IPv6協定與轉換機制介紹

課程大綱

- IPv6協定與轉換機制介紹
  - IPv6 Addressing
  - IPv6 Header Format
  - IPv6 Core Protocols
    - ICMPv6
    - Neighbor Discovery (ND)
  - IPv6 Routing
  - 轉換機制
    - IPv6/IPv4 雙IP機制(Dual Stack)
    - 通道機制(Tunneling)
    - 位址協定轉換機制(Translator)

IPv6定址

IPv6 位址表示法 (native)

- IPv6使用128Bit的位址空間，也就是最高可有2^128的位址空間，以16進位(2^4)表示，可寫成32組十六進位數字
- 如二進位0010在十六進位中即為2
- 0010 0000 0000 0011 即為2003
- 用以下位址為例
- 20030000000000B30000000000001234 (太長容易記錯)
- >2003:0000:0000:00B3:0000:0000:0000:1234(分為八段，以冒號分隔)
- >2003:0:0:B3::1234(簡寫)
- 簡寫規則:
  - 每16Bits如開頭之4bit表示為0，即可省略
  - 若16Bits全為0，則可簡寫為0
  - 若連續完整之16Bits段落皆為0000，則可全省略，簡寫為::，但以一次為限

IPv6位址表示法(IPv4 Embedded)

- **IPv6 Address 可使用IPv4位址作為其位址的末32bit**

例如:

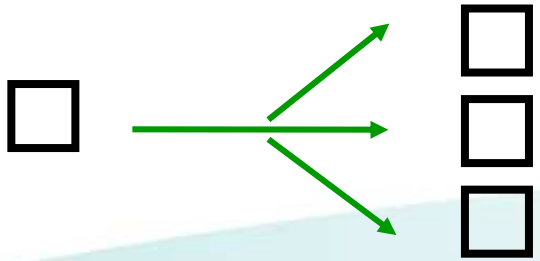
1. **2003:0:0:B3::192.168.0.1=2003:0:0:B3::C0A8:1**
2. **2003:0:0:B3:0:ffff:172.16.0.1**
3. **2003:0:0:B3:0:5efe:10.10.0.1**

注意，**IPv4**部份用句點分隔，以十進位表示， **IPv6**部份用冒號分隔，以十六進位表示。

Basic Address Types

- Unicast (點對點傳輸)
  - Address of a single interface
  - Delivery to single interface
  - for one-to-one communication

- Multicast (群播傳輸)
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
  - for one-to-many communication

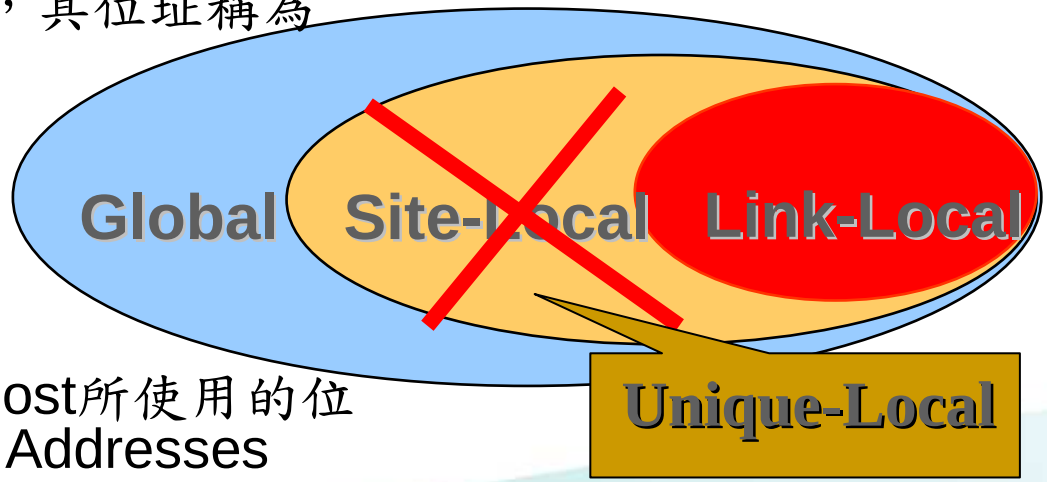


- Anycast (多點備援傳輸，運作機制尚在制定中)
  - Address of a set of interfaces
  - Delivery to a single interface in the set
  - for one-to-nearest communication
  - Nearest is defined as being closest in term of routing distance

Unicast Address Scoping

- Global Scope:

可在Internet上互連之位址空間，其位址稱為Global Unicast Addresses



- Link Local Scope:

所有在同一個Layer2網路下的Host所使用的位址空間，其位址稱為Link-Local Addresses

- Unique-Local Scope (類似IPv4的Private Address) :

所有在一個網路管理機制下之私用網路位址空間，其位址稱為 Unique-Local Addresses

Unicast Address Structure

2003:0:0:B3::1234/64

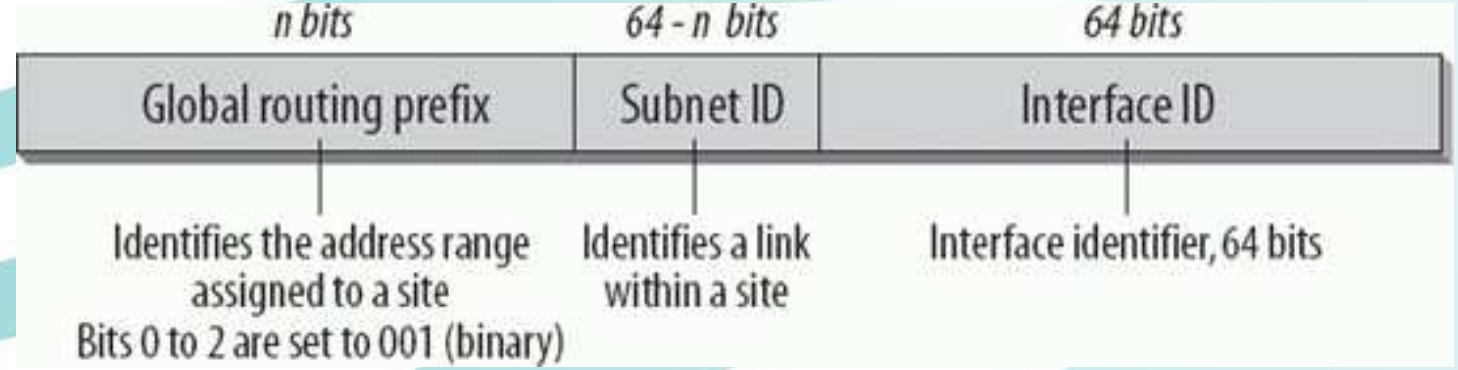
網路位址部份 **2003:0:0:B3**

Interface 位址部份: 非簡寫樣式 **:0:0:0:1234**

簡寫樣式 **::1234**

Network位址基本上由網路設備發送

Interface位址基本上由**Host**端決定



Network ID 設定與配送機制

1. 採用**Neighbor Discovery (ND)**，播放**Router Advertisement**
2. **DHCPv6 – Prefix-Delegation**
3. 手動設定
4. **Tunnel Server** 系統自動產生或指定 **(IPv4**下**)**
5. **VPN Server (IPv4 and/or IPv6)**

IPv6 Prefix 表示法

- CIDR方式

IPv6完全使用 /X 取代IPv4 Subnet mask之表示方式 X 可由0至127
例如:
1. 2003:1234:3344::34ff:2314/64 代表了Network ID部份為 64bit
2. 2003:1234:3344::34ff:2314/60 代表了Network ID的部份為60bit
3. 2003:1234:3344::34ff:2314/127 代表了Network ID的部份為127bit

於2003:1234:3344::34ff:2314/127中有更多的意義:
其中Network ID 部份為2003:1234:3344::34ff:2314
此網段僅包含了兩個Host，與IPv4不同的是這兩個Host皆可使用，如
2003:1234:3344::34ff:2314/127 與2003:1234:3344::34ff:2315/127

Interface ID 產生方式

1. 採用modified EUI-64 演算法，經由MAC Address計算出Interface 位址
2. 作業系統自動產生隨機位址
3. 手動設定
4. Tunnel Server系統自動產生或指定
5. 經由加密機制產生之虛擬位址(IPv6 IPSec)
6. DHCPv6伺服器指定(Stateful)

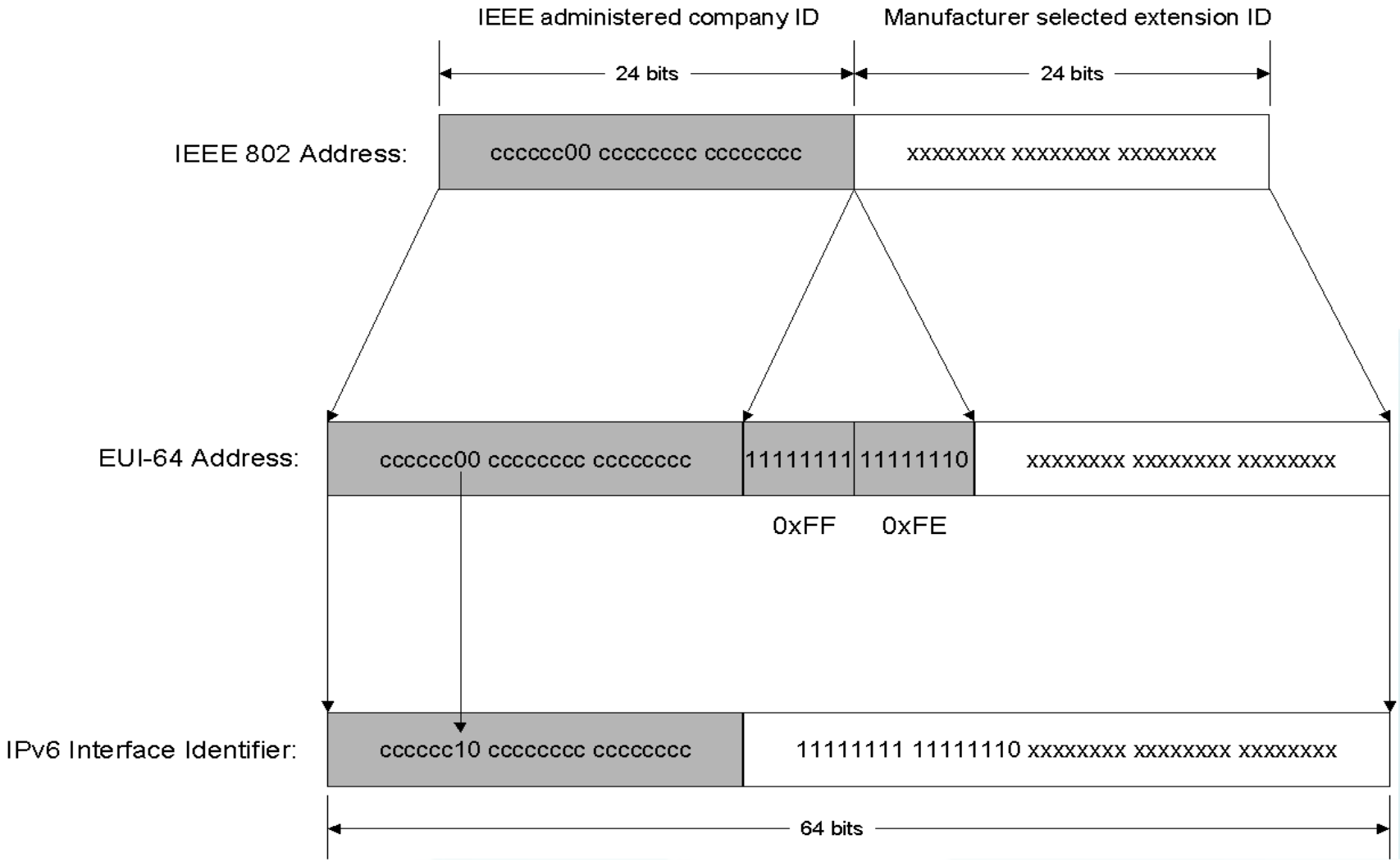
由MAC Address 產生Interface ID

1. First three octets of MAC is Company-ID
2. Last three octets of MAC is Node-ID
3. 將 FFFE置入Company ID與Node-ID間
4. Company ID 2進位表示法之第7碼為Univeral/Local-Bit，設為1表示Global Scope

如: MAC Address為 00-C0-3F-BB-93-91，則

1. Company ID 為00-C0-3F, Node ID為BB-93-91
2. 00-C0-3F-FF-FE-BB-93-91
3. Company ID 2進位表示法為00000000 11000000 00111111
4. 將第7bit改為1，為00000010 11000000 001111111
5. 重組為02-C0-3F
6. Interface ID為 2C0:3FFF:FEBB:9391

The conversion of a universally administered, unicast IEEE 802 address to an IPv6 interface identifier



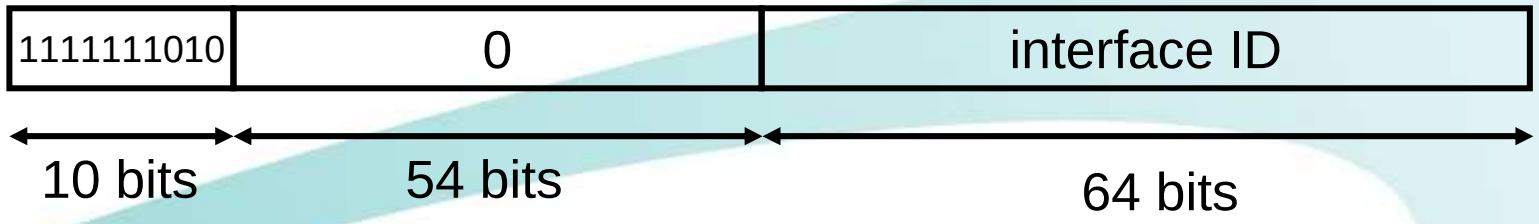
Global Unicast Address 分配表

Allocation	Prefix binary	Prefix hex	Fraction of address space
Unassigned	0000 0000	::0/8	1/256
Reserved	0000 001		1/128
Global unicast	001	2000::/3	1/8
Link-local unicast	1111 1110 10	FE80::/10	1/1024
Reserved (formely Site-local unicast)	1111 1110 11	FEC0::/10* * deprecated	1/1024
Local IPv6 address	1111 110	FC00::/7	
Private administration	1111 1101	FD00::/8	
Multicast	1111 1111	FF00::/8	1/256

The updated list of address allocations can be found at: http://www.iana.org/assignments/ipv6-address-space.

Link-Local Address

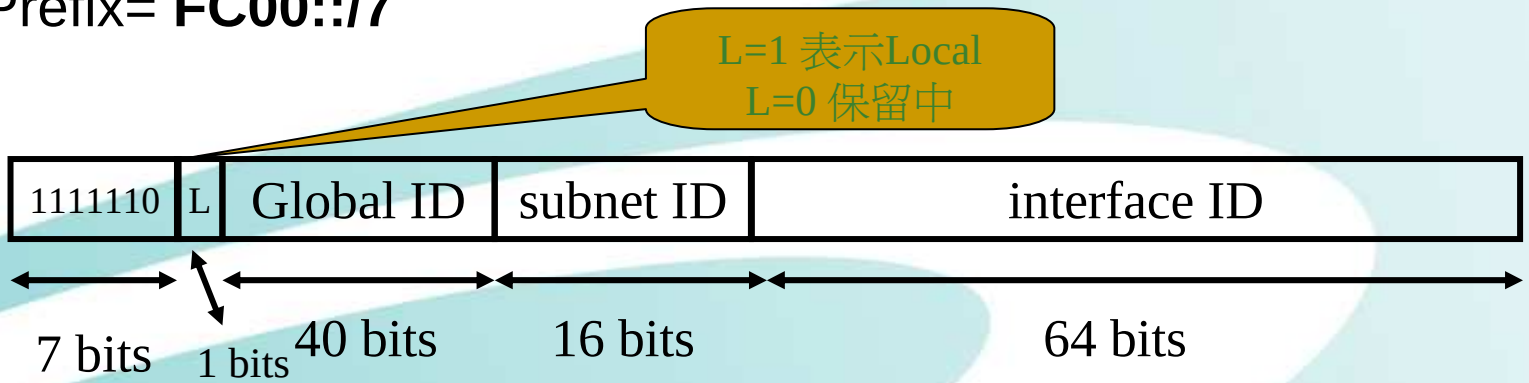
- Meaningful only in a single link zone, and may be re-used on other links
- Link-local addresses for use during auto-configuration and when no routers are present
- Required for Neighbor Discovery process, always automatically configuration
- An IPv6 router never forwards link-local traffic beyond the link
- Prefix= **FE80::/64**



引用自TWNIC IPv6技術理論與實務研習班講義

Unique-Local Address

- meaningful only in a single site zone, and can not be re-used in other sites
- Equivalent to the IPv4 private address space
- Replace Site-Local Addresses
- L identifies the assignment policy. Only value 1 (FD00::/8) is currently in use designating a local assignment*
- Global ID is a 40-bit identifier that ensures the global uniqueness of the address. It is generated pseudo-randomly and must not be sequential. Because ULAs should not be globally routed, they do not need to be aggregated, so sequential global IDs are not necessary *
- Prefix= **FC00::/7**



*引用自Deploying IPv6 Network, Cisco Press 2006

IPv6 Multicast Addresses

- Multicast address can not be used as source or as intermediate destination in a Routing header
- Flag field 0RPT 4bits
  - The low-order Transient(T) flag indicates permanent (T=0) / transient(T=1) group
  - The P bit is defined in RFC 3306, and it indicates whether the multicast address is built based on a unicast prefix (set to 1) or not (set to 0).
  - The R bit defined in RFC 3956, if set to 1, indicates that the multicast group address contains the unicast address of the RP servicing that group.
- Scope field
  - 0: reserved
  - 1: Interface-Local
  - 2: Link-Local
  - 3: reserved
  - 4: Admin-Local Scope
  - 5: Site-Local
  - 8: Organization-Local
  - E: Global
  - Others: reserved

FF02::/16 表示為Multicast 位址區段，Flag標示此為永久group ID，不使用unicast prefix也不包含RP資訊，其Scope為link-local

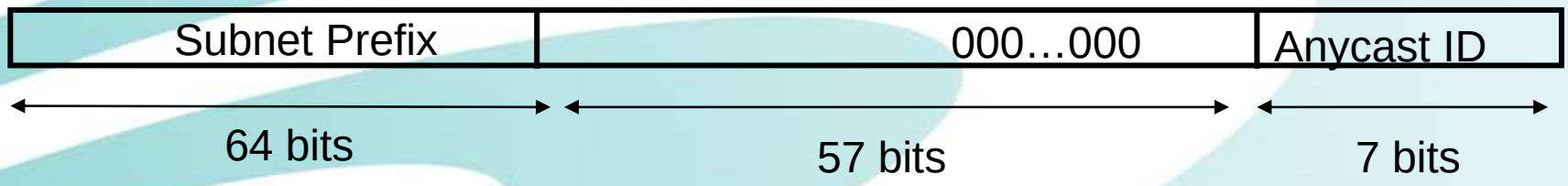
IPv6 Well-known multicast addresses

IPv6 Well-known multicast address	IPv4 Well-known multicast address	Multicast Group
Node-local scope		
FF01:0:0:0:0:0:0:1	224.0.0.1	All-nodes address
FF01:0:0:0:0:0:0:2	224.0.0.2	All-routers address
Link-local scope		
FF02:0:0:0:0:0:0:1	224.0.0.1	All-nodes address
FF02:0:0:0:0:0:0:2	224.0.0.2	All-routers address
FF02:0:0:0:0:0:0:5	224.0.0.5	OSPFIGP
FF02:0:0:0:0:0:0:6	224.0.0.6	OSPFIGP-DR‘s
FF02:0:0:0:0:0:0:9	224.0.0.9	RIP routers
FF02:0:0:0:0:0:0:D	224.0.0.13	All PIM routers
Site-local scope		
FF05:0:0:0:0:0:0:2	224.0.0.2	All-routers address
Any valid scope		
FF0X:0:0:0:0:0:0:101	224.0.1.1	Network time protocol NTP

IPv6 Anycast Address

- Assigned to multiple interface
- Only used as destination address
- Only assigned to router
- anycast addresses are indistinguishable from unicast
- Subnet-router anycast address is predefined and required
- IPv6 reserved anycast address for future use
- Anycast ID: 0-125, 127(00-7D, 7F)為保留數值
- Anycast ID:126 (7E)，目前訂為Mobile IPv6 home agent's anycast addresses

Unicast Address with EUI-64 Interface ID (保留給未來全球公認之Anycast服務使用)



RFC 5156 SPECIAL-USE Addresses

- **Unspecified address(0:0:0:0:0:0:0:0 or ::)**
  - **Indicate the absence of an address**
  - **Equivalent to IPv4 0.0.0.0**
  - **Never assigned to an interface or used as a destination address**
- **Loopback address (0:0:0:0:0:0:0:1 or ::1) 相當於 IPv4 127.0.0.1**
  - **Identify a loopback interface**
- **IPv4-compatible address (0:0:0:0:0:0:w.c.x.z or ::w.c.x.z) (不再使用)**
  - **Used by dual-stack nodes**
  - **IPv6 traffic is automatically encapsulated with an IPv4 header and send to the destination using the IPv4 infrastructure**
- **IPv4 mapped address (0:0:0:0:0:FFFF:w.c.x.z or ::FFFF:w.c.x.z)**
  - **Represent an IPv4-only node to an IPv6 node**
  - **Never used as a source or destination address of IPv6 packet**

IPv6位址分配政策摘要

- RIR所配發的最小位址空間為/32。
- (3)　Utilization Metric

$$\text{HD-Ratio} = \frac{\text{Log (number of allocated objects)}}{\text{Log (maximum number of allocable objects)}}$$

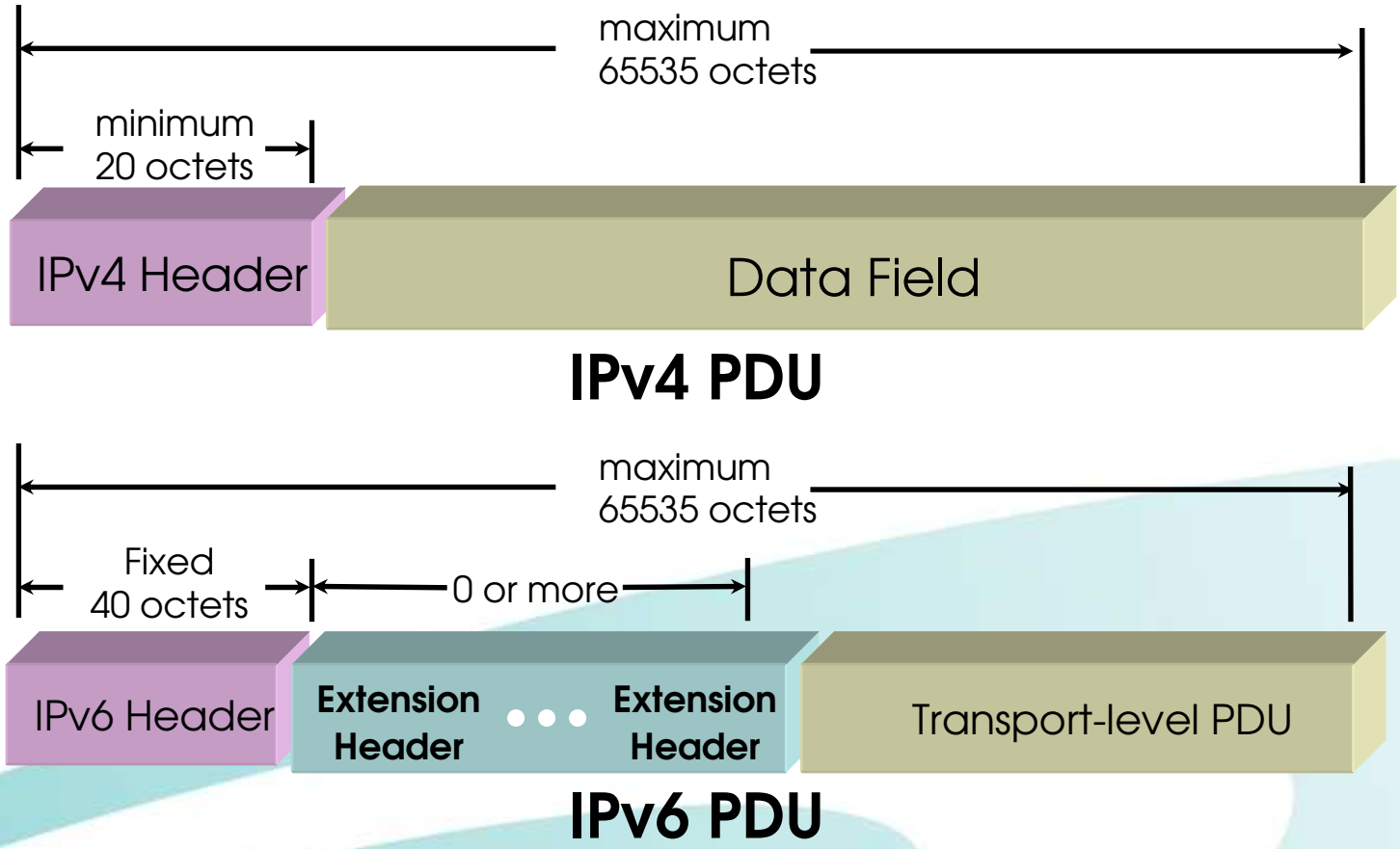
- 其中objects指的是長度為/56的IPv6位址空間。當HD-Ratio大於0.94時，即可提出增加位址配發的需求。
- LIR/ISP配發IPv6位址空間給end user的基本原則
  - /64：申請單位只需要使用唯一一個 (one and only one) subnet時，可給予申請單位::/64位址空間。
  - /56：一般情形下給予申請單位::/56位址空間。

IPv4 Addresses and IPv6 Equivalents

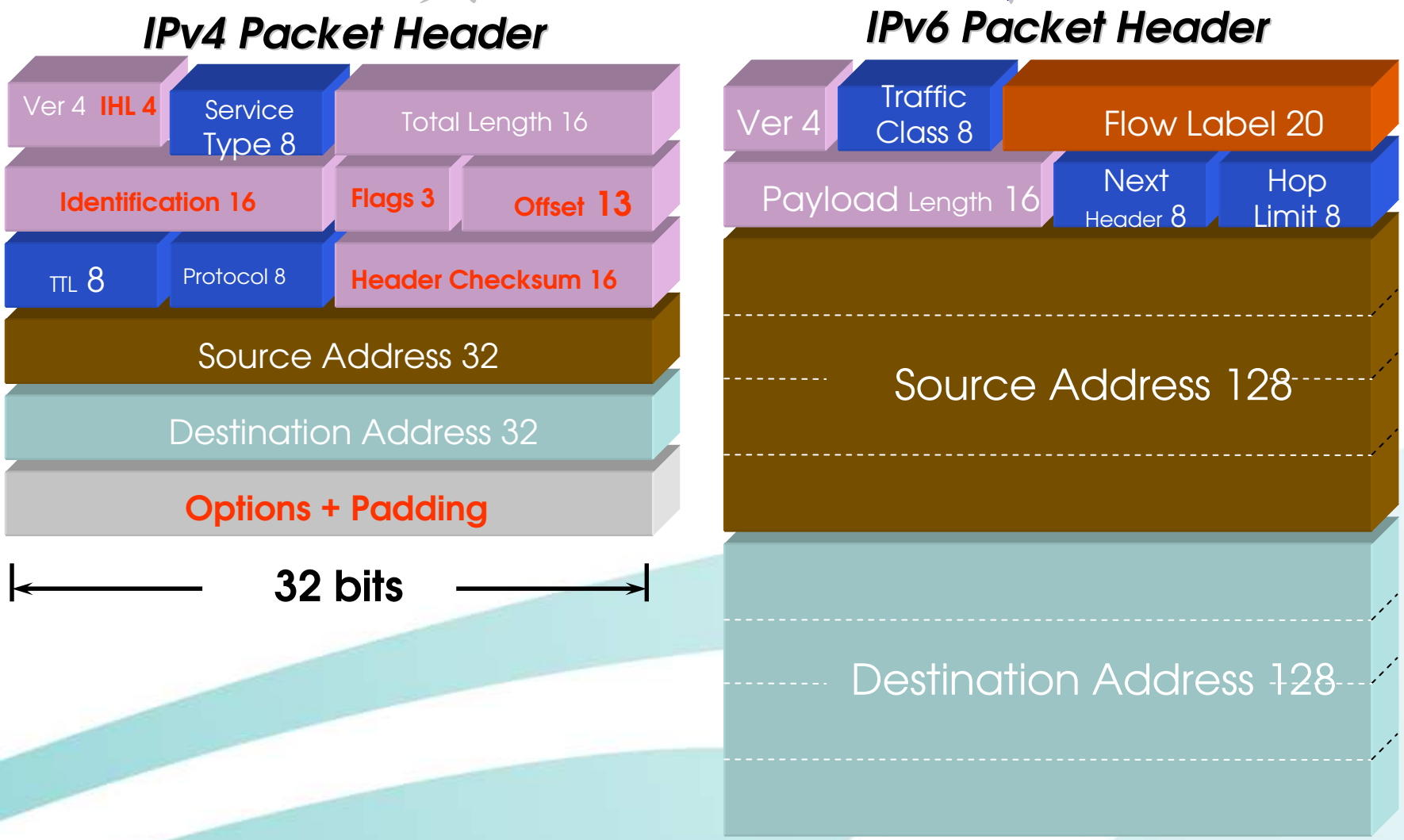
IPv4 Address	IPv6 Address
Internet address classes	N/A
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	N/A
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Aggregatable global unicast addresses
Private IP addresses	Site-local addresses (FEC0::/48)
APIPA addresses	Link-local addresses (FE80::/64)
Dotted decimal notation	Colon hexadecimal format
Subnet mask or prefix length	Prefix length notation only

The IPv6 Header

IPv6 vs. IPv4 Packet Data Unit



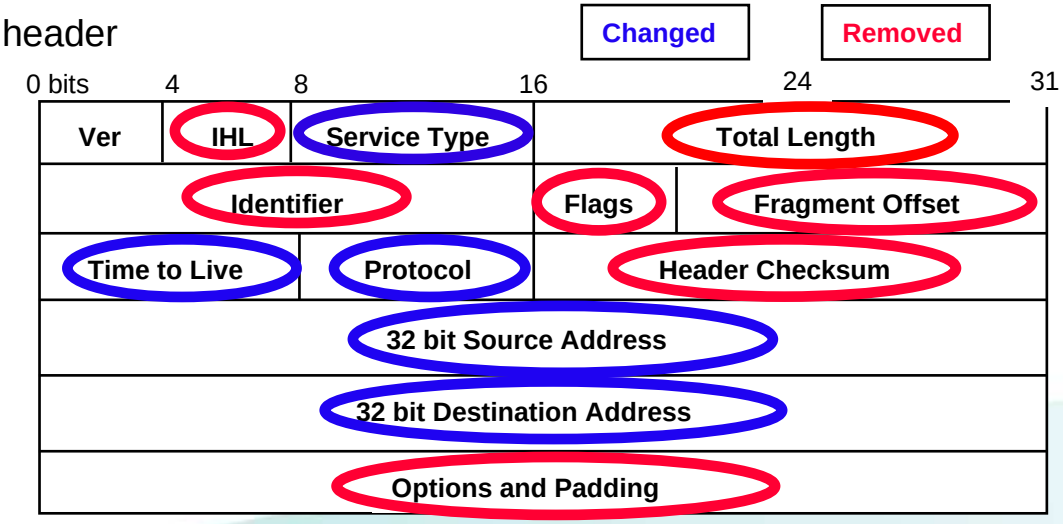
IPv6 Header與IPv4 Header 比較



引用自TWNIC IPv6技術理論與實務研習班講義

IPv4與IPv6 Header之差異

- Streamlined (六個欄位被移除)
  - Fragmentation fields moved out of base header
  - IP options moved out of base header
  - Header Checksum eliminated
  - Header Length field eliminated
  - Length field excludes IPv6 header
  - Alignment changed from 32 to 64 bits
- Revised (三個欄位被重新命名)
  - Time to Live → Hop Limit
  - Protocol → Next Header
  - Precedence & TOS → Traffic Class
  - Addresses increased 32 bits → 128 bits
- Extended (新增一個欄位)
  - Flow Label field added



*引用自Introduction to IPv6, Cisco 2001

IPv4 vs. IPv6 header

- 相同的部分

IPv4 header	IPv6 header	功能
Version	Version	IP的版本
Traffic class	Type of service	區別具有不同優先權的封包
Payload length	Payload length	header後面成載資料的長度
Protocol type	Next header	下一個header的協定號碼
Time to live	Hop limit	封包可以存活在網路上的時間

IPv4 vs. IPv6 header

- 增減的部分

IPv4 header	IPv6 header	增減的原因
IHL		有Payload length就足夠了, 因為IPv6 header長度固定
Identifier, flags, offsets		Fragment extension header 處理分割封包的動作
checksum		減少計算所花的時間和系統資源
	Flow label	用flow來標示需同處理連續的封包, 更有效率

IPv6 extension header

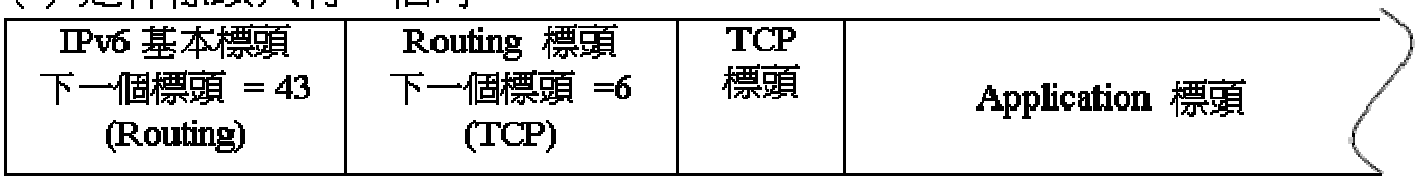
IPv6 PDU general form

- Hop-by-hop options header
  - 用於指定到目的的路徑上每個躍點處的參數
- Routing header
  - IPv6 來源節點可以使用 Routing 擴充標頭指定來源路由，它是封包通往最終目的主機的路徑上通過的中間目的主機的清單
- Fragment header
  - 用於 IPv6 分段以及重新組裝服務
- Authentication header
  - 為 IPv6 封包提供資料驗證 (對傳送該封包的節點進行驗證)、資料完整性 (確認傳輸程序中資料沒有被修改) 以及防重播保護 (確保擷取的封包不被重新傳閱並接受為有效的資料)
- Encapsulating security payload header
  - 標頭和標尾為壓縮的 payload 提供資料保密性、資料驗證和資料完整性服務
- Destination options header
  - 用於指定中間目的或最終目的主機的封包傳輸參數

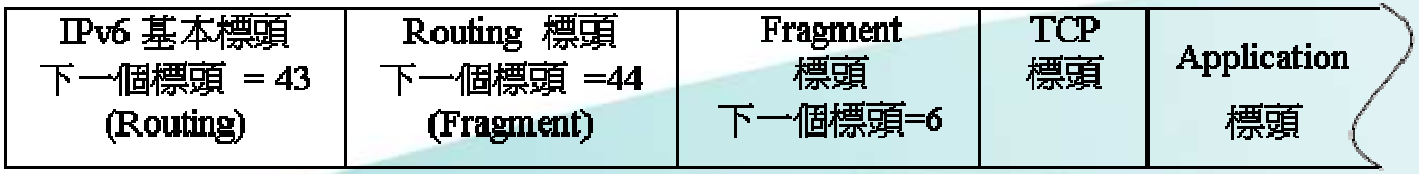
IPv6 封包延伸標頭的例子

(1) 沒有延伸標頭時

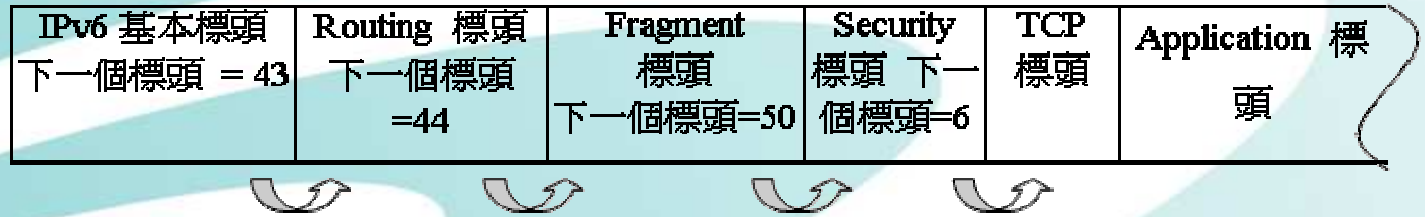
(2) 延伸標頭只有一個時



(3) 延伸標頭只有兩個時

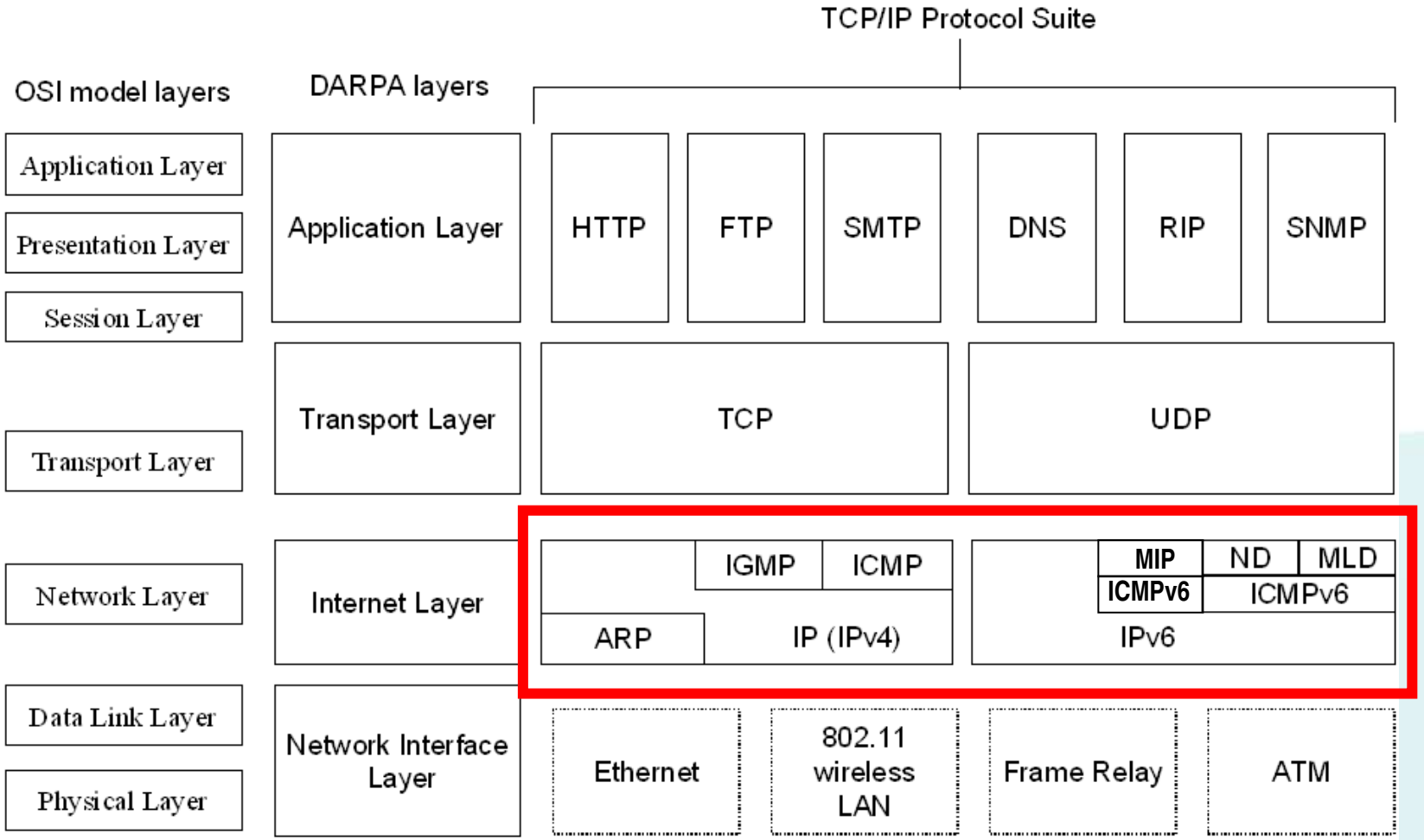


(4) 延伸標頭只有三個時



IPv6 Core Protocols

Dual Stack TCP/IP Protocol Suite



引用自TCP/IP Fundamentals for Microsoft Windows Chapter 2

IPv6 Core Protocols

- 為核心之通訊協定，缺少一項機制，IPv6就無法運作

Core Protocols		說明
IPv6	**於IPv4的類似機制**	雖然可在IPv4找出類似的機制，但IPv6 Core Protocols的功能強大許多
IPv6	IPv4	IPv6 is a routable protocol that addresses, routes, fragments, and reassembles packets
ICMPv6	ICMP	ICMPv6 provides diagnostic functions and reports errors when IPv6 packets cannot be delivered.
ND	ARP	**ND manages interaction between neighboring nodes, including automatically configuring addresses and resolving next-hop IPv6 addresses to MAC addresses.**
MLD	IGMP	MLD manages IPv6 multicast group membership.

引用自TCP/IP Fundamentals for Microsoft Windows Chapter 2

ICMPv6 Message格式

Type [8]	Code [8]	Checksum [16]
Message Body [N*32]		

- Type
  - 表示 ICMPv6 訊息的類型。該欄位大小為 8 位元。在 ICMPv6 錯誤訊息中，高序位位元設為 0；在 ICMPv6 資訊訊息中，高序位位元設為 1。
- Code
  - 區分給定訊息類型的多個訊息。該欄位大小為 8 位元。對於給定類型，如果只有一個訊息，則 Code 欄位設為 0。
- Checksum
  - 存放 ICMP 訊息的檢查值。該欄位大小為 16 位元。計算檢查值時，將 IPv6 Pseudo header加入到 ICMPv6 訊息中。
- Message body
  - 包含 ICMPv6 訊息特有的資料。

Neighbor Discovery (ND)

- RFC 2461(→RFC 4861) (Updated by RFC4311)
- 確定相鄰節點之間關係的一組訊息和程序
- 取代IPv4中的ARP, ICMP Router Discovery, ICMP Redirect

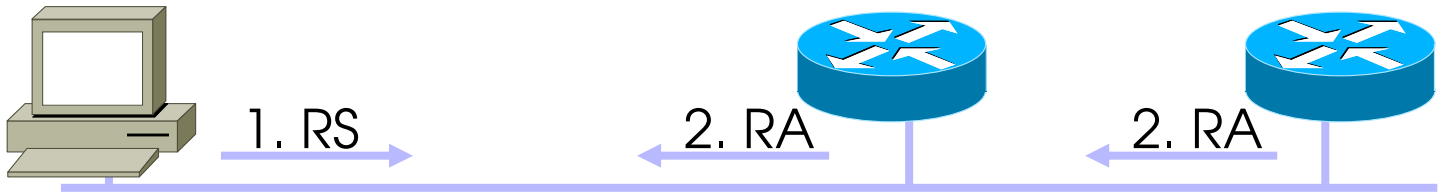
- ICMP message型態:
  - Router Solicitation (詢問Link上有無路由器存在)
  - Router Advertisement (群播Network Prefix與相關參數)
  - Neighbor Solicitation (ARP Request)
  - Neighbor Advertisement (ARP Reply)
  - Redirect

Neighbor Discovery (ND)功能

- Router Discovery
  - 主機發現相連連結上本機路由器的程序
- Prefix Discovery
  - 主機使用此程序發現本機連結目的的網路prefix
- autoconfiguration of address & other parameters
  - 自動進行IPv6位址設定
- Duplicate Address Detection (DAD)
  - 使用此程序確定要使用的位址還沒有被相鄰節點使用
- Neighbor Unreachability Detection (NUD)
  - 使用此程序確定相鄰節點的 IPv6 層不再接收封包
- Link-Layer address resolution
  - 位址解析節點使用此程序將相鄰節點的 IPv6 位址解析為其連結層位址。它相當於 IPv4 中的 ARP
- first-hop redirect
  - 有一個更好的第一躍點 IPv6 位址可以到達目的

*引用自Introduction to IPv6, Cisco 2001

ND Autoconfiguration, Prefix & Router Discovery



1. RS:

ICMP Type = 133

Src = ::

Dst = All-Routers multicast Address (FF02::2)

query= please send RA

2. RA:

ICMP Type = 134

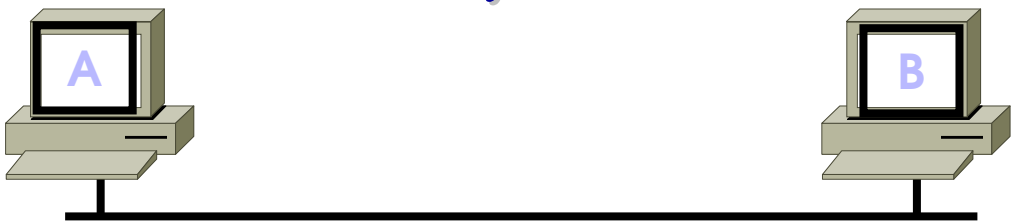
Src = Router Link-local Address

Dst = All-nodes multicast address (FF02::1)

Data= MTU, options, **prefix**, lifetime, autoconfig flag

- Router solicitation are sent by booting nodes to request RAs for configuring the interfaces.

ND Address Resolution & Neighbor Unreachability Detection

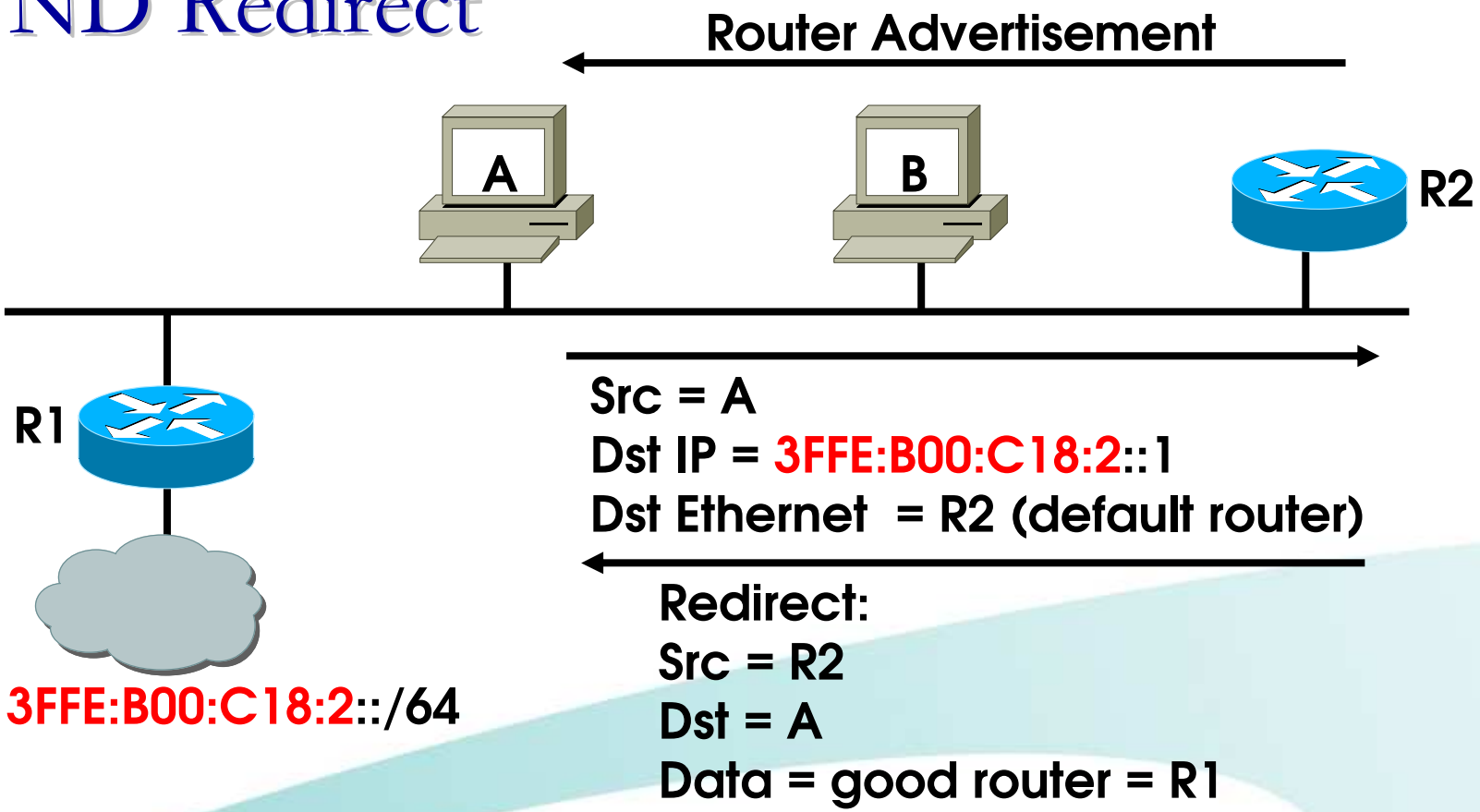


ICMP type = 135 (NS)
Src = A
Dst = Solicited-node multicast of B
Data = link-layer address of A
Query = what is your link address?

ICMP type = 136 (NA)
Src = B
Dst = A
Data = link-layer address of B

A and B can now exchange packets on this link

ND Redirect



- Redirect is used by a router to signal the reroute of a packet to an onlink host to a better router or to another host on the link

最小MTU

- Link MTU
  - 一個 link層最大的傳輸單位
- Path MTU
  - 來源到目的間所有連結層的最小MTU量測
- IPv6最小的link MTU是1280位元 (IPv4為68位元)
- IPv6 來源主機可以使用上述程序和 Fragment 標頭 將大於路徑 MTU 的上層通訊協定 payload 分段。IPv6 節點必須能夠重新組裝至少為 1500 位元組的分段封包。

Path MTU Discovery

- 傳送節點假定路徑 MTU 是轉寄通訊的介面的連結 MTU。
- 傳送節點以此路徑 MTU 的大小傳送 IP 資料電報。
- 如果路徑上的路由器無法在連結 MTU 小於某封包尺寸的連結上轉寄該封包，它就會丟棄 IPv6 封包，並將 ICMP Packet Too Big 訊息發回到傳送節點。ICMP Packet Too Big 訊息包含轉寄失敗所在連結的連結 MTU。
- 傳送節點將發向目的的封包的路徑 MTU 設定為 ICMPv6 Packet Too Big 訊息中 MTU 欄位值。

IPv6 Routing

Routing in IPv6 (1/3)

- As in IPv4, IPv6 supports IGP and EGP routing protocols:
  - IGP for within an autonomous system are
    - RIPng (RFC 2080)
    - OSPFv3 (RFC 2740)
    - Integrated IS-ISv6 (draft-ietf-isis-ipv6-07.txt)(2007/10/04)
  - EGP for peering between autonomous systems
    - MP-BGP4 (RFC 4271, RFC 4760 and RFC 2545)
- IPv6 still uses the longest-prefix match routing algorithm

Routing in IPv6 (2/3)

- RIPng
  - RIPv2, supports split-horizon with poisoned reverse
  - RFC2080
- IS-ISv6
  - Shared IGP for IPv4 & IPv6
  - Route from A to B same for IPv4 & IPv6
  - Separate SPF may provide SIN routing
- OSPFv3
  - « Ships in the Night » routing
  - Need to run OSPFv2 for IPv4
  - Route from A to B may differ for IPv4 & IPv6

Routing in IPv6 (3/3)

- BGP4+
  - Added IPv6 address-family
  - Added IPv6 transport
  - Runs within the same process - only one AS supported
  - All generic BGP functionality works as for IPv4
  - Added functionality to route-maps and prefix-lists

IPv4與IPv6比較(1/2)

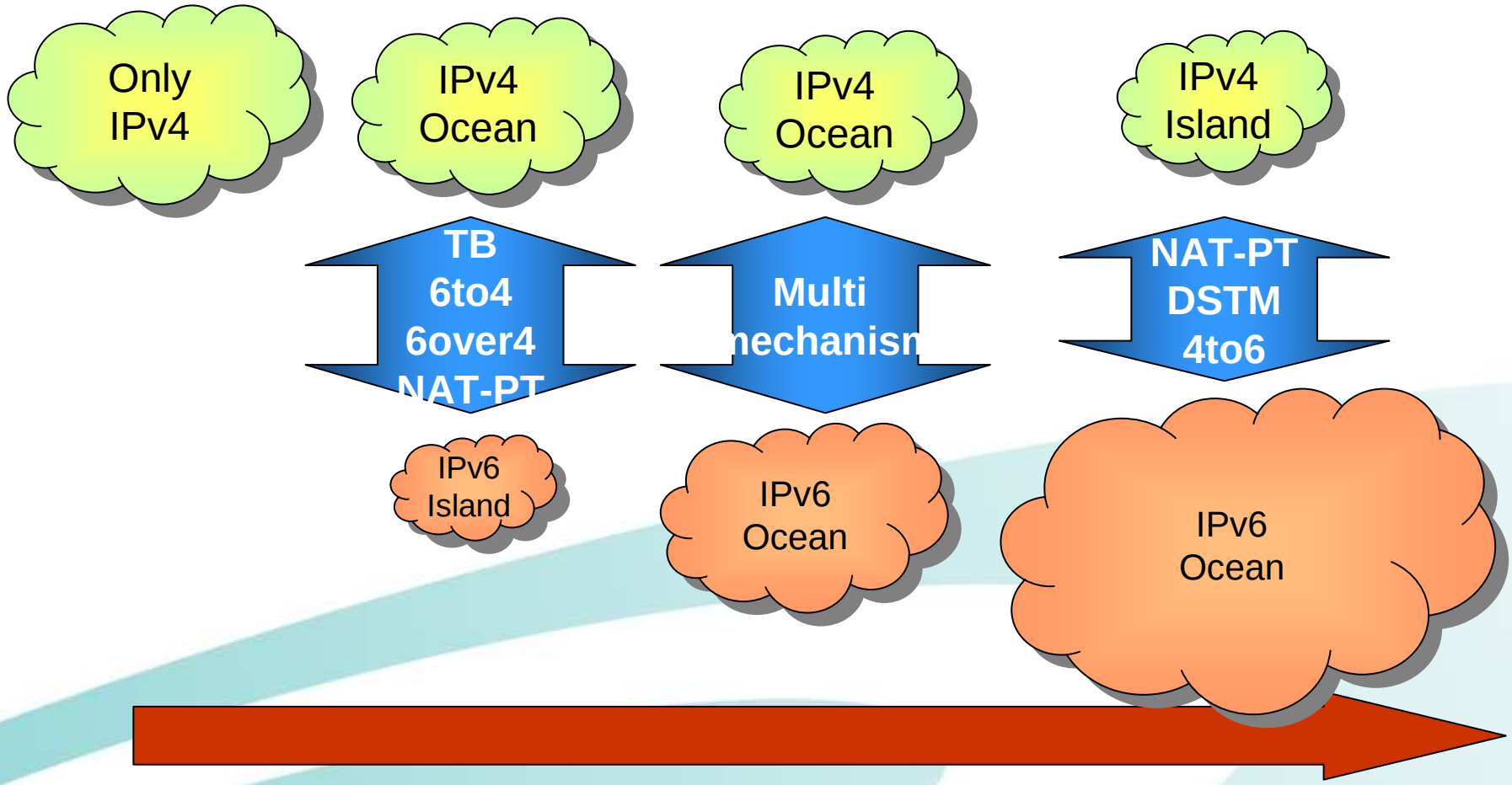
Feature	IPv4	IPv6
Source and destination address	32 bits	128 bits
IPSec	Optional	required
Payload identification for QoS in the header	No identification	Using Flow label field
Fragmentation	Both router and the sending hosts	Only supported at the sending hosts
Checksum of header	included	Not included
Resolve address to a link layer address	broadcast ARP request	Multicast Neighbor Solicitation message

IPv4與IPv6比較(2/2)

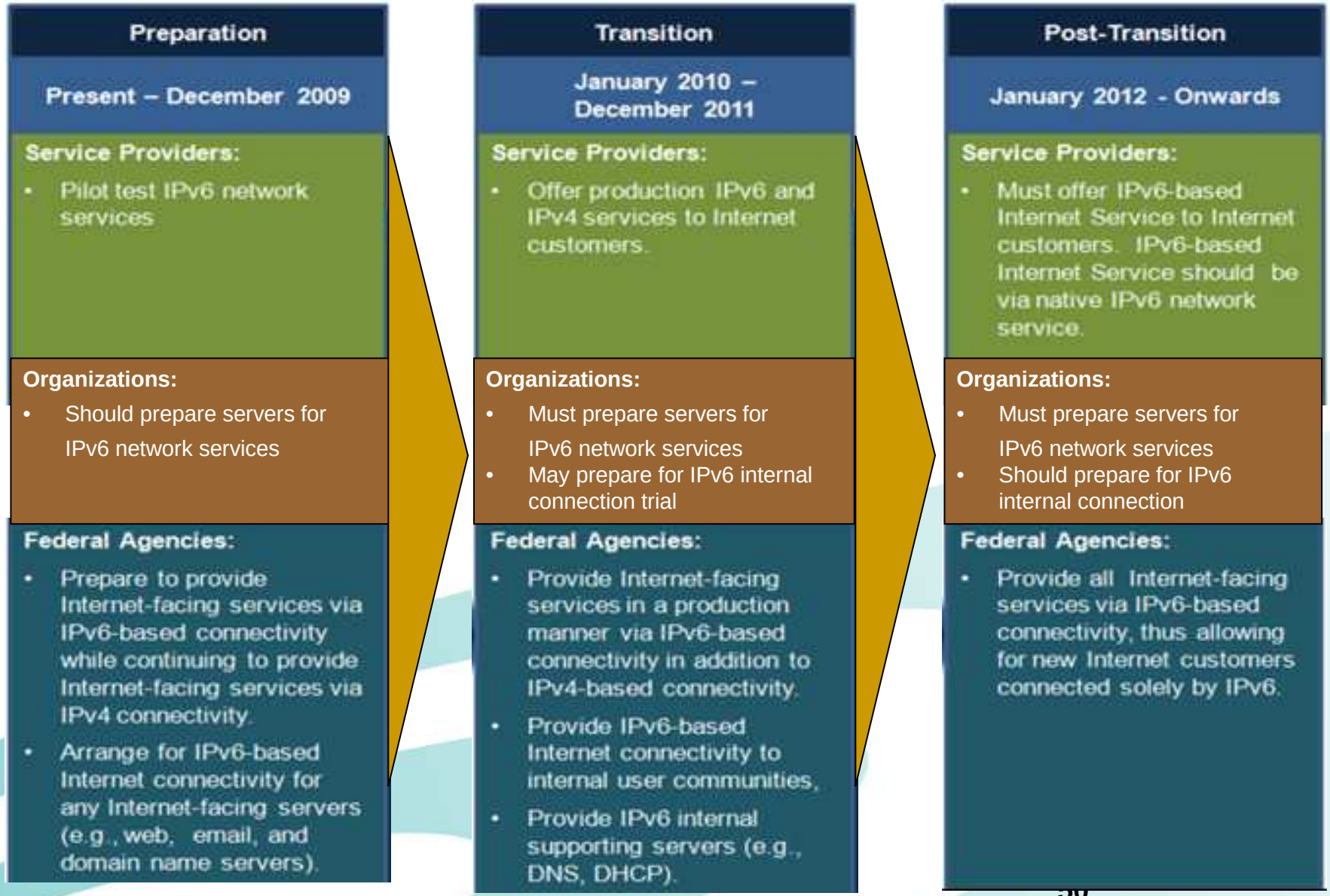
Feature	IPv4	IPv6
Determine the address of the best default gateway	ICMP Router Discovery (optional)	ICMPv6 Router Solicitation and Router Advertisement (required)
Send traffic to all nodes on a subnet	Broadcast	Link-Local scope all-nodes multicast address
Payload identification for QoS in the header	No identification	Using Flow Label field
Configure address	Manually or DHCP	Autoconfiguration/DHCPv6
Map hosts name to addresses	A	AAAA
Manage local subnet group membership	IGMP	Multicast Listener Discovery (MLD)

IPv6/IPv4 Transition 機制

Internet Transition Trend



RFC 5211 - An Internet Transition Plan

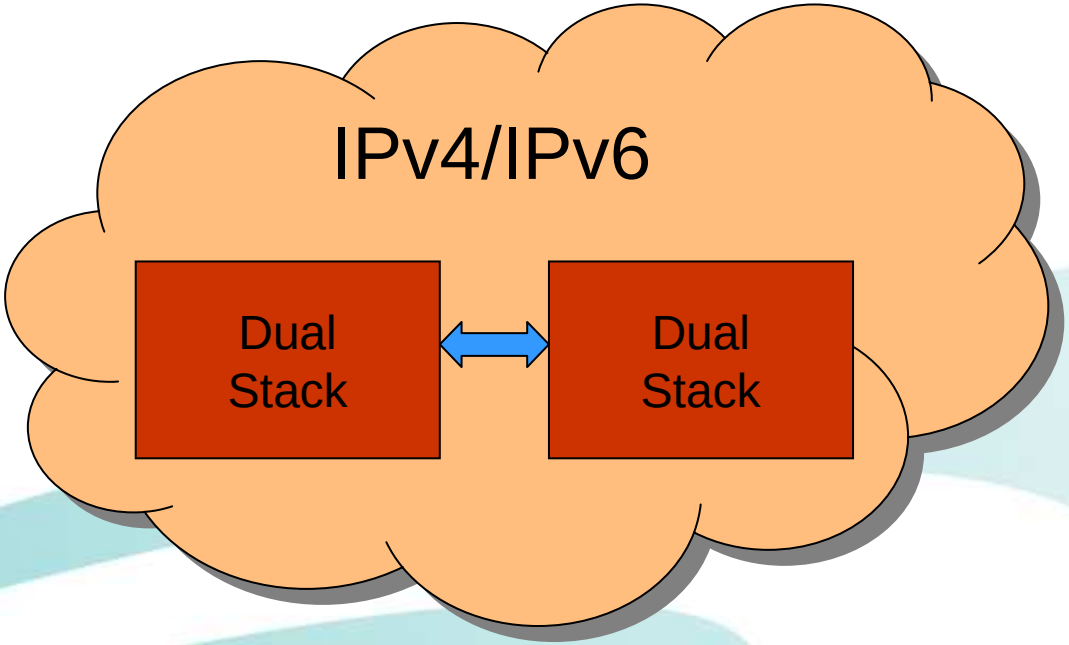


三大類過渡技術

1. IPv6/IPv4 Dual Stack (即在同一條線路上，同時提供IPv6及IPv4的通訊協定)
2. Tunneling (即在現有的兩個IPv4的端點間，建IPv6的隧道，使兩端後的使用Dual Stack作業系統的使用者能以IPv6互通)
3. Translator(理論上，透過轉換機制可讓僅支援IPv4的使用者，可與僅支援IPv6的HOST連線，並讓僅支援IPv6的使用者，與僅支援IPv4的HOST連線)

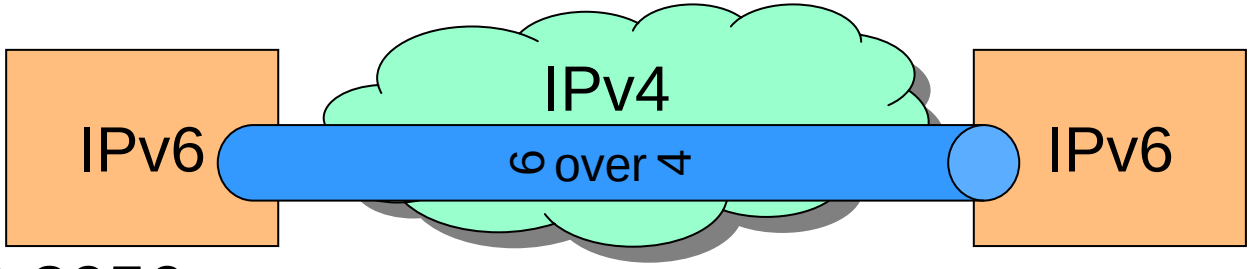
Dual Stack

- RFC 2893 -> RFC 4213

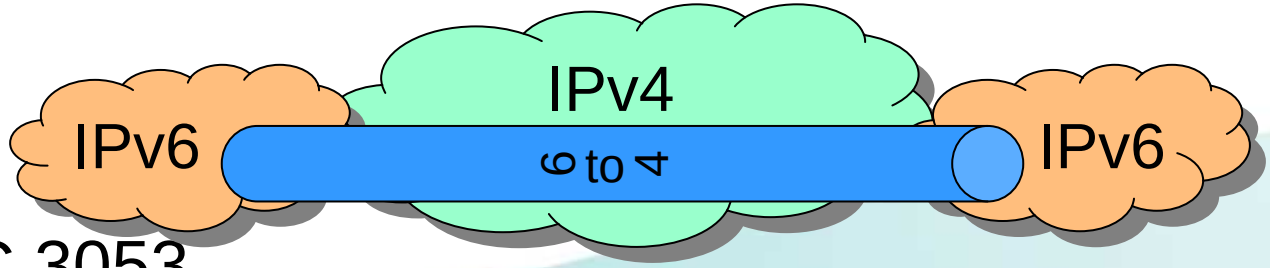


Tunneling

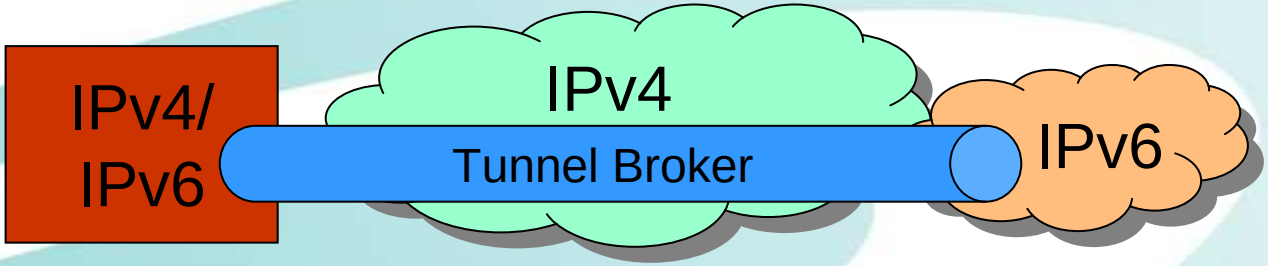
- RFC 2529



- RFC 3056

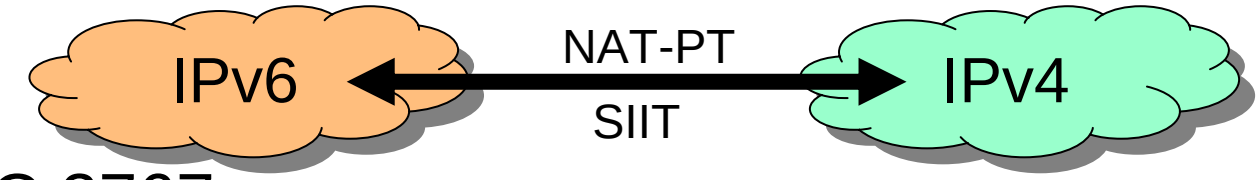


- RFC 3053



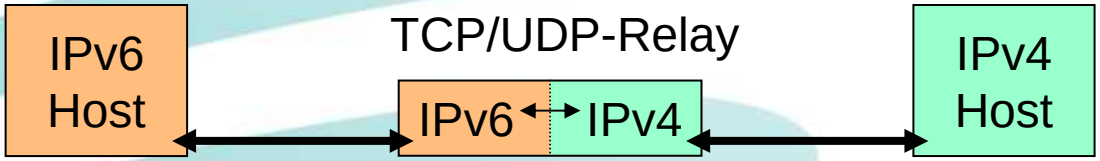
Translator

- RFC 2765；RFC 2766



- RFC 2767

- RFC 3142



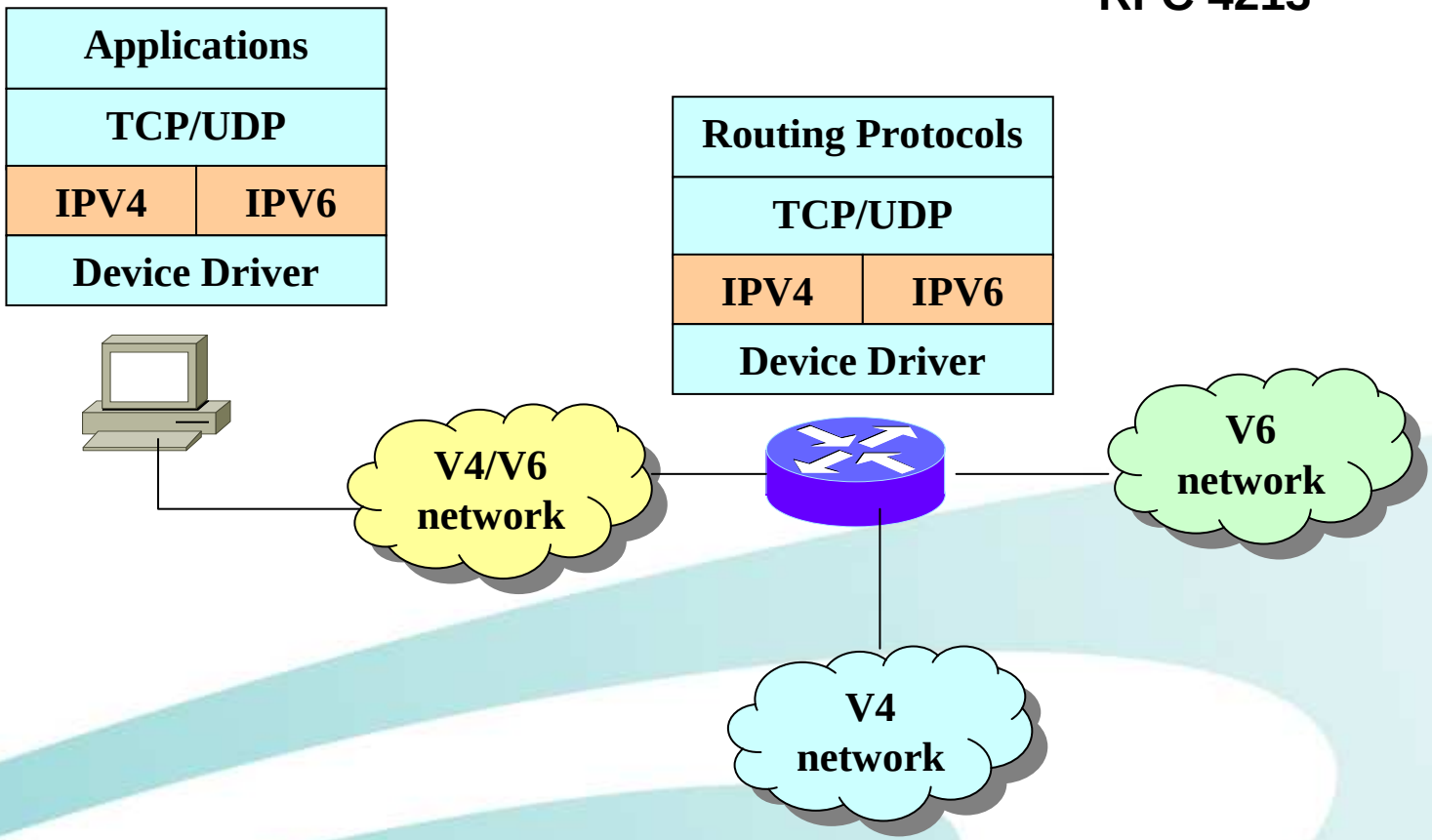
Dual Stack

Dual Stack Mechanisms (1/2)

- **Dual IP Layer Operation (dual stack)**
  - **Both IPv4 and IPv6 are directly supported**
- **IPv6/IPv4 nodes**
  - for IPv6 nodes to remain compatible with IPv4-only nodes
  - operated in one of three modes:
    - IPv4 stack enabled and IPv6 stack disabled
    - IPv6 stack enabled and IPv4 stack disabled
    - both stacks enabled.

Dual Stack Mechanisms (2/2)

RFC 4213



雙協定堆疊(Dual Stack)技術優缺點比較表

IPv4/IPv6雙協定堆疊(Dual Stack)轉移技術	
優點	缺點
容易設置與易懂。	擴展性(scalability)差。因為每個節點需1個IPv6位址及1個IPv4位址。
端點對端點連線模式未遭破壞。	系統複雜度及負擔增加，需維持2個IP協定個別的routing table及相關網管資訊。
雙堆疊主機可與其它雙協定堆疊主機、純IPv4主機或純IPv6主機互連。	無法提供純IPv4主機與純IPv6主機的互通。

通道機制 (Tunneling)

Tunneling

Tunneling分類

a. 手動
b. 全自動
   6to4, ISATAP, Teredo
a. 半自動
   Tunnel broker

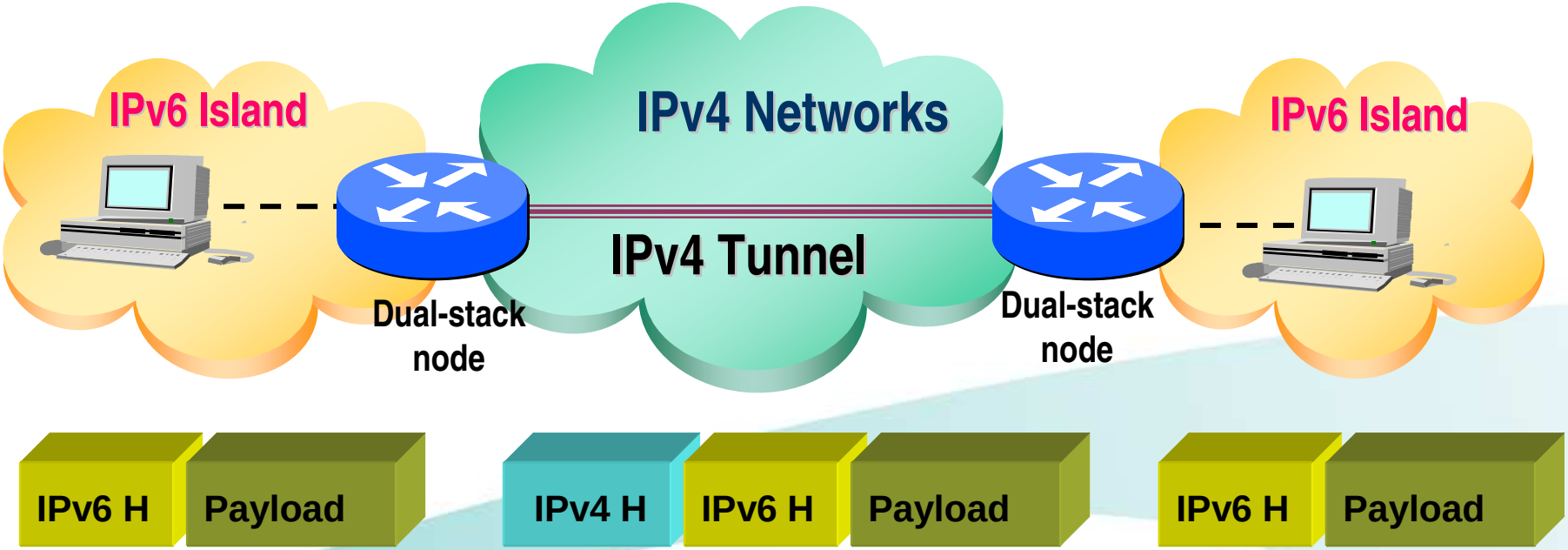
Tunnel 大致包含了下列元件

a. Tunnel Server: 提供Tunnel 服務之局端設備
b. Tunnel Client: 與Tunnel Server建立連線，並由Tunnel Server取得IPv6網址之使用者端網路設備
c. Tunnel Broker (optional for tunnel service, but required for tunnel: 用來進行Tunnel Server的認証機制，經用Tunnel Broker的管制可以僅讓有權限的Tunnel Client能夠與Tunnel Server連線

RFC 4213 - Configured Tunnel

- Mechanism to carry IPv6 packets over IPv4 infrastructure
- Encapsulate IPv6 in IPv4
- Tunnel endpoints are explicitly configured
  - All IPv6 implementations support this
- Tunnel endpoints must be dual stack nodes
  - The IPv4 address is the endpoint for the tunnel

Configured Tunnel



Connection of IPv6 Domains via IPv4 Clouds (6to4)

RFC3056

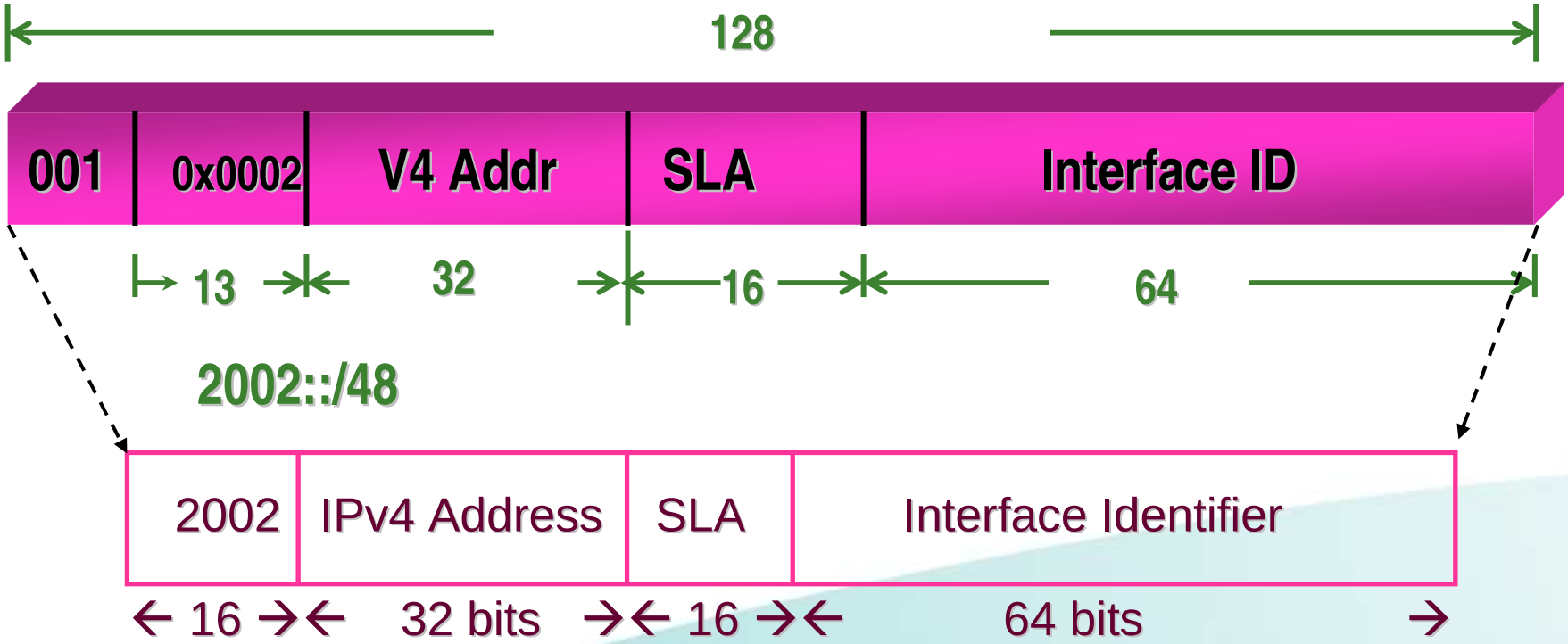
6to4

- 在現有的IPv4網路中，自動建立Tunnel連線至IPv6網路
- 僅能在Public IPv4位址下使用
- 通常建在企業的border router

- 身為**6to4**的**egress router**必須
  - **Have a dual stack (IPv4/IPv6)**
  - **Have a globally routable IPv4 address**
  - **Implement 6to4**

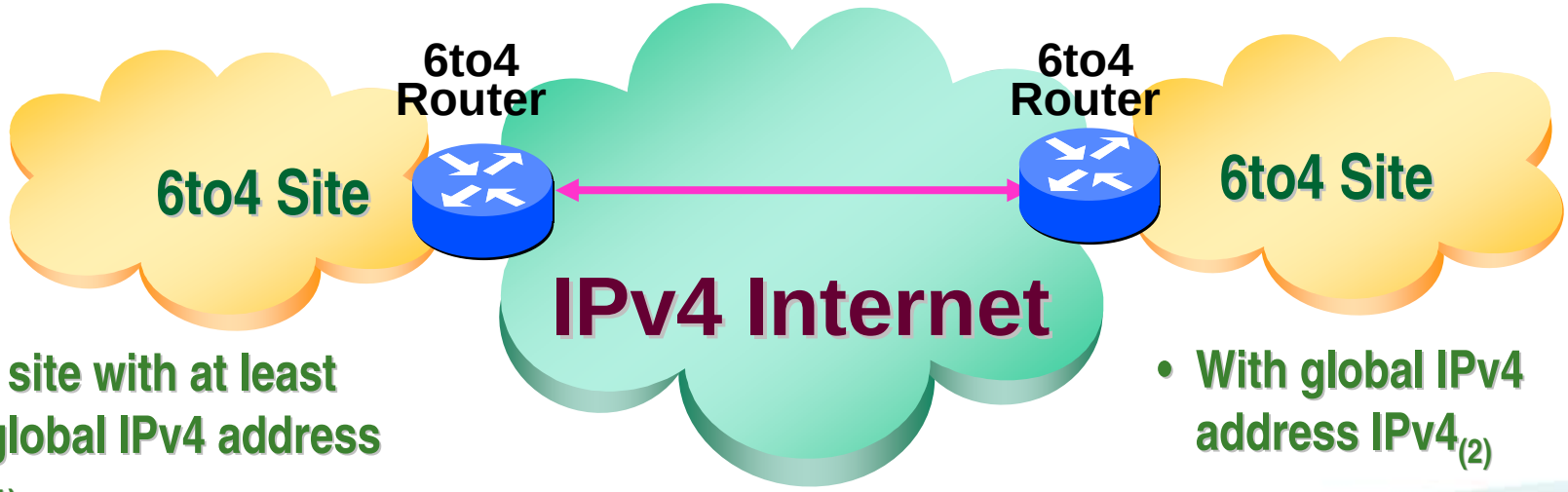
- 使用 **6to4 TLA** (2002) 開頭的 **IPv6 prefix**

Address Prefix for 6to4

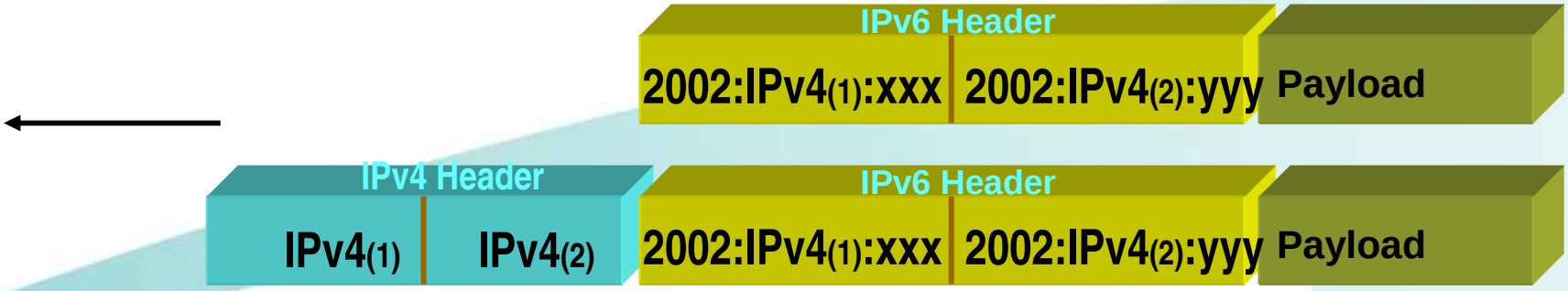


- Site creates a 48 bit prefix using its gateway router's public IPv4 address
  - 2002:A.B:C.D::/48 for IPv4 address A.B.C.D

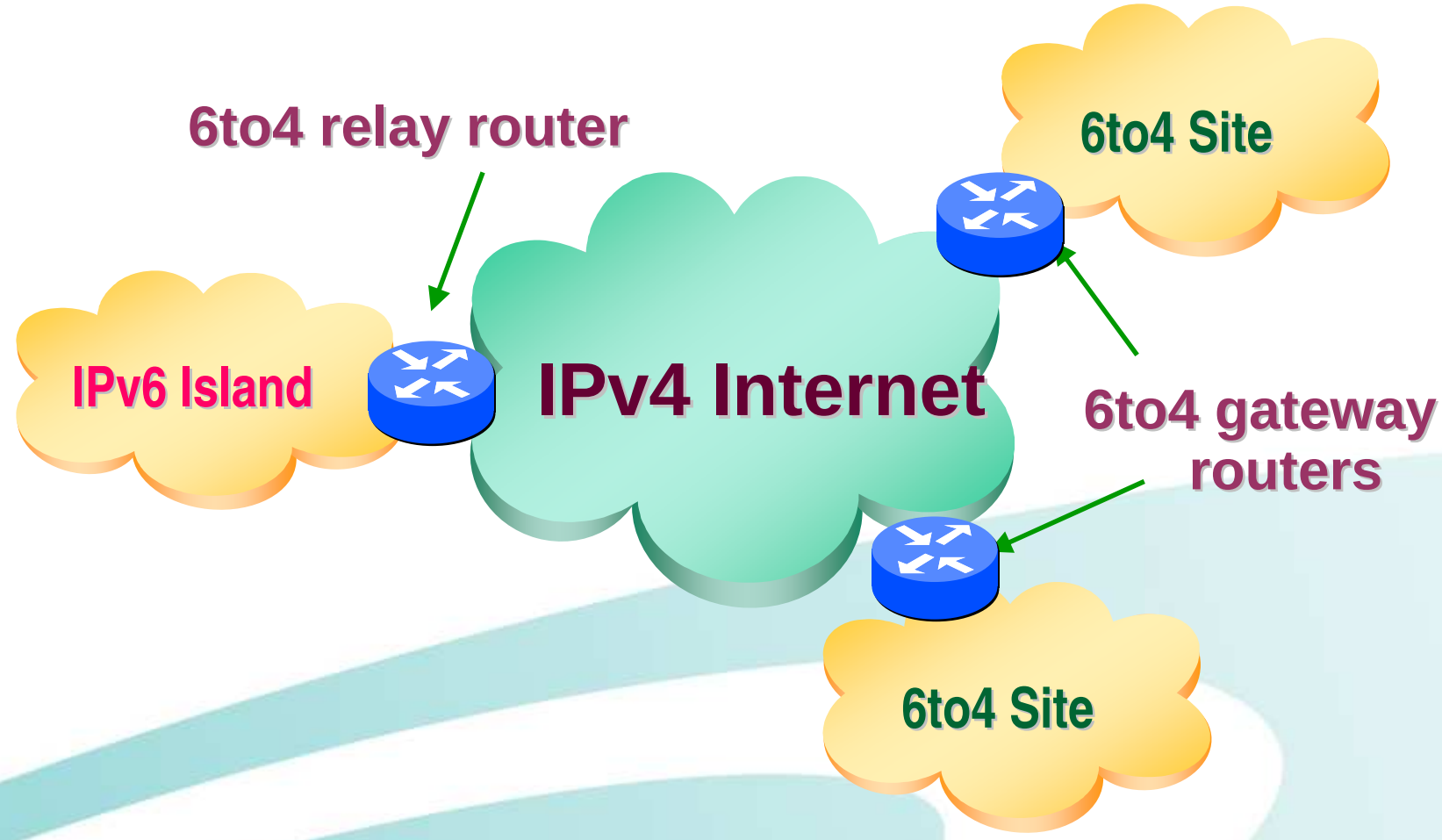
6to4



- Each site with at least one global IPv4 address IPv4(1)
- With global IPv4 address IPv4(2)



6to4 佈建


6to4 relay router
6to4 Site
IPv6 Island
IPv4 Internet
6to4 gateway routers
6to4 Site

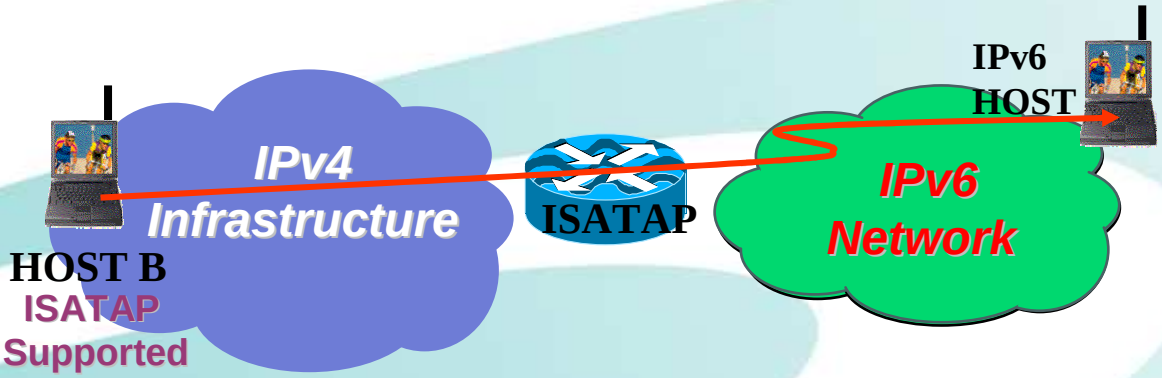
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

RFC4214 -> 5214

ISATAP

- 在現有的IPv4網路中，自動建立Tunnel連線至IPv6網路

- Example: ISATAP host communicates with IPv6 host (no ISATAP support).
  - The ISATAP host is isolated in an IPv4 network whereas the IPv6 host is in a IPv6 network

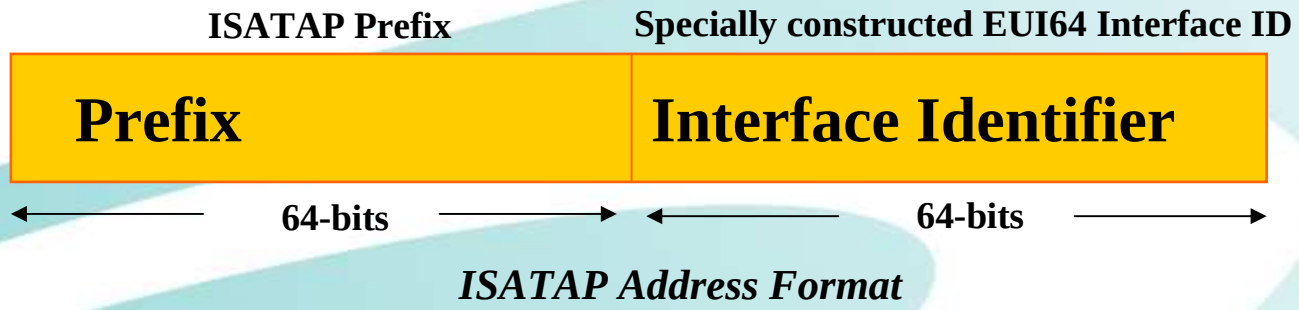


Construction of ISATAP address

- ISATAP interface identifier can be combined with any 64-bit prefix (including 6to4 prefixes) to form an RFC 2373 compliant IPv6 globally aggregatable unicast address.
- IPv4 address inside EUI-64 interface identifier

  ::0:5EFE:A.B.C.D for IPv4 address A.B.C.D

  The **0:5EFE** portion is formed from the combination of the Organizational Unit Identifier (OUI) that is assigned to IANA, and a type that indicates an embedded IPv4 address (**FE**).

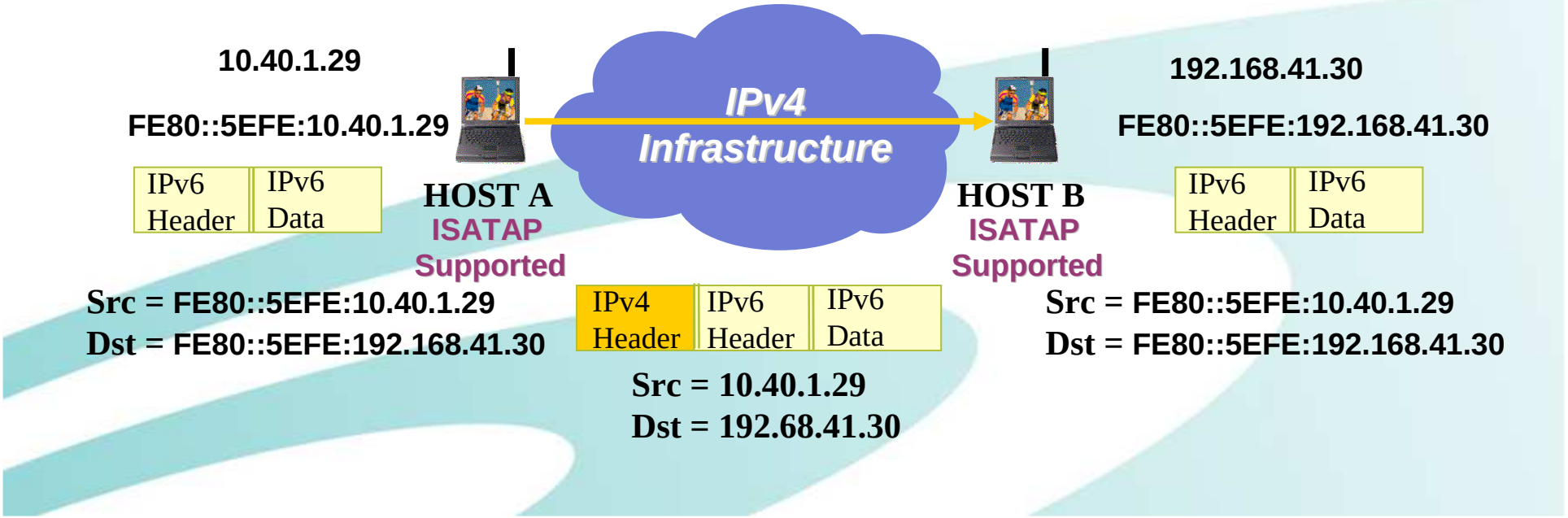


ISATAP Address Format

ISATAP Operation (1/2)

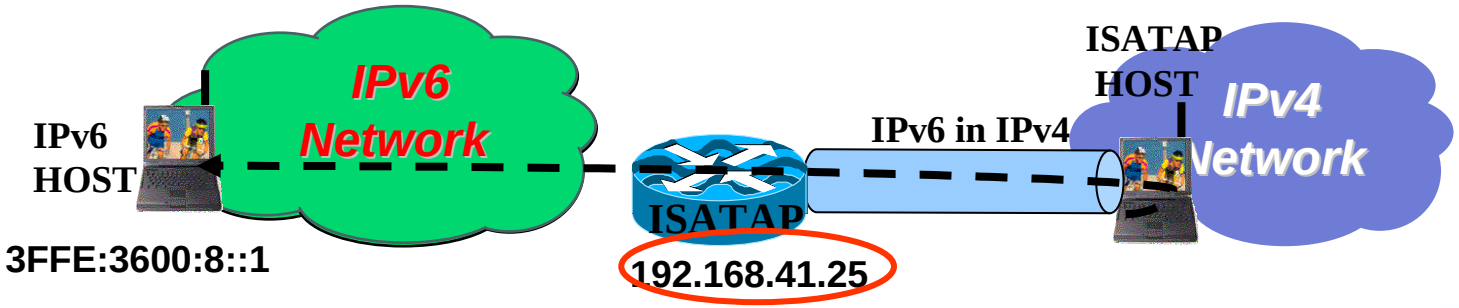
Simple Deployment Scenario of ISATAP (Hosts….)

The Automatic Tunneling Pseudo-Interface uses the link-local ISATAP address assigned to the interface as a source, and uses the last 32 bits in the source and destination IPv6 addresses (corresponding to the embedded IPv4 addresses) as the source and destination IPv4 addresses



ISATAP Operation (2/2)

Simple Deployment Scenario of ISATAP (Routers…)



IPv4 Header	IPv6 Header	IPv6 Data

Src = 10.40.1.29
Dst = 192.68.41.25

IPv6 Header	IPv6 Data

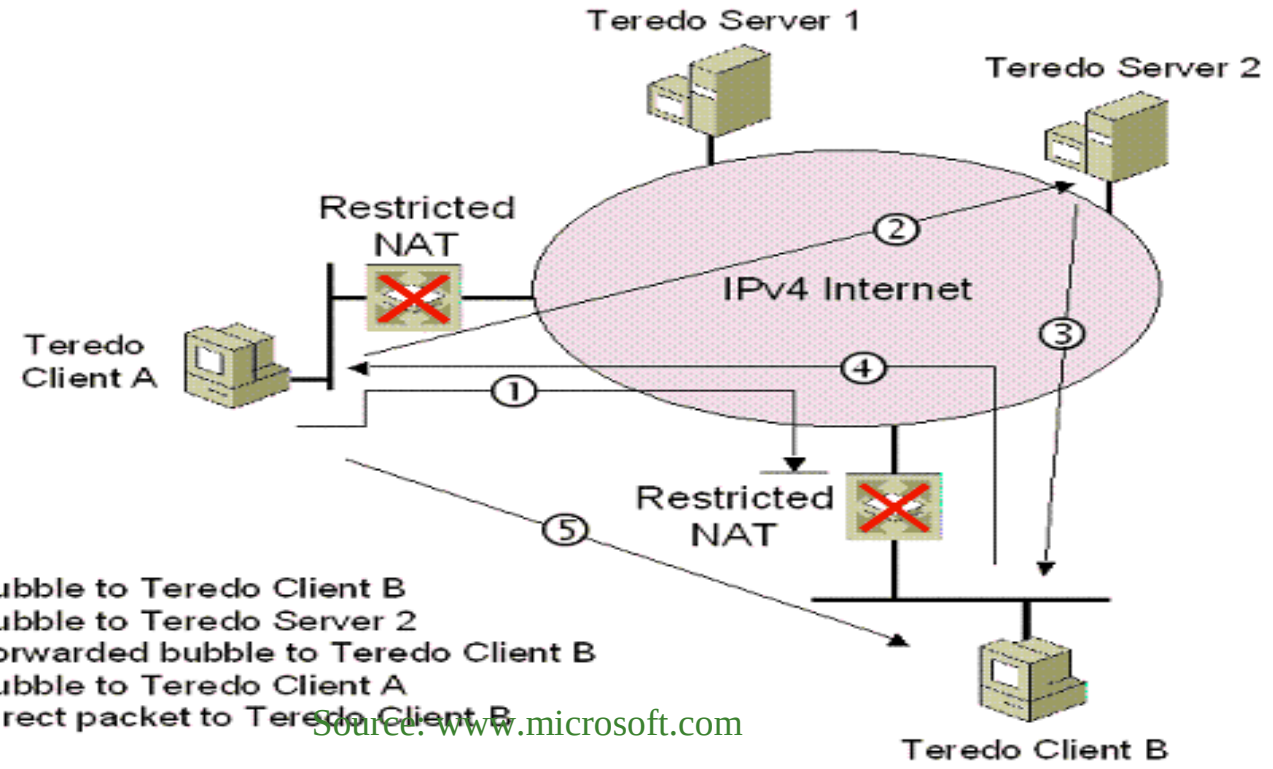
Src = 3FFE:1A05:5102412:5EFE:10.40.1.29
Dst = 3FFE:3600:8::1

IPv6 Header	IPv6 Data

Src = 3FFE:1A05:5102412:5EFE:10.40.1.29
Next = 3FFE:1A05:5102412:5EFE:192.168.41.25
Dst = 3FFE:3600:8::1

Teredo

- 在現有的IPv4網路中，自動建立Tunnel連線至IPv6網路
- 可解決IPv4為private IPv4位址時可連出去至IPv6網路



Source: www.microsoft.com

Automatic Tunnel

ISATAP:

優點: 使用者完全不用進行設定，適用於企業內部網路之步署。可為Private IPv4使用者提供Public IPv6 之位址, Cisco路由器支援

缺點: 安全性不足,會造成Bottle Neck。但如配合Firewall使用，即為安全性最佳之解決方案。

6to4:

優點: 適用於WAN端連結，Cisco路由器支援

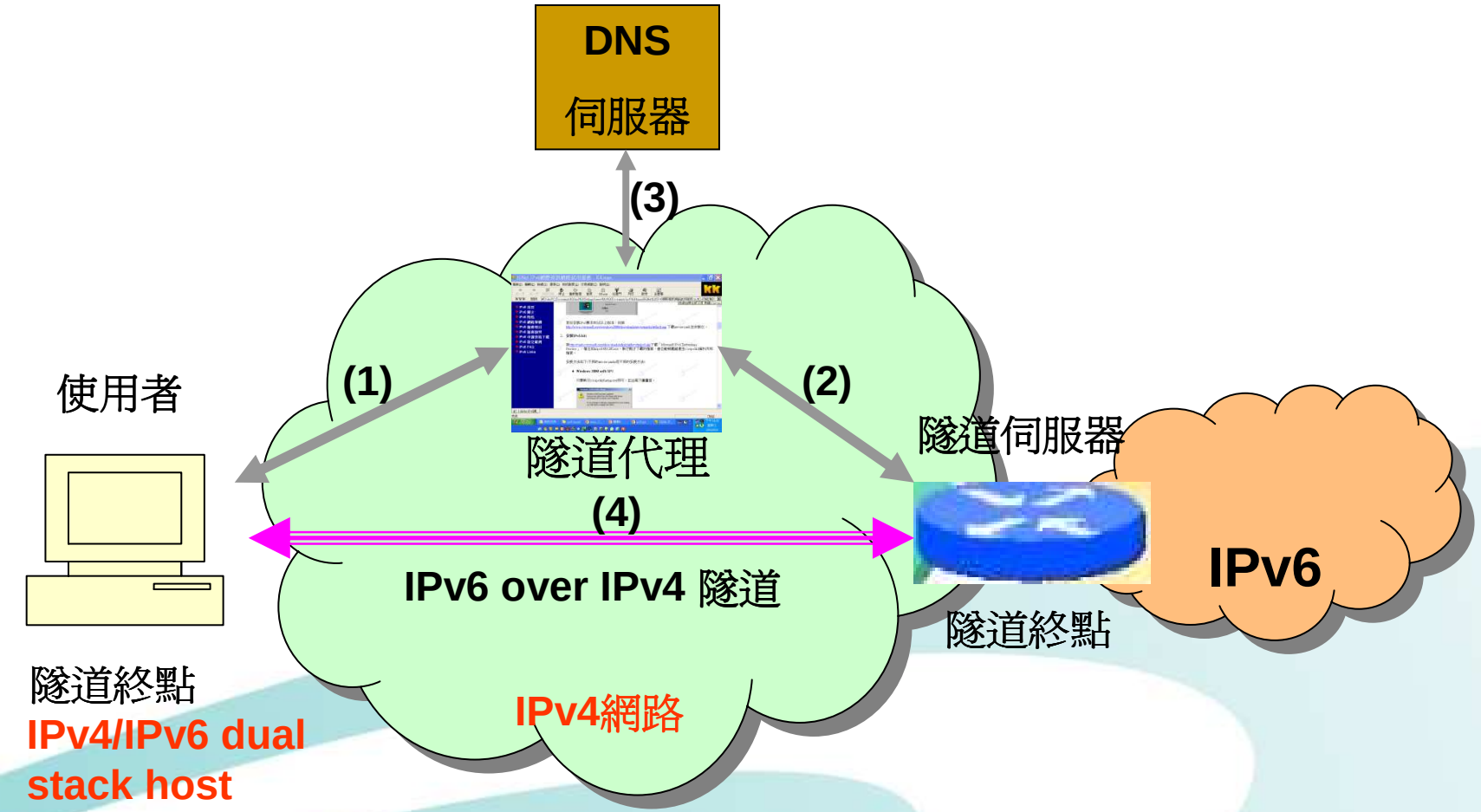
缺點: 安全性不足，網際網路連線能力不足，沒有Business Model

Teredo:

優點:可以讓在IP分享器後之虛擬IP Tunnel Client 與使用Public IP之Teredo Tunnel Server 建立IPv6 Tunnel

缺點: 使用者需進行設定、安全性不足、難以控管、會造成Bottle Neck、 Cisco路由器不支援。

IPv6 Tunnel broker



穿隧(Tunneling)技術優缺點比較表

IPv4/IPv6穿隧(Tunneling)轉移技術	
優點	缺點
節點對節點的連線方式未遭破壞。	需要IPv4網路架構。
利用現有IPv4網路，可降低成本。	無法解決IPv4位址不足的問題。
	封裝及解封裝增加網路額外負擔。
	需要人工的設定與維護，增加網管者沈重的工作負擔。

Translator

Translator的功用

1. IPv6在根本上改進了IPv4原有的缺點，並移除了原來IPv4最仰賴的Broadcast機制。因此原有在IPv4上的應用必須重寫才能支援IPv6.
2. 為了讓原IPv4的應用可以用到IPv6網路上，必須要經過Translator的轉換，將IPv4的模式及IPv6的模式相互轉換，才有機會讓應用程式能夠互通
3. 很多應用程式在IPv6時的編寫標準與IPv4不時是有差異的，必須要靠依據個別程式的特性，打造其專屬的轉換機制

Translator 技術一覽

- RFC 2765: Stateless IP/ICMP Translation Algorithm (SIIT)
- RFC 2766: Network Address Translation - Protocol Translation (NAT-PT)
- RFC 2767: Dual Stack Hosts using the Bump-in-the-Stack technique
- RFC 3338: Dual Stack Hosts Using "Bump-in-the-API (BIA)
- RFC 3089: A SOCKS-based IPv6/IPv4 Gateway Mechanism
- RFC 3142: An IPv6-to-IPv4 transport relay translator

但目前實際上被大部份路由器及防火牆廠商接受的只有SIIT, NAT-PT以及其外掛之Application Layer Gateway, 因此以下僅企紹NAT-PT及其相關技術

Translator 技術之限制

1. 現實上，不可能為每一個Application都寫出其特定的ALG，因此Translator技術僅適用於特定的情境，可作為ICP以IPv4 only的Web-Server及FTP Server提供Content給IPv6使用者，或ITSP業者以現有IPv4平台提供服務給VoIPv6使用者等服務之解決方案。
2. 只能進行特定對特定或不特定對特定之轉換，無法提供不特定對不特定或特定對不特定之轉換

轉換(Translation)技術優缺點比較表

IPv4/IPv6轉換(Translation)技術 NAT-PT	
優點	缺點
NAT-PT可建構在IPv4與IPv6網路交界位置，提供純IPv4與純IPv6間的通訊，免除將主機升級為雙IP協定堆疊的麻煩。	經由NAT-PT處理的session，在整個session過程中，所有封包均需流經此NAT-PT。因此NAT-PT轉換器可能成為網路運作的瓶頸點，會危及整體網路運作。
NAT-PT的運作對end-user而言幾乎是透通的。	需借助DNS-ALG、FTP-ALG 以及各種應用程式ALG(Application Layer Gateway)方能處理封包酬載中位址的轉換，達成應用層雙向互連。

導入IPv6行動準則建議

- Three Types of Transition Mechanisms
  - Dual Stack、Tunnelling、Translator
- No single mechanism applies to all situations
- Dual Stack為建議之機制，設備汰換時，可將IPv6功能列入考量。(實際運作時，可考慮是否要啟用)
- 除設備考量外，軟體、應用服務及OS也需注意IPv6功能支援
- 網路導入基本原則：Dual stack where you can, Tunneling where you must, Translation where you have no other solutions.
  - 網路設備逐步IP dual stack，先形成點狀分佈，善用tunneling技術將”點”互連，再逐步由點而面
- 服務導入基本原則： Dual stack where you can, independence each other where you must , Translation where you have no other solutions.
  - 新建服務平台要求必須支援IP dual stack access
  - 既有服務平台若為獨立系統，與其他平台無介接，則可優先考慮以IP dual stack方式導入
  - 若既有服務平台與其他平台介接且複雜，則建議將既有服務平台mirror成兩套，IPv4 & IPv6 user彼此分開

謝謝