED
TCP	192.168.1.102:1117	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1125	72.14.203.102:80	ESTABLISHED
TCP	192.168.1.102:1126	72.14.203.102:80	ESTABLISHED
TCP	192.168.1.102:1127	74.125.71.91:80	ESTABLISHED
TCP	192.168.1.102:1128	74.125.71.139:80	ESTABLISHED
TCP	192.168.1.102:1136	192.168.1.1:49152	CLOSE_WAIT
TCP	192.168.1.102:1140	74.125.71.102:80	ESTABLISHED
TCP	192.168.1.102:1141	72.14.203.139:80	ESTABLISHED
TCP	192.168.1.102:1142	174.36.215.20:80	CLOSE_WAIT
TCP	192.168.1.102:1143	74.125.71.102:80	TIME_WAIT
TCP	192.168.1.102:1144	74.125.71.102:80	ESTABLISHED
TCP	192.168.1.102:1145	74.125.71.106:80	TIME_WAIT
TCP	192.168.1.102:1146	74.125.71.105:80	ESTABLISHED
TCP	192.168.1.102:1148	74.125.71.105:80	ESTABLISHED
TCP	192.168.1.102:1149	74.125.71.105:80	ESTABLISHED
TCP	192.168.1.102:1150	74.125.71.105:80	ESTABLISHED
TCP	192.168.1.102:1152	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1153	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1154	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1155	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1156	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1157	74.125.71.100:80	ESTABLISHED
TCP	192.168.1.102:1158	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1159	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1160	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1161	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1162	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1163	74.125.71.113:80	ESTABLISHED
TCP	192.168.1.102:1164	72.14.203.99:80	ESTABLISHED
TCP	192.168.1.102:1165	72.14.203.99:80	ESTABLISHED
TCP	192.168.1.102:1166	72.14.203.99:80	ESTABLISHED
TCP	192.168.1.102:1167	72.14.203.99:80	TIME_WAIT
TCP	192.168.1.102:1168	72.14.203.99:80	TIME_WAIT
TCP	192.168.1.102:1169	72.14.203.99:80	TIME_WAIT
TCP	192.168.1.102:2869	192.168.1.1:3707	CLOSE_WAIT
TCP	192.168.1.102:2869	192.168.1.1:3710	CLOSE_WAIT

Concurrently open  
38 ports just for  
Google Map !

# IPv6 on 4G LTE network

---

- Verizon LTE launched in mid March 2011
- One NATed IPv4 address and an IPv6 address
- A strong stimulus for global IPv6 development





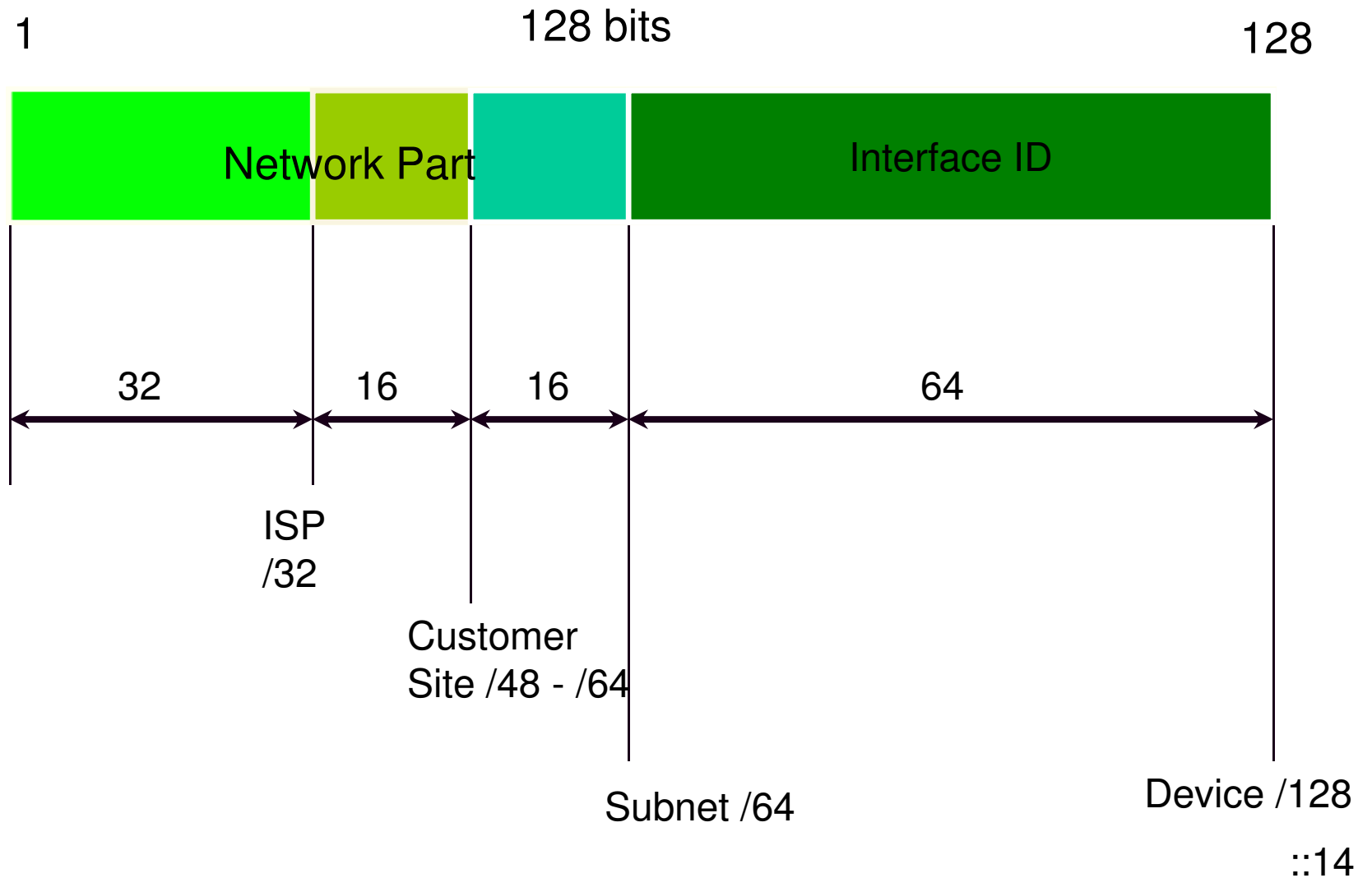
*The Internet is for Everyone.*  
*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

# Addressing and Capacity

# IPv6 Addressing Structure

---



# Capacity of an IPv6 ISP

---

- Allocated a /32 block initially
- Can serve 65536 ( $2^{16}$ ) corporate customer (/48 per corporate customer)
- Each corporate customer can have 65536 ( $2^{16}$ ) subnets
- Or can server 4.3 billion ( $2^{32}$ ) broadband home users
- Each home network can have unlimited home PCs with routable IPv6 address

# Assign IPv6 address to host

---

- Auto-configuration
- Manual Configuration
  - Set IP address, subnet prefix ? (like subnet mask in IPv4)
  - Set default route and other routes
  - Set IP address of 2 DNS resolvers
  - The only methods for servers, routers and firewalls
- Dynamic IP configuration
  - Employ a DHCPv6 Server in the network segment

# Windows - TCP/IPv6 Interface

**Internet Protocol Version 6 (TCP/IPv6) Properties**

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

Obtain an IPv6 address automatically

Use the following IPv6 address:

IPv6 address: 2001:2[redacted]:2

Subnet prefix length: 64

Default gateway: 2001:[redacted]2::1

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: 2001[redacted]:11

Alternate DNS server: 2001[redacted]::101

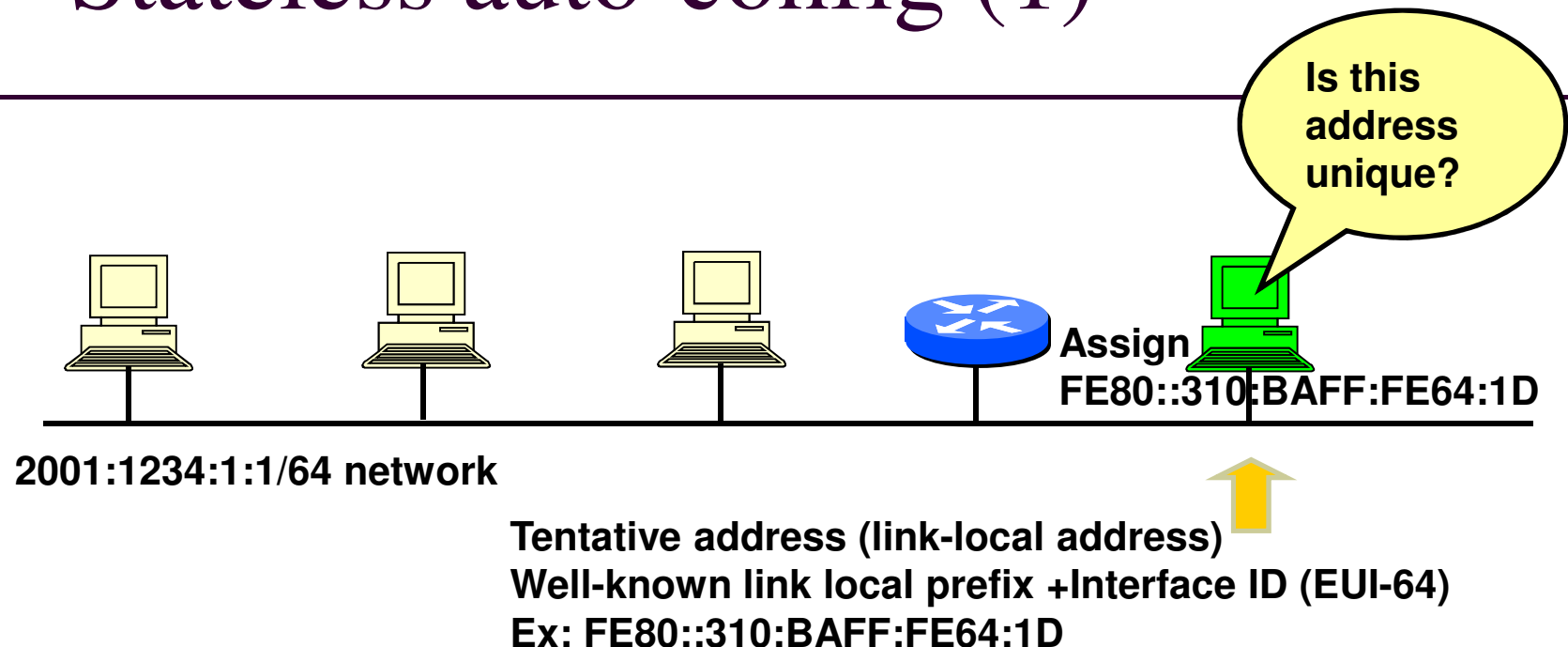
Validate settings upon exit

Advanced...

OK Cancel

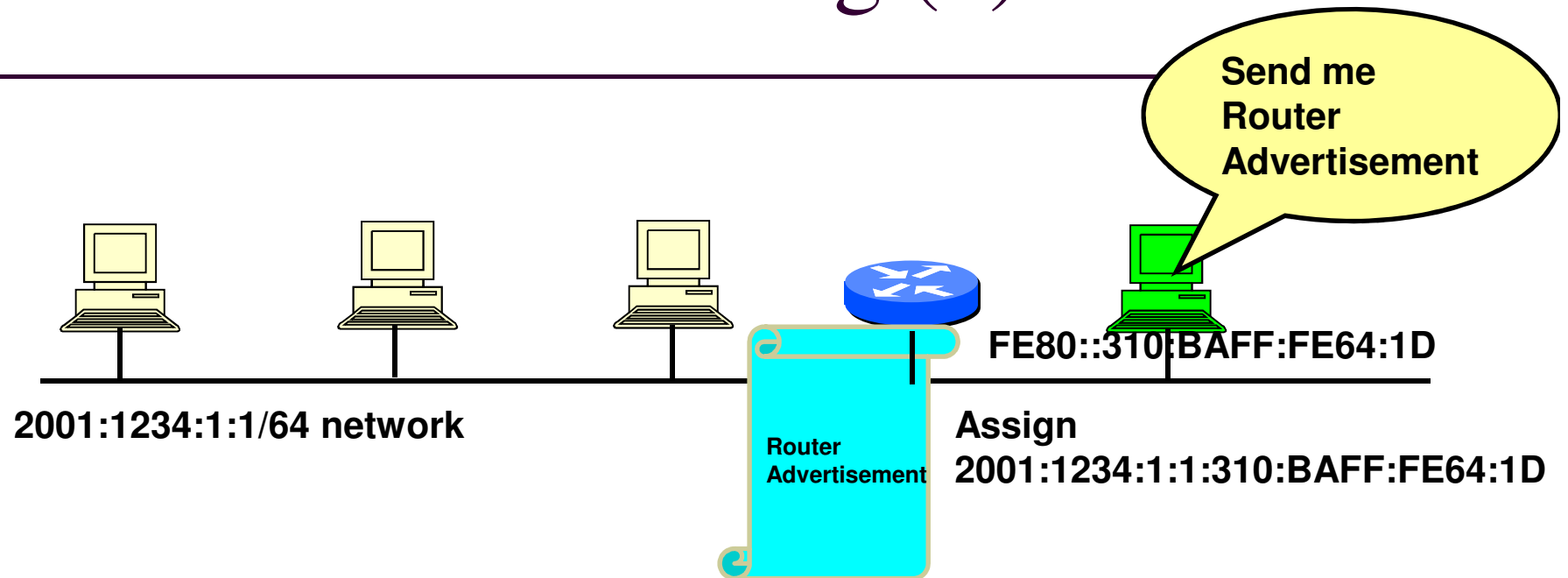
- Similar to TCP/IPv4
- Careful input to avoid missing colon and hex digits
- Support DHCPv6 and static assignment

# Stateless auto-config (1)



1. A new host is turned on.
2. Tentative address will be assigned to the new host.
3. Duplicate Address Detection (DAD) is performed. First the host transmit a Neighbor Solicitation (NS) message to all-nodes multicast address (FF02::1)
5. If no Neighbor Advertisement (NA) message comes back then the address is unique.
6. FE80::310:BAFF:FE64:1D will be assigned to the new host.

# Stateless auto-config (2)



1. The new host will send Router Solicitation (RS) request to the all-routers multicast group (FE02::2).
2. The router will reply Routing Advertisement (RA).
3. The new host will learn the network prefix. E.g, 2001:1234:1:1/64
4. The new host will assign a new address Network prefix+Interface ID  
E.g, 2001:1234:1:1:310:BAFF:FE64:1D



*The Internet is for Everyone.*

*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

# **DNS, Firewall, Security and Transition Issues**

# IPv6 forward name lookup

---

To resolve a host name into address

IPv4 uses A record to specify an address

IPv6 uses AAAA record to do the same

Example

```
[root@localhost ~]# host -t a www.arin.net
```

```
www.arin.net has address 192.149.252.75
```

```
[root@localhost ~]# host -t aaaa www.arin.net
```

```
www.arin.net has IPv6 address 2001:500:4:13::80
```

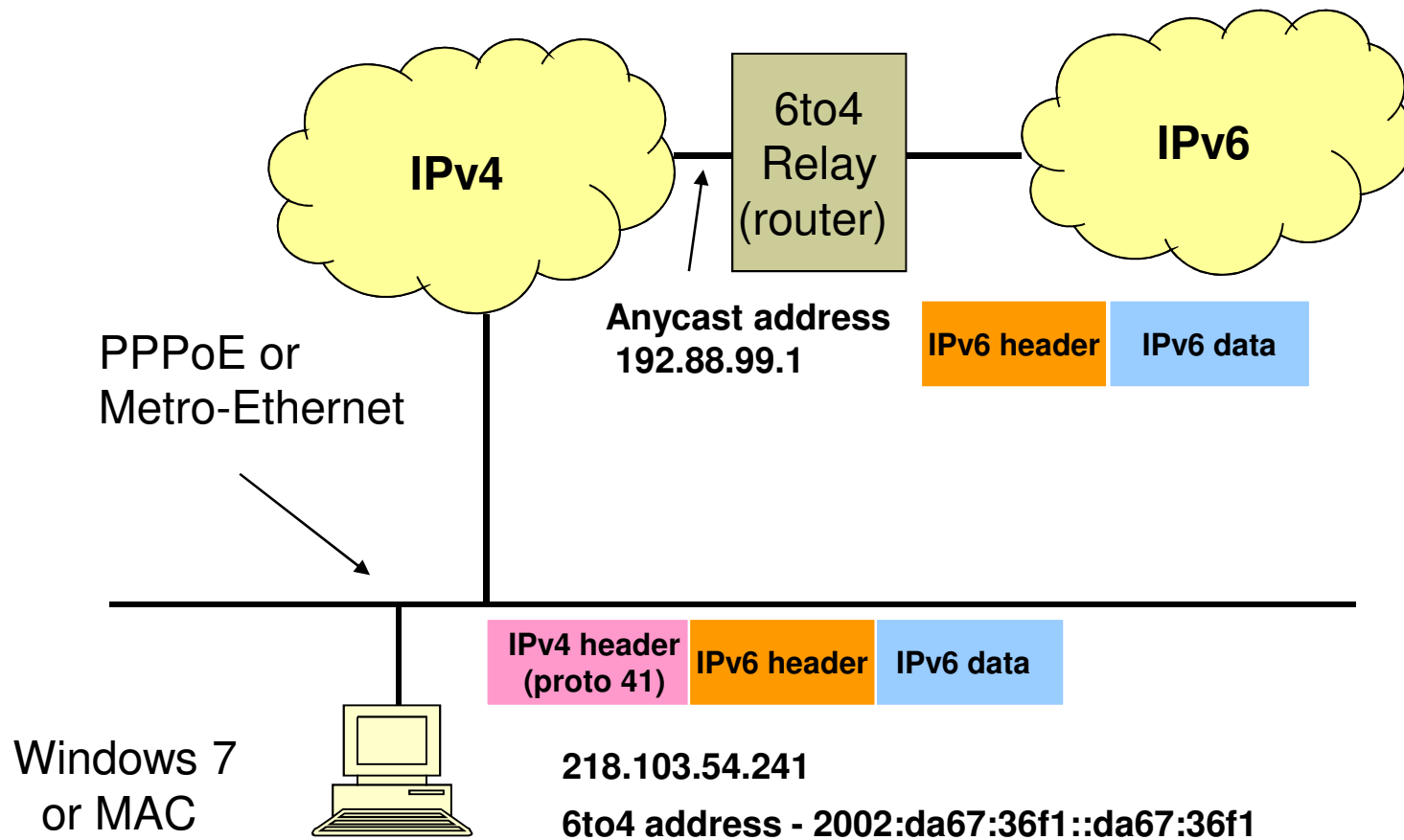


# IPv6 Firewall

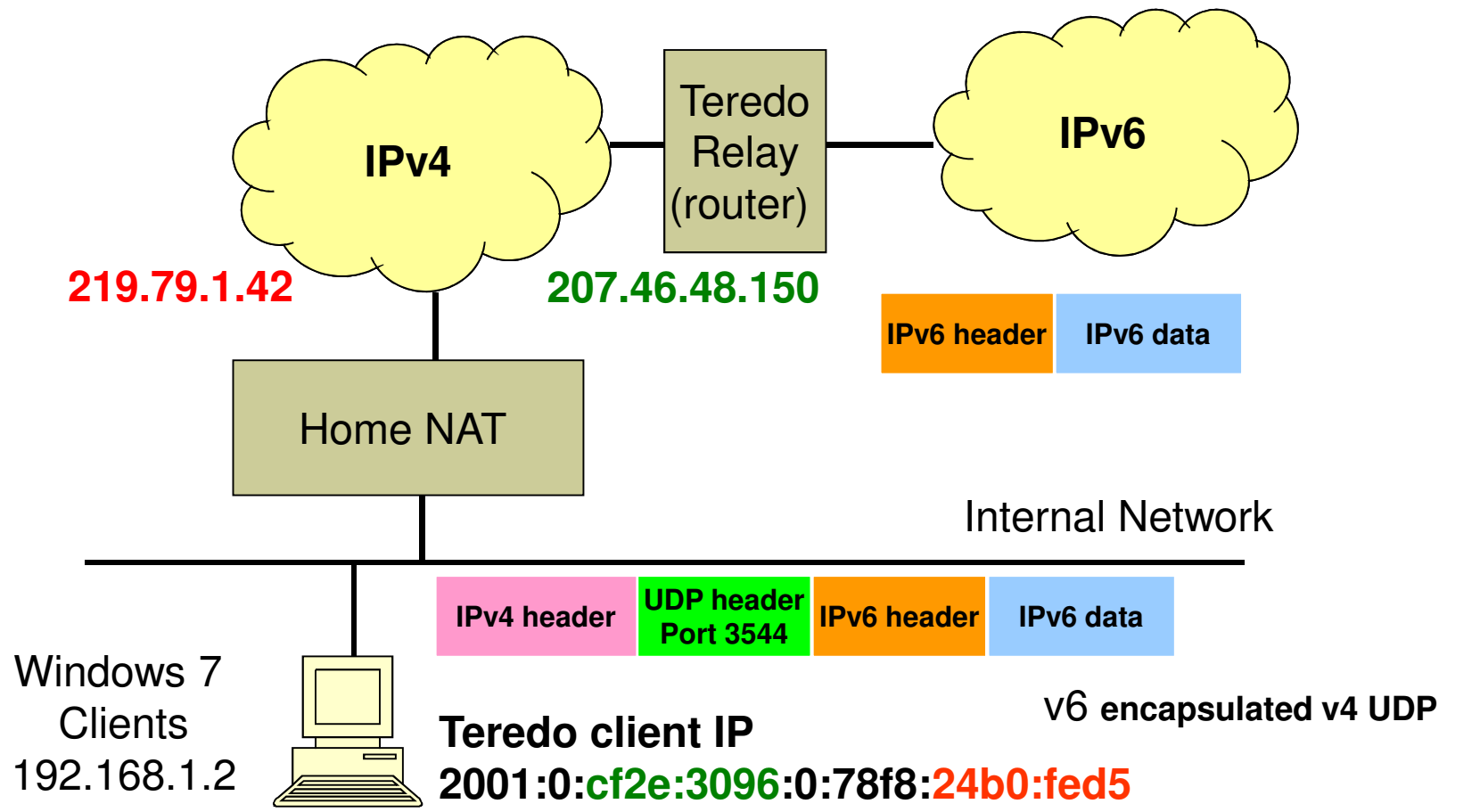
---

- Mature and affordable products
- Open Source - Linux ip6tables offers stateful packet inspection
- Permit UDP > 512 bytes to pass for DNS traffic
- Proper filtering of ICMPv6 messages
  - e.g. - Packet too big and destination unreachable should not be blocked
  - block inbound Router Advertisement
- Do not blindly replicate v4 rules

# Windows 6to4 tunnel for Home Users



# Windows Teredo tunnel for home users



# A look at Teredo and 6to4 tunnels

```
C:\Windows\system32\cmd.exe
乙太網路卡 區域連線:
 連線特定 DNS 尾碼 . . . . . :
 連結-本機 IPv6 位址 . . . . . : fe80::712c:1e45:a4db:4ca9%12
  IPv4 位址 . . . . . : 192.168.1.101
 子網路遮罩 . . . . . : 255.255.255.0
 預設閘道 . . . . . : 192.168.1.1

無線區域網路介面卡 無線網路連線:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

通道介面卡 isatap.{F7089D8F-1870-491B-8A54-8E9CABDC63DF}:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

通道介面卡 isatap.{14E6FBF6-6306-41D5-B31E-A92DF8B1B784}:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

通道介面卡 Teredo Tunneling Pseudo-Interface:
 連線特定 DNS 尾碼 . . . . . :
  IPv6 位址 . . . . . : 2001:0:4137:9e76:1092:3774:24b2:f622
 連結-本機 IPv6 位址 . . . . . : fe80::1092:3774:24b2:f622%13
 預設閘道 . . . . . :

C:\Users\USER>
```

Teredo Tunnel

```
C:\Windows\system32\cmd.exe
 連線特定 DNS 尾碼 . . . . . :
通道介面卡 isatap.{14E6FBF6-6306-41D5-B31E-A92DF8B1B784}:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

通道介面卡 6T04 Adapter:
 連線特定 DNS 尾碼 . . . . . :
  IPv6 位址 . . . . . : 2002:db4d:17ca::db4d:17ca
 預設閘道 . . . . . : 2002:c058:6301::c058:6301

通道介面卡 Teredo Tunneling Pseudo-Interface:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

通道介面卡 isatap.{32DF7C51-4A00-46AE-829D-0F70115D8171}:
 媒體狀態 . . . . . : 媒體已中斷連線
 連線特定 DNS 尾碼 . . . . . :

C:\Users\USER>
```

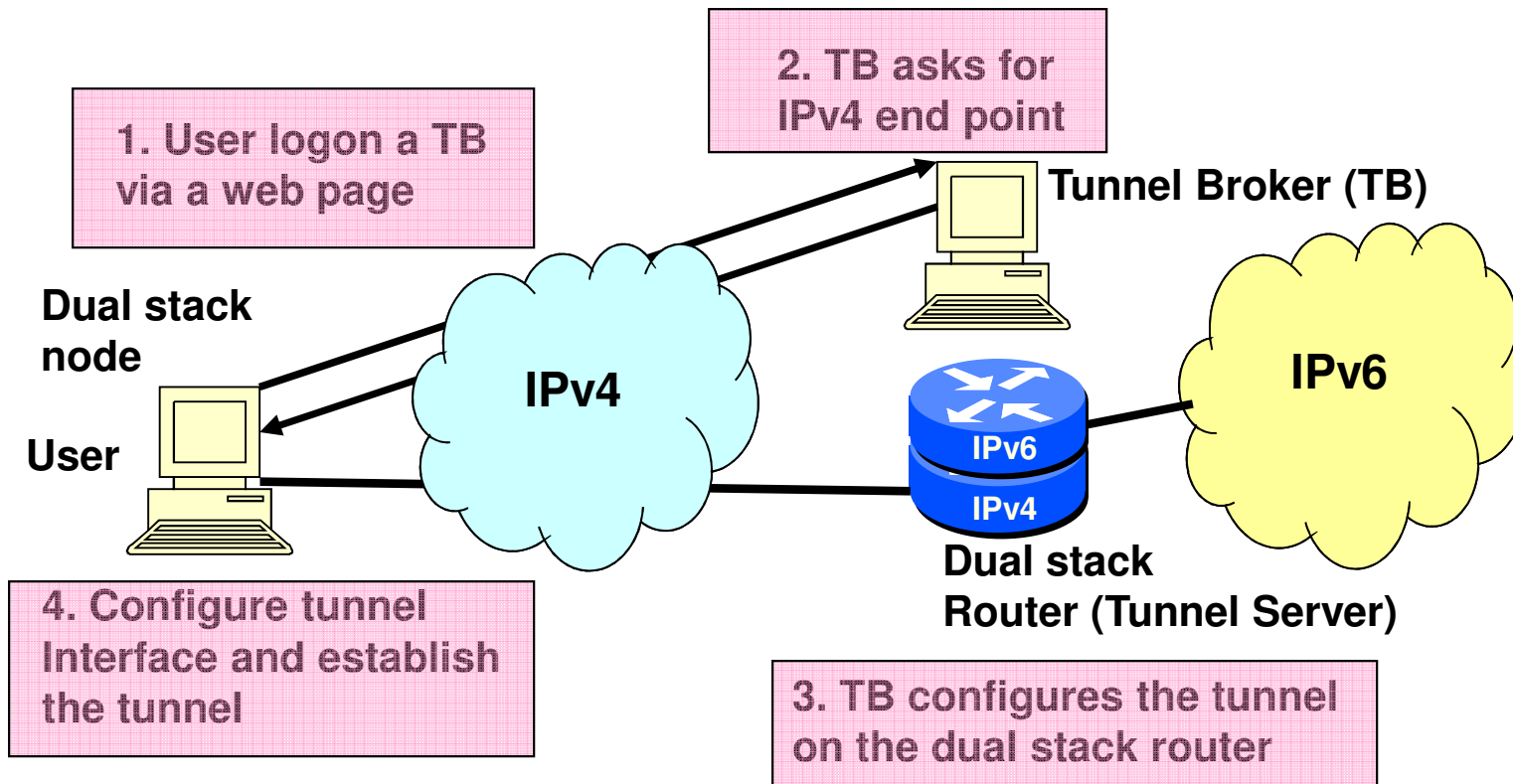
6to4 Tunnel

# Tunnel Broker Service

---

- Very popular in the IPv6 user community
- Well-known brokers are Hurricane Electric ([tunnelbroker.net](http://tunnelbroker.net)) and gogoClient ([gogonet.gogo6.com](http://gogonet.gogo6.com))
- Enable a dual stack host to gain IPv6 connectivity via IPv4 Internet
- Web-based and client-based

# Tunnel Broker Interaction



# A look at tunnel broker



The screenshot shows the 'gogoCLIENT Utility' window with the 'Status' tab selected. The 'Connection Status' section displays the following information:

Virtual Tunneling Adapter:	區域連線 2
Tunnel Mode:	IPv6-in-UDP-IPv4 Tunnel (NAT Traversal)
Local Endpoint Addresses:	219.77.9.221
Remote Endpoint Addresses:	202.169.175.22
Server Address:	anon-taipei.freenet6.net
Delegated Prefix:	(none)
Delegated User Domain:	(none)
Tunnel Status:	Connected
Tunnel Duration:	1m33s
Last Error:	(none)

The 'Activity' section shows a packet flow diagram with 'Sent' (6) and 'Received' (13) counts.

At the bottom, a diagram shows the connection path: i3way-7519179a1 → gogoSERVER → Internet.

The 'Tunnel Details' page shows the following information:

- Account:** [Redacted] [Delete Tunnel](#)
- Tunnel ID:** [Redacted]
- Description:** [Redacted]
- Registration Date:** Tue, Mar 15, 2011

**IPv6 Tunnel Endpoints**

Server IPv4 address:	216.86.86.86
Server IPv6 address:	2001:470:0:0:0:0:0:1/64
Client IPv4 address:	219.77.9.221
Client IPv6 address:	2001:470:0:0:0:0:0:2/64

**Available DNS Resolvers**

Anycasted IPv6 Caching Nameserver:	2001:470:20::2
Anycasted IPv4 Caching Nameserver:	74.82.42.42

**Routed IPv6 Prefixes and rDNS Delegations**

Routed /48:	2001:470:0:0:0:0:0:1/48
Routed /64:	2001:470:0:0:0:0:0:1/64
RDNS Delegation NS1:	none
RDNS Delegation NS2:	none
RDNS Delegation NS3:	none
RDNS Delegation NS4:	none
RDNS Delegation NS5:	none

**Example IPv6 Tunnel Configurations by OS (Windows, Linux, etc.):**

Linux-route2 [Show Config](#)

The configurations provided are only example configurations and may be different depending on the version OS or tools you are using. If you have any issues getting your tunnel to work please contact us at [ipv6@he.net](mailto:ipv6@he.net) and we will be happy to assist you.

Gogoclient

# Security strength and weakness due to large address space

---

## Pros

- Network scanning from Internet difficult
- IPv6 worms hard to propagate
- A hosting web server can support multiple digital certificates (IP-based virtual hosting)

## Cons

- Hard to build anti-spam IP blacklist system

# IPv6 and Email Spam

---

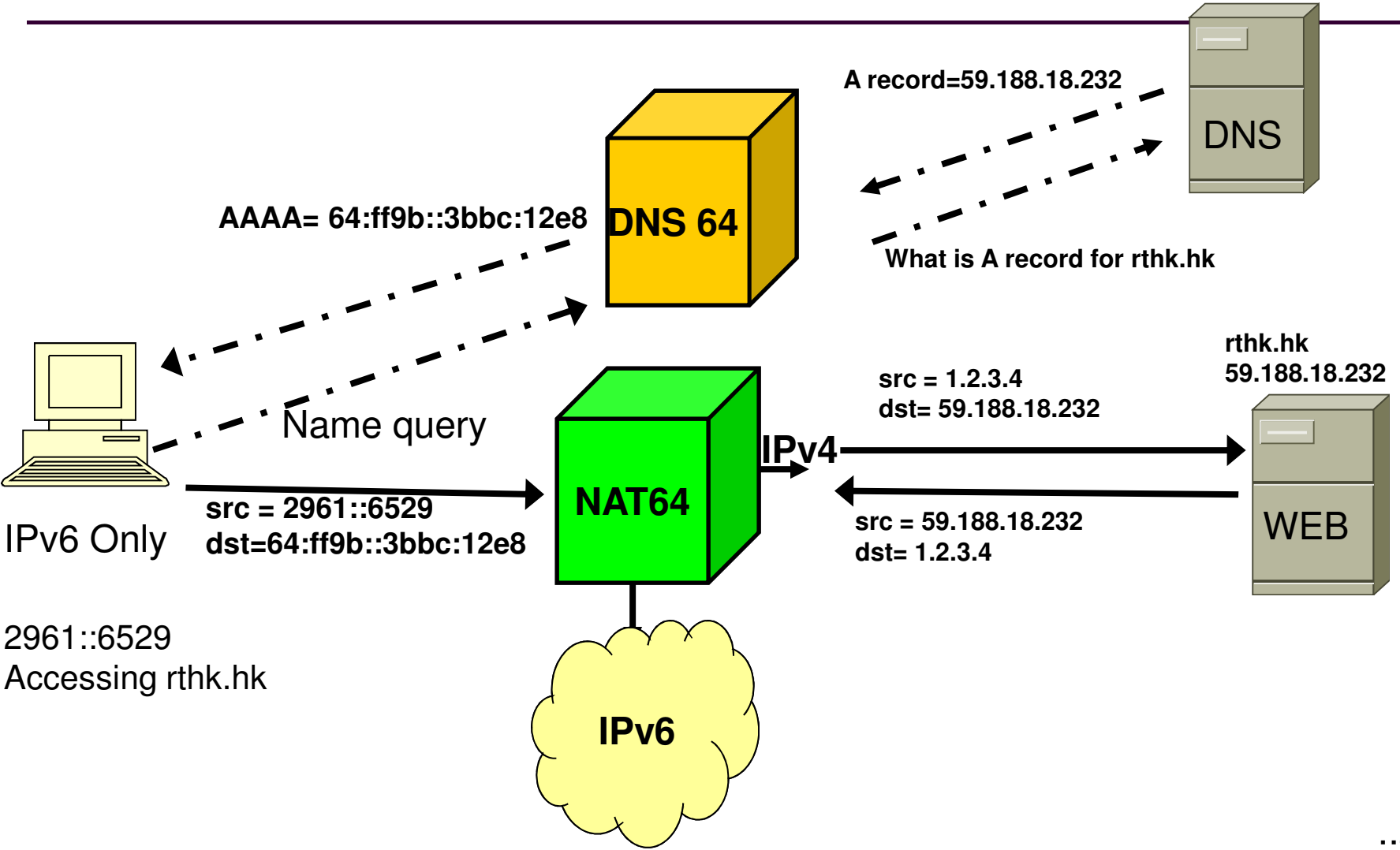
## Issue

- Spamming hosts/servers can change IPv6 addresses every second
- IP-based Blacklists Systems not effective

## Remedy

- SMTP uses mandatory reverse lookup
- Greylisting
- Use Content Filter Anti-spam Engine
- banning on a /64 subnet basis

# DNS64 + NAT64 for IPv6 only network



# A look at DNS64

```
C:\Windows\system32\cmd.exe - nslookup
名稱:      www.facebook.com
Addresses: 64:ff9b::42dc:932c
           66.220.147.44

> www.aol.com
伺服器:    UnKnown
Address:   2001:df9:105::1

未經授權的回答:
名稱:      www-west.aol.com.aol.akadns.net
Addresses: 64:ff9b::cfc8:6f01
           207.200.111.1
Aliases:   www.aol.com
           www.aol.com.aol.akadns.net

> www.cnn.com
伺服器:    UnKnown
Address:   2001:df9:105::1

未經授權的回答:
名稱:      www.cnn.com
Addresses: 64:ff9b::9da6:e019
           64:ff9b::9da6:e219
           64:ff9b::9da6:e21a
           64:ff9b::9da6:ff12
           64:ff9b::9da6:ff13
           157.166.224.26
           157.166.226.25
           157.166.226.26
           157.166.255.18
           157.166.255.19
           157.166.224.25
```

## www.cnn.com

A record	AAAA record
157.166.224.26	64:ff9b::9da6:e01a
157.166.226.25	64:ff9b::9da6:e219

# Phased Implementation Approach

---

- Buy new IPv6 ready equipment in system replacement exercise or upgrading
- Order dual-stack link for capacity expansion
- Adopt dual stack approach as far as possible
- Source suitable firewall or upgrade existing one
- Enable IPv6 on all public facing servers first (Web, Email and name servers)
- Enable IPv6 in Intranet when all internal hosts are running Win7, Win2008 and Linux etc)
- A phased approach reduce complexity
- Training of network administrators on IPv6

# IPv6 has come and will grow fast

---

- IPv6 is our present and future
- IPv6 solves many problems of IPv4
- IPv6 has been deployed in large scale commercial networks (Verizon LTE)
- No more excuse of chicken and egg
- The Internet can not be converted to IPv6 overnight, but all stakeholders must take action now
- Do IPv6 NOT for us, for the future of our kids !

# IPv6 – the future of our kids

---

[http://www.youtube.com/watch?v=2CvbMZlgBU0&feature=player\\_embedded#at=18](http://www.youtube.com/watch?v=2CvbMZlgBU0&feature=player_embedded#at=18)



::2a



*The Internet is for Everyone.*  
*Become an ISOC Member. [www.isoc.hk](http://www.isoc.hk)*

---

**Thank You !**  
**[www.isoc.hk](http://www.isoc.hk)**