IPv6轉移機制之介紹

CHT-TL IPv6測試實驗室

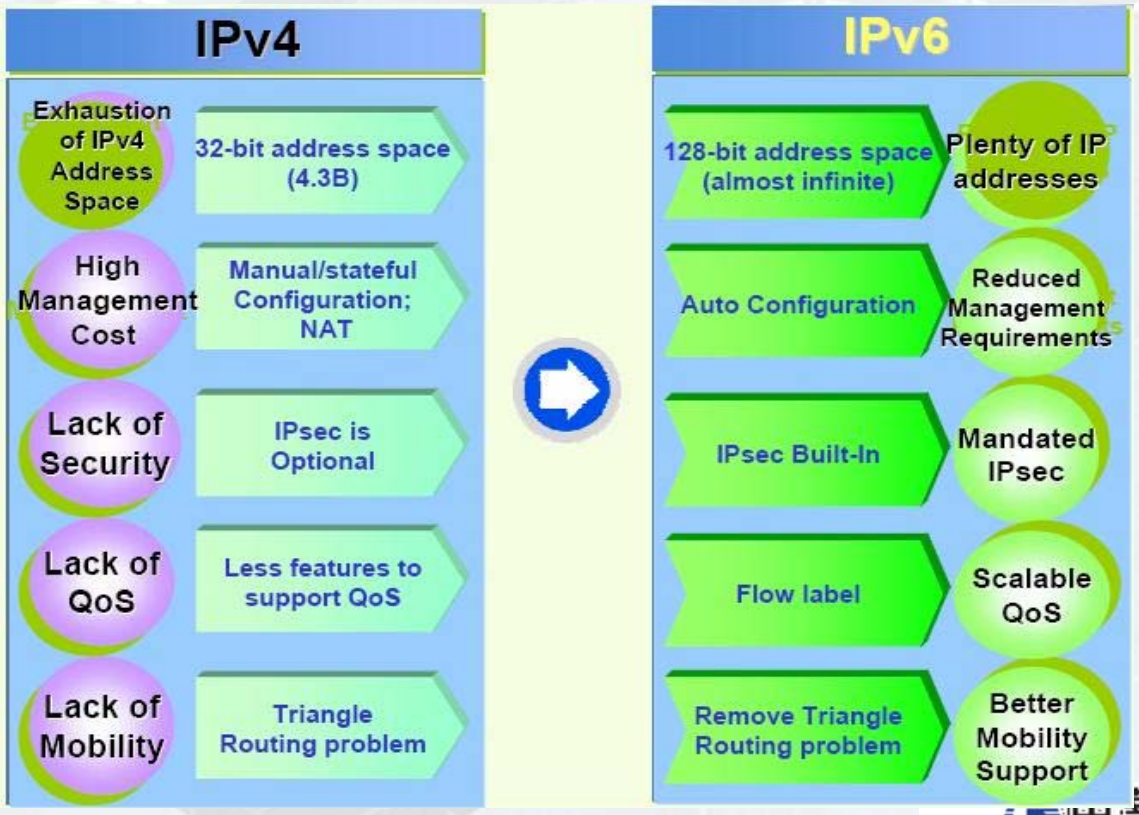
目 錄

- 簡介
- IPv6/IPv4 雙IP機制(Dual Stack)
- 通道機制(Tunneling)
- 位址協定轉換機制(Translator)
- RFC 5211-An Internet Transition Plan
- 導入IPv6行動準則建議

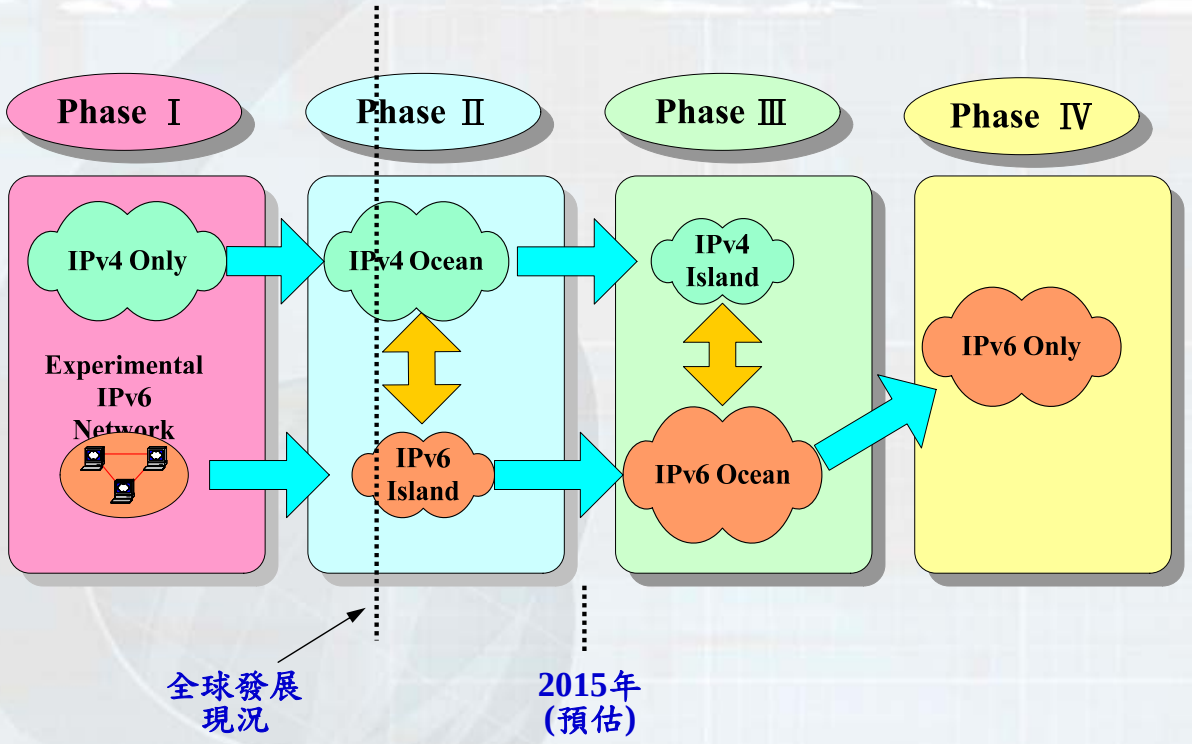
目 錄

- 簡介
- IPv6/IPv4 雙IP機制(Dual Stack)
- 通道機制(Tunneling)
- 位址協定轉換機制(Translator)
- RFC 5211-An Internet Transition Plan
- 導入IPv6行動準則建議

IPv4 to IPv6



為何需要Transition機制?



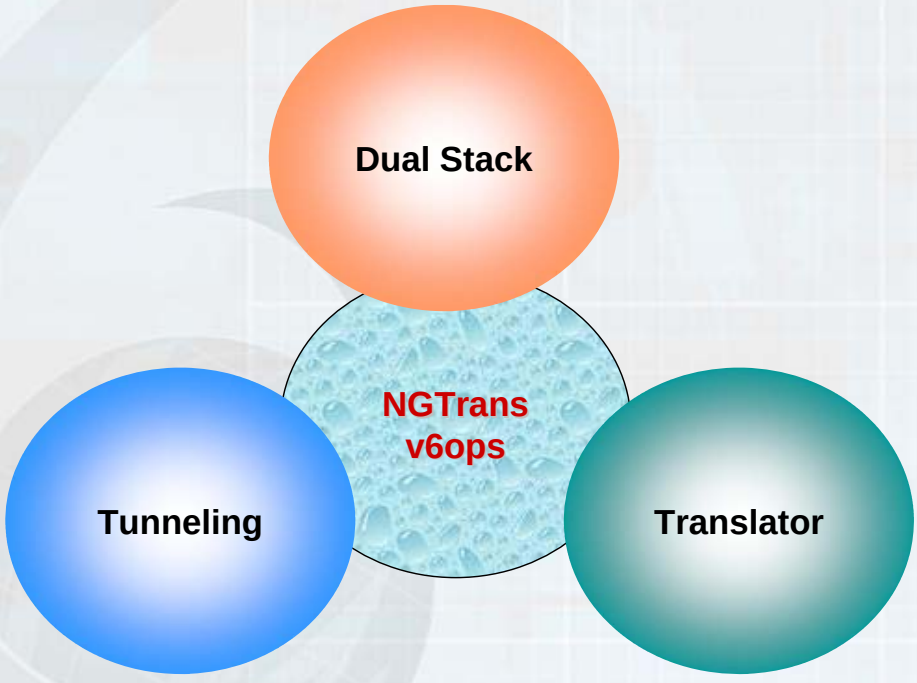
IP網路與服務

Servers	Networks	Clients
IPv4	IPv4	IPv6
IPv4	IPv6	IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv4
IPv6	IPv4	IPv6
IPv4	IPv6	IPv4

IETF ngtrans(V6OPS) *Working Group*

- Next Generation Transition (ngtrans) working group of the IETF
- Replaced by V6OPS working group
- overall goal : assisting the transition to IPv6

Next Generation Transition

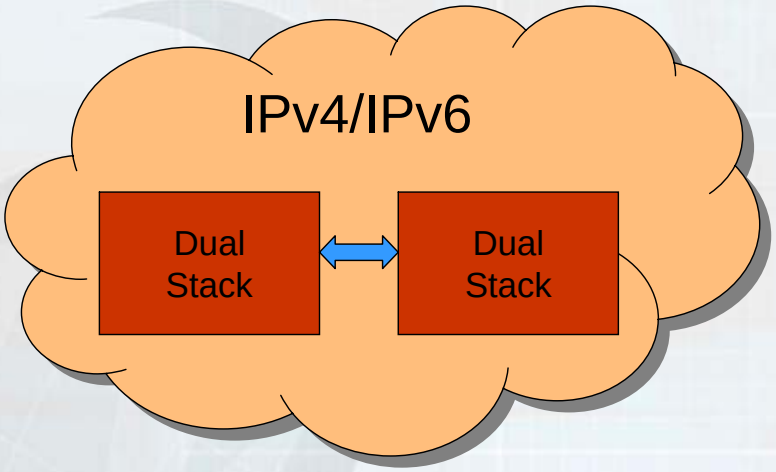


Transition mechanism

- Dual stack
  - allow IPv4 and IPv6 to co-exist in the same devices and networks.
- Tunneling
  - enable network edge devices to interconnect over incompatible networks.
- Translation
  - allow IPv6-only devices to communicate with IPv4-only devices

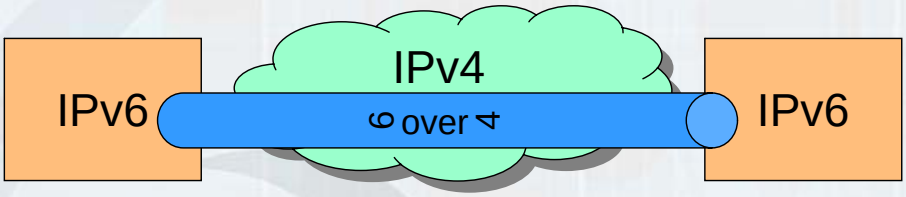
Dual Stack

- RFC 2893 -> RFC 4213

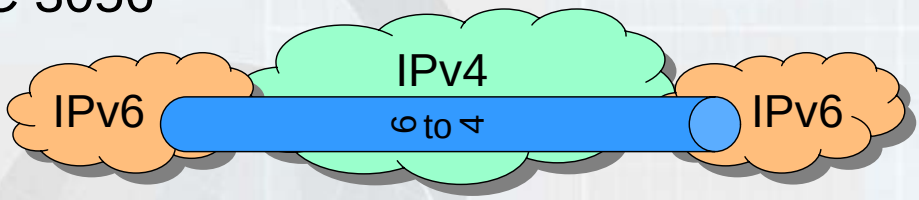


Tunneling

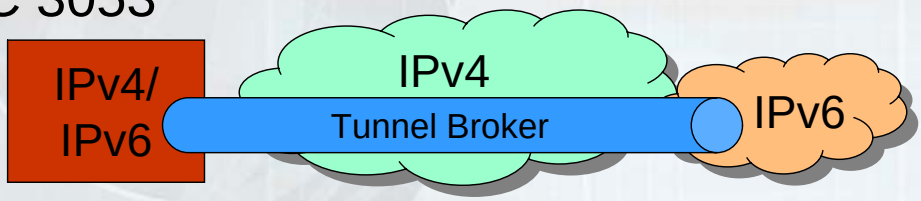
- RFC 2529



- RFC 3056



- RFC 3053

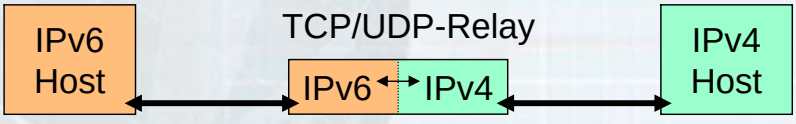


Translator

- RFC 2765；RFC 2766

- RFC 2767

- RFC 3142



目 錄

- 簡介
- IPv6/IPv4 雙IP機制(Dual Stack)
- 通道機制(Tunneling)
- 位址協定轉換機制(Translator)
- RFC 5211-An Internet Transition Plan
- 導入IPv6行動準則建議

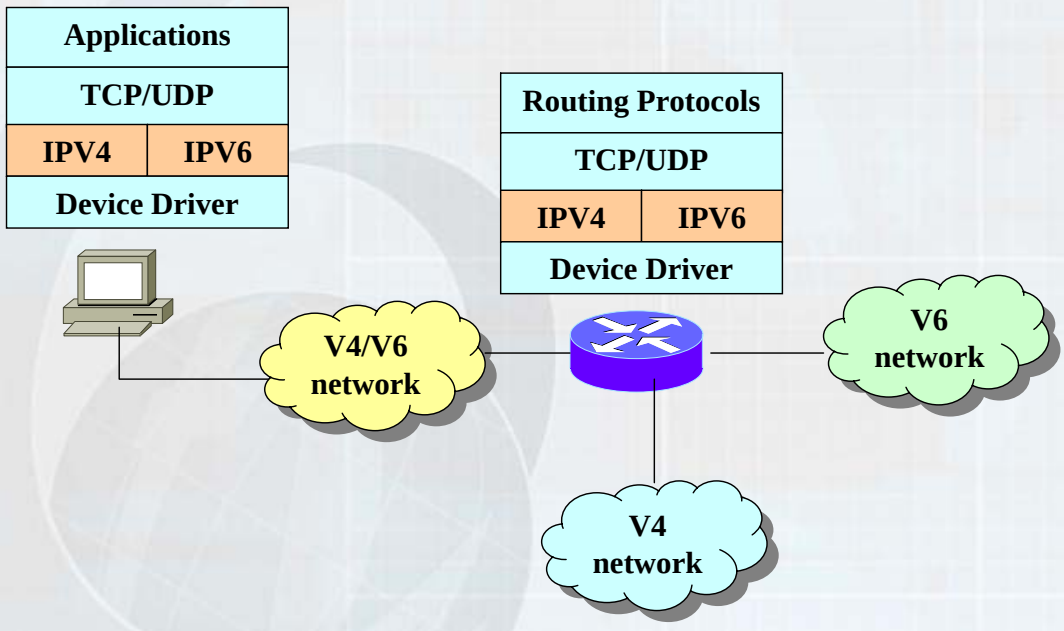
RFC 4213

- **RFC 4213 obsoletes RFC2893**
- **RFC 4213 “Basic Transition Mechanisms for IPv6 Hosts and Routers “ , Oct.,2005**
- **RFC 4213 defines two mechanisms that IPv6 hosts and routers may implement in order to be compatible with IPv4 hosts and routers.**
  - **Dual IP layer (Dual stack)**
  - **Configured tunnels**
  - Other transition mechanisms, including other tunneling mechanisms, are outside the scope of this document

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)



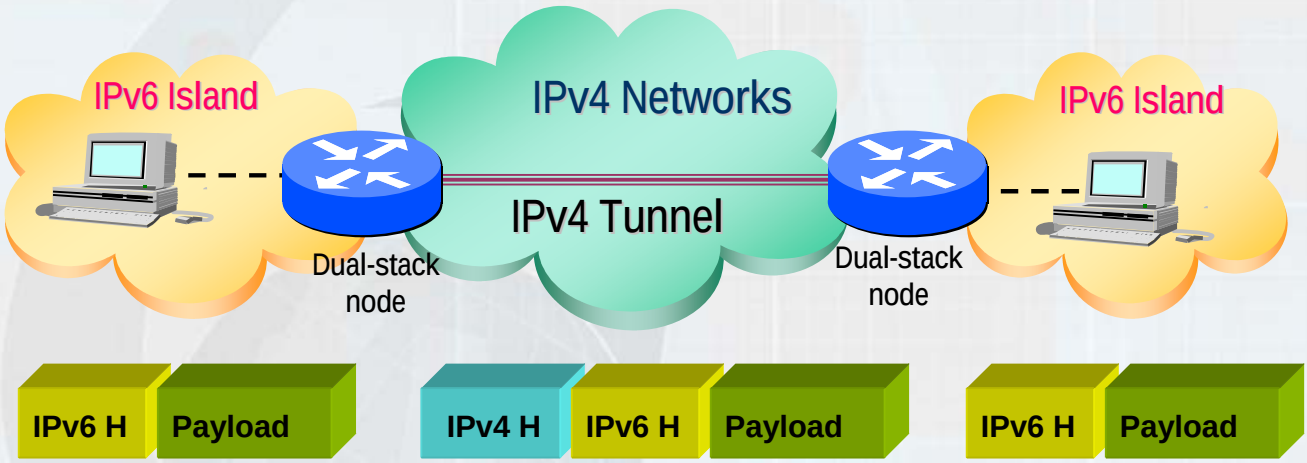
目 錄

- 簡介
- IPv6/IPv4 雙IP機制(Dual Stack)
- 通道機制(Tunneling)
- 位址協定轉換機制(Translator)
- RFC 5211-An Internet Transition Plan
- 導入IPv6行動準則建議

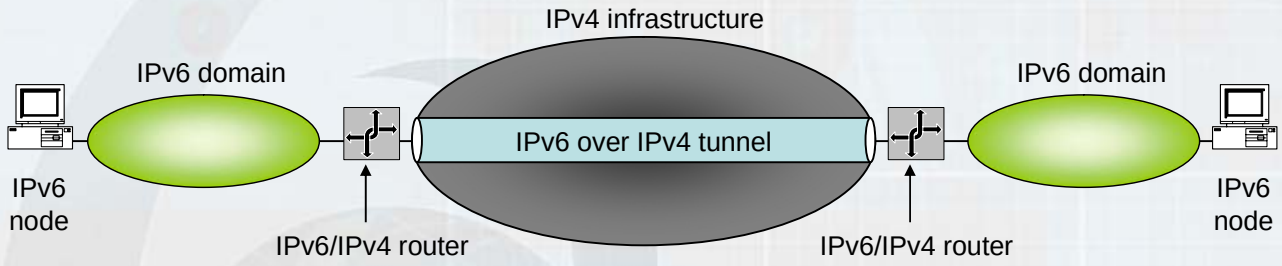
RFC 4213 - Configured Tunnel

- 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

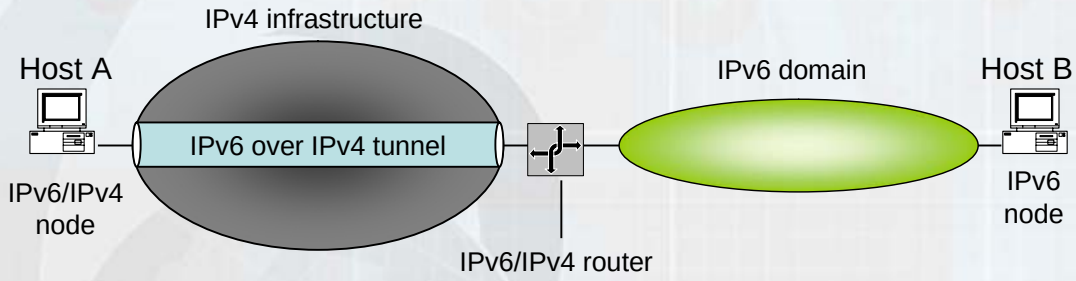
Configured Tunnel



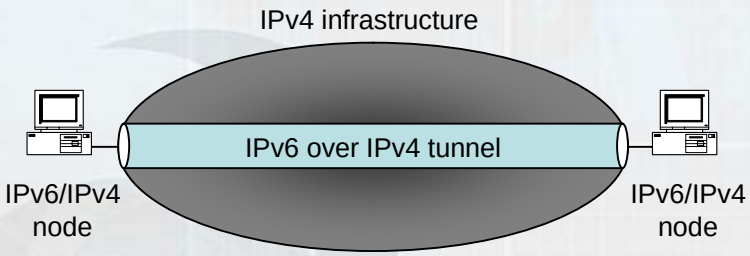
Router-to-Router



Host-to-Router



Host-to-Host



IPv6 Tunnel Broker

RFC 3053

23

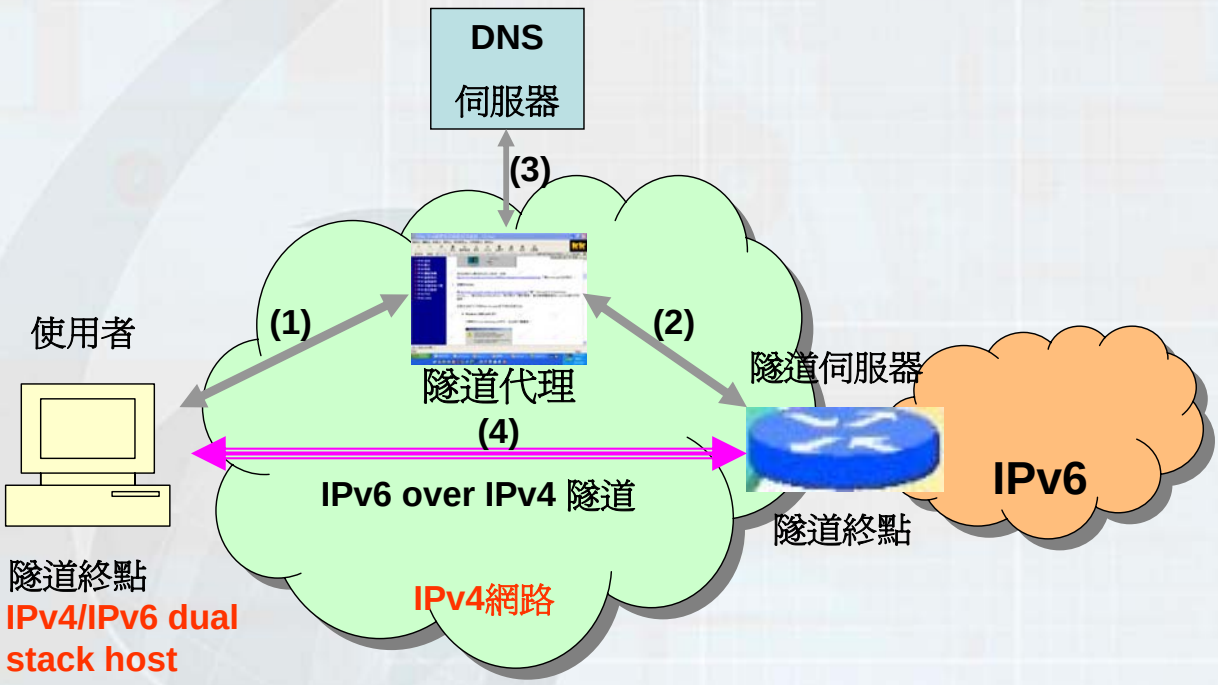
Motivation

- **IPv6 tunneling over the internet requires heavy manual configuration**
  - Network administrators are faced with overwhelming management load
  - Getting connected to the IPv6 world is not an easy task for IPv6 beginners
- **The Tunnel Broker approach is an opportunity to solve the problem**
  - The basic idea is to provide tunnel broker to automatically manage tunnel requests coming from the users
- **Benefits**
  - Stimulate the growth of IPv6 interconnected hosts
  - Allow to early IPv6 network providers the provision of easy access to their IPv6 networks

Tunnel Broker

- **Tunnel broker automatically manages tunnel requests coming from the users**
  - The Tunnel Broker fits well for small isolated IPv6 sites, especially isolated IPv6 hosts on the IPv4 Internet
- **Client node must be dual stack (IPv4/IPv6)**
- **The client IPv4 address must be globally routable (no NAT)**

Tunnel broker



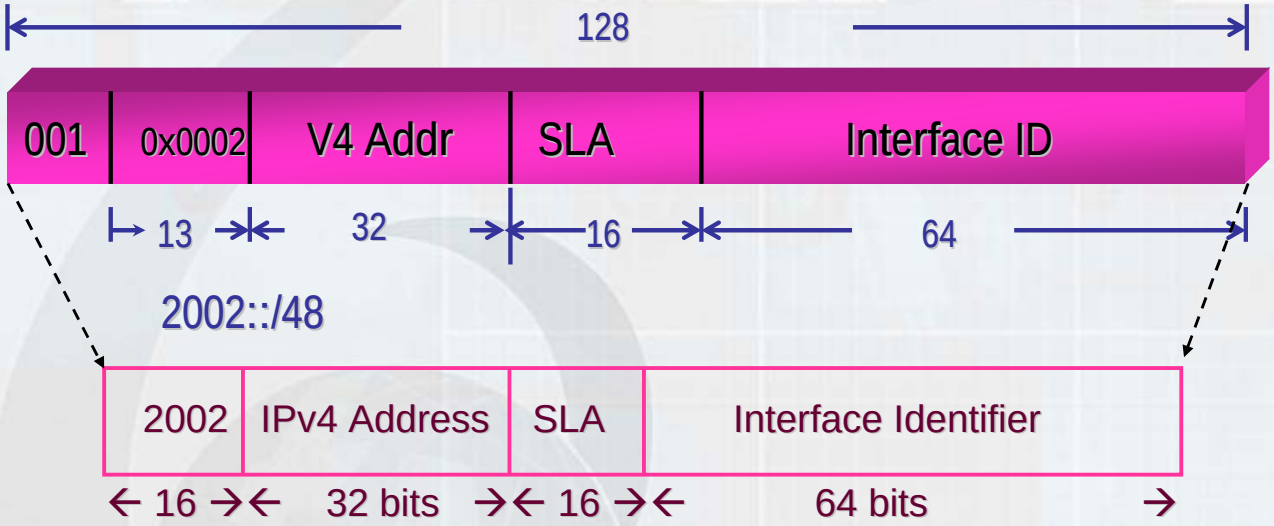
Connection of IPv6 Domains via IPv4 Clouds (6to4)

RFC3056

6to4

- Interconnection of isolated IPv6 domains in an IPv4 world
- No explicit tunnels
  - No scaling issues
- The egress router of the 6to4 site must
  - Have a dual stack (IPv4/IPv6)
  - Have a globally routable IPv4 address
  - Implement 6to4
- The site uses the 6to4 TLA (0x2002) for the site IPv6 prefix

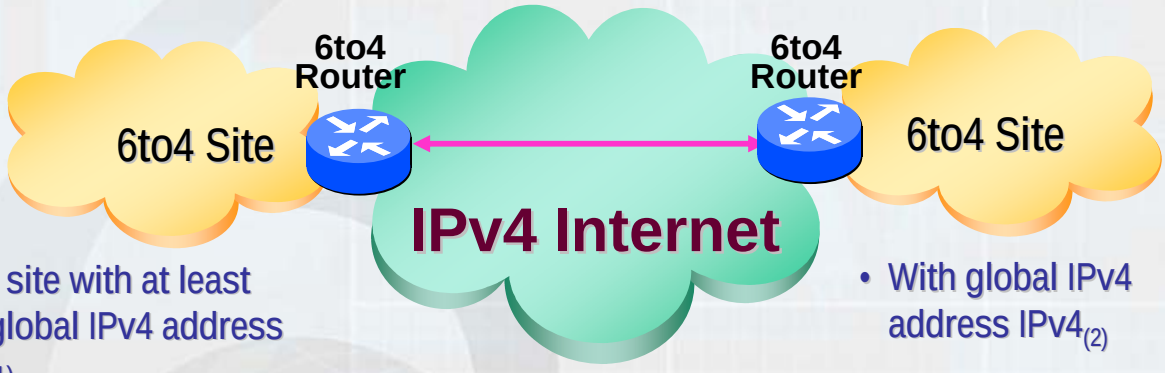
Address Prefix for 6to4



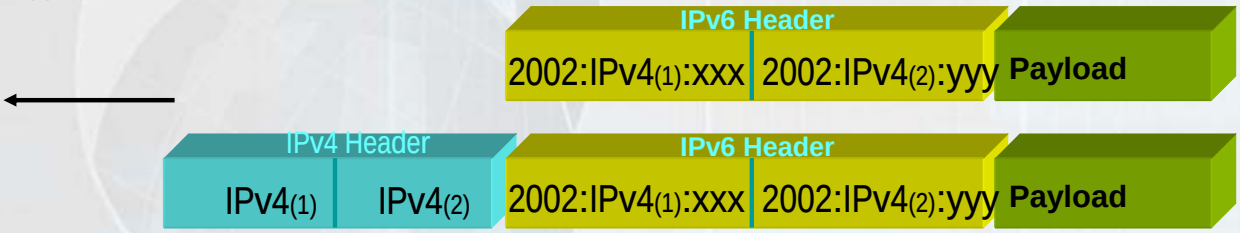
- Site creates a 48 bit prefix using its gateway router's public IPv4 address
  - 2002:A:B:C:D::/48 for IPv4 address A.B.C.D

例如，IPv4 位址 131.107.0.1 的 6to4 位址首碼是 2002:836B:1::/48

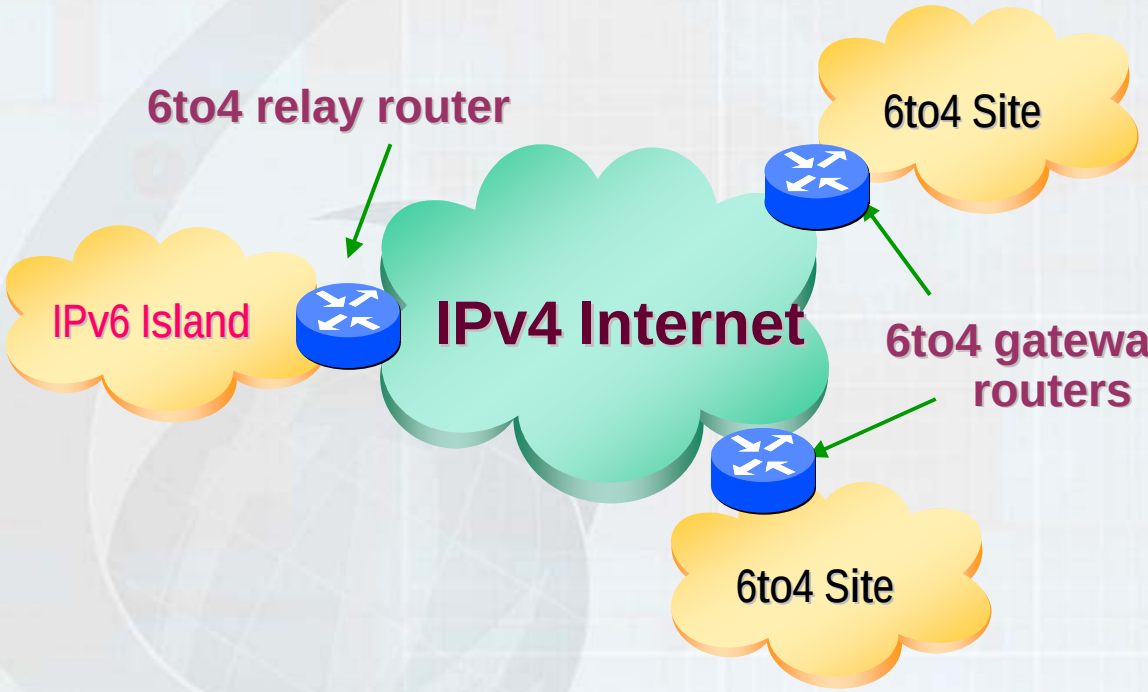
6to4



- Each site with at least one global IPv4 address $IPv4_{(1)}$
- With global IPv4 address $IPv4_{(2)}$

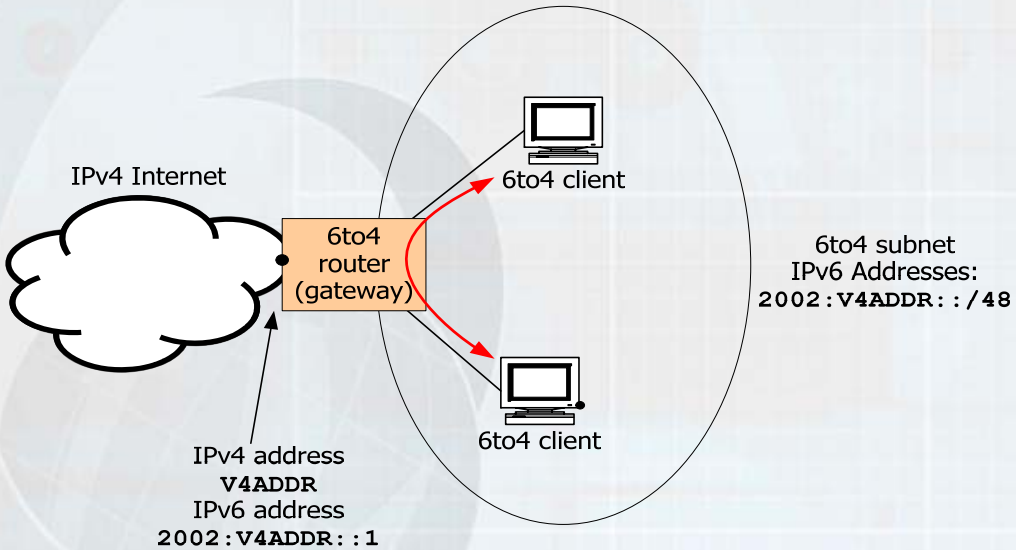


6to4 Deployment



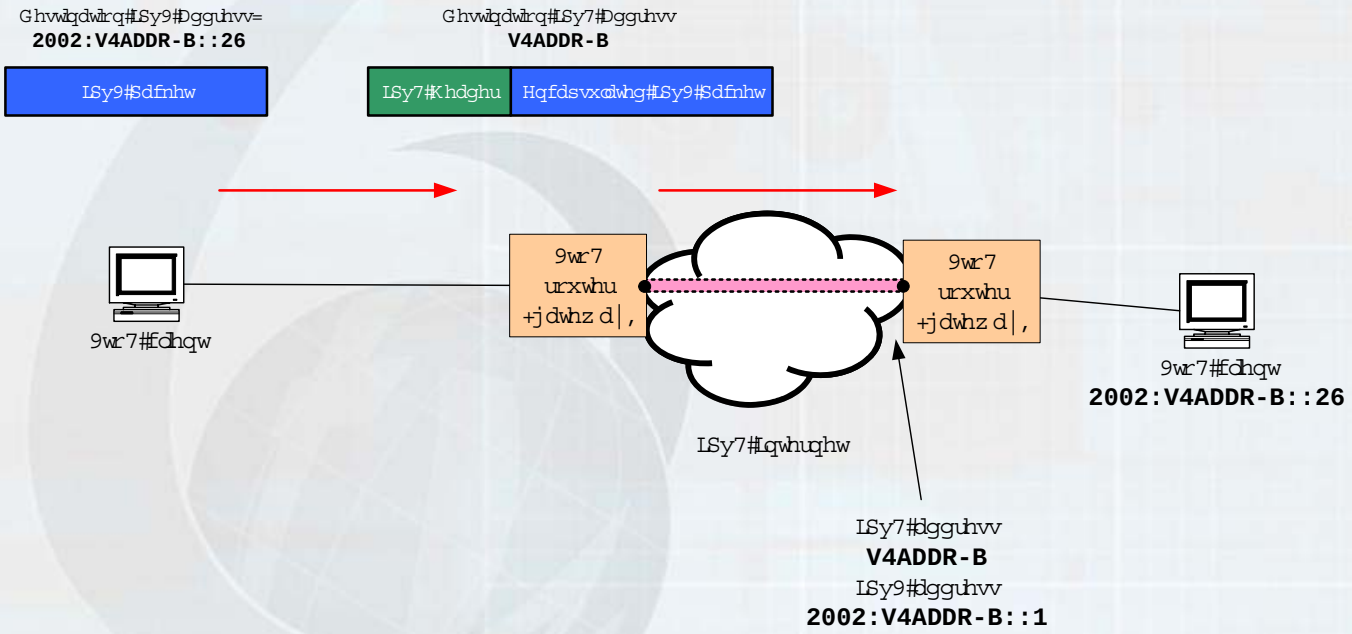
6to4應用 案例一

- 6to4 host to 6to4 host



6to4應用案例二

- Between two 6to4 sites



6to4機制的安全弱點

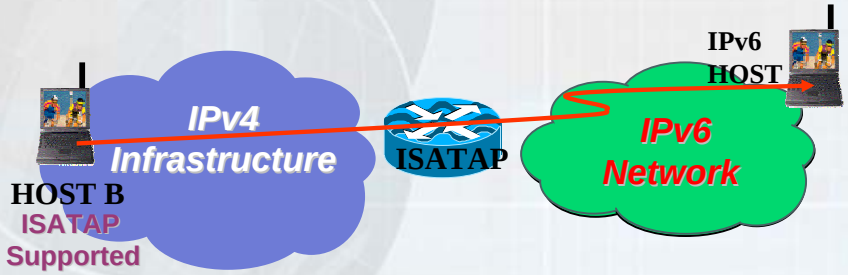
- Vulnerabilities
  - µ 6to4 routers must accept packets from ALL 6to4 relay routers
    - ˇ It's not possible to know if the relay router is "Trusted" or even existent
  - µ 6to4 relay routers have to accept packets from 6to4 routers and native IPv6 hosts without any checks
- Threats
  - µ DoS/DDoS against 6to4 components may result in unavailability
  - – 6to4 routers/relay routers may be used or "reflected" DDoS attacks
  - – "Service theft": unauthorized usage of relay router services
  - – Local IPv4 broadcast attacks
  - – Neighbor Discovery attacks

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

RFC4214 -> 5214

ISATAP

- The primary function of ISATAP is to allow hosts that are multiple IPv4 hops away from an IPv6 router to participate in the IPv6 network by automatically tunneling IPv6 packets over IPv4 to the next-hop address.
- 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 Address Example

EUI-64 Format Interface Identifier

- **If TYPE = 0xFF and TSE = 0xFE, TSD contains legacy EUI48 (TSE = 0xFF reserved by IEEE).**
- **If TYPE = 0xFE, TSE and TSD together contain embedded IPv4 address.**

IPv4 address is: 140.173.129.3

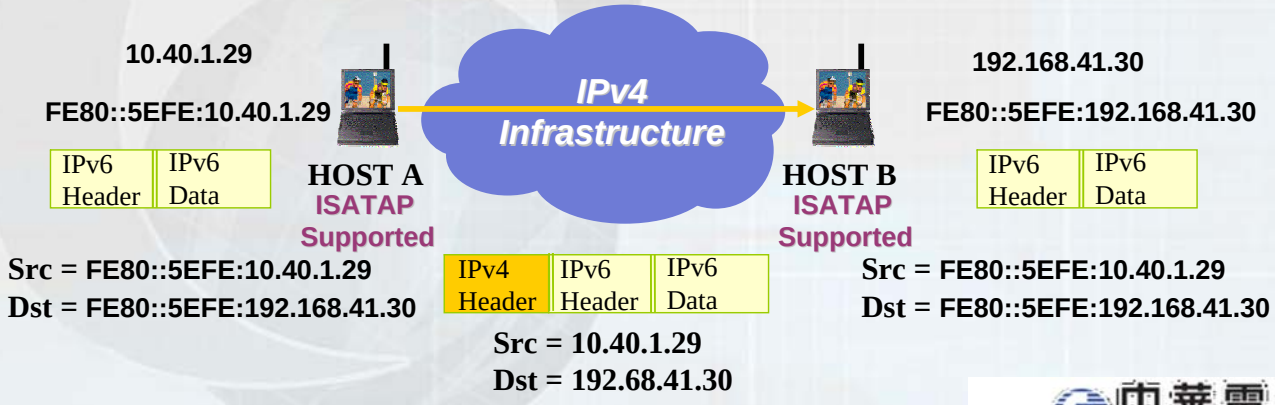
routing prefix is: 3FFE:1A05:510:2412

ISATAP IPv6 address is: 3FFE:1A05:510:2412:0:5EFE:140.173.129.3

ISATAP Operation (1/2)

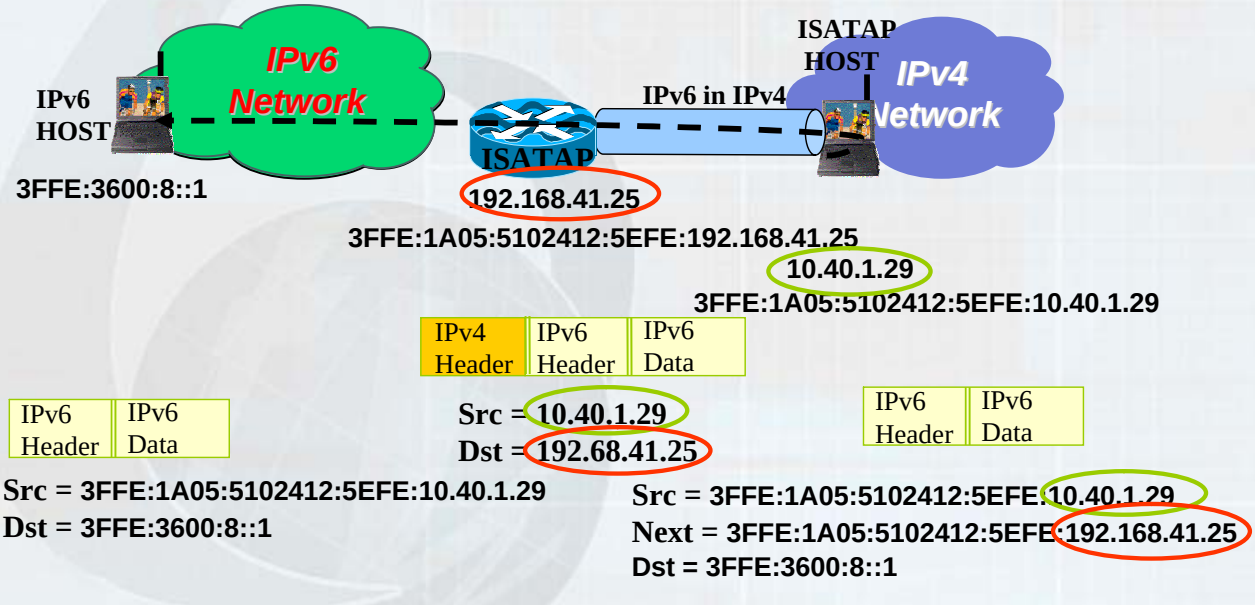
Simple Deployment Scenario of ISATAP (Hosts….)

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)

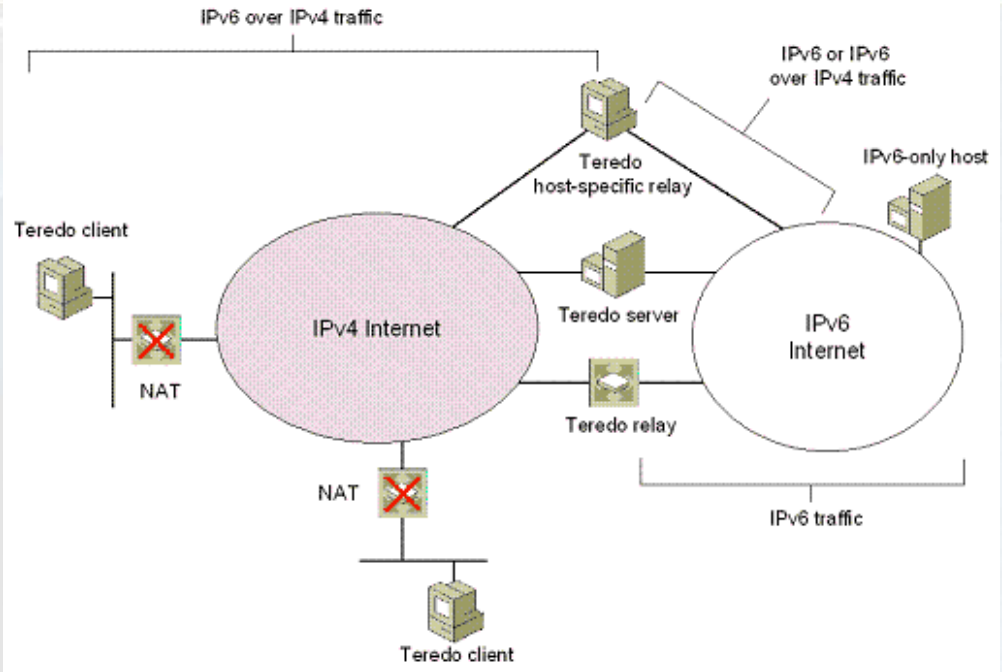
Simple Deployment Scenario of ISATAP (Routers…)

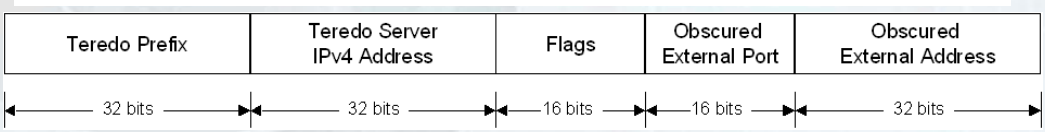


Teredo: Tunneling IPv6 over UDP through Network Address Translations

RFC4380

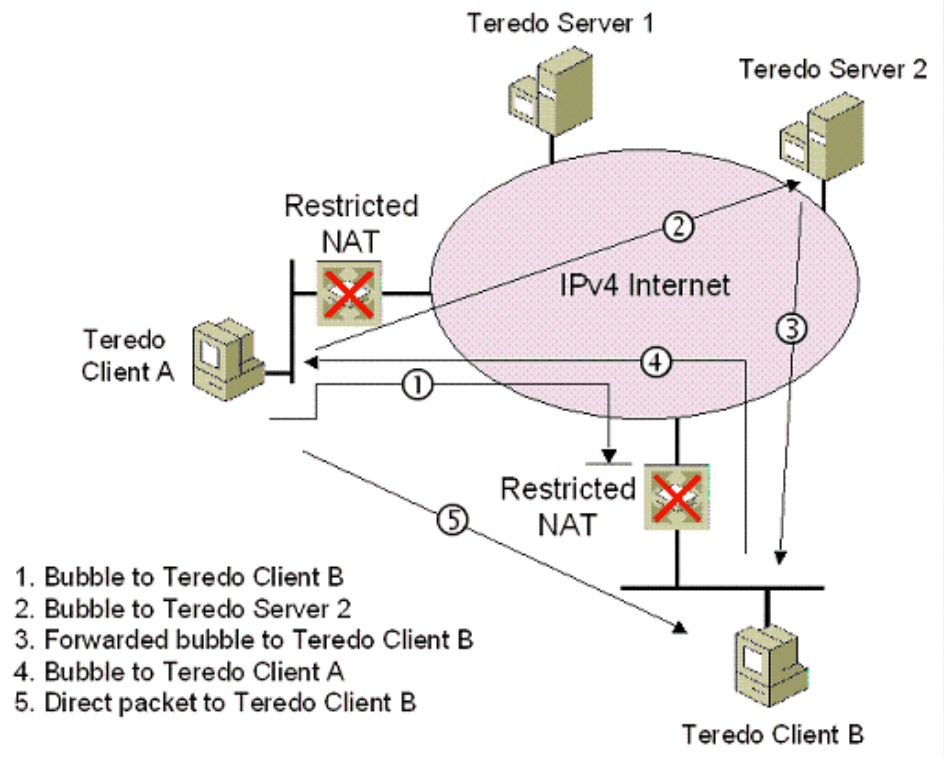
Teredo機制的架構與元件





Source: www.microsoft.com

Teredo應用案例



Source: www.microsoft.com

目 錄

- 簡介
- IPv6/IPv4 雙IP機制(Dual Stack)
- 通道機制(Tunneling)
- 位址協定轉換機制(Translator)
- RFC 5211-An Internet Transition Plan
- 導入IPv6行動準則建議

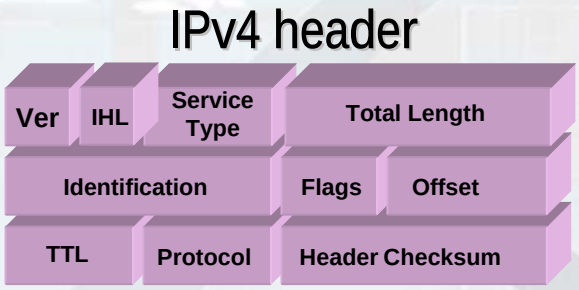
Stateless IP/ICMP Translation algorithm (SIIT)

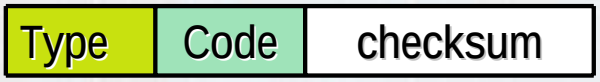
RFC 2765

SIIT (Stateless IP/ICMP Translation algorithm)

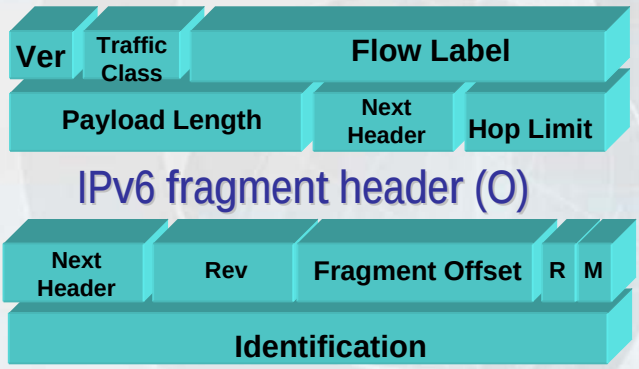
- Allows IPv6-only hosts to talk to IPv4 hosts
- Translation on IP packet header (including ICMP headers) in separate translator boxes in the network without requiring any per-connection state in those boxes.
- Use IPv4-translatable IPv6 address (0::ffff:0:a.b.c.d)
- Most option fields can not be translated
- Requires one temporary IPv4 address per host

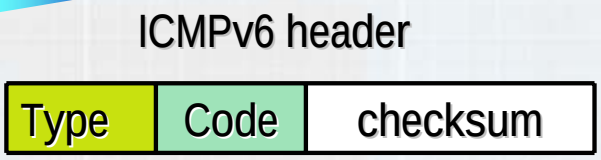
SIIT





SIIT





(1) SIIT 的優點：
1. Stateless，轉換是針對packet，與flow 無關。
(2) SIIT 的缺點：
1. Not be able to use IPv6-AH
2. Multicast address could not be mapped

中華電信 電信研究所

Network Address Translation – Protocol Translation (NAT-PT)

RFC 2766

CHT-TL IPv6 Testing Laboratory

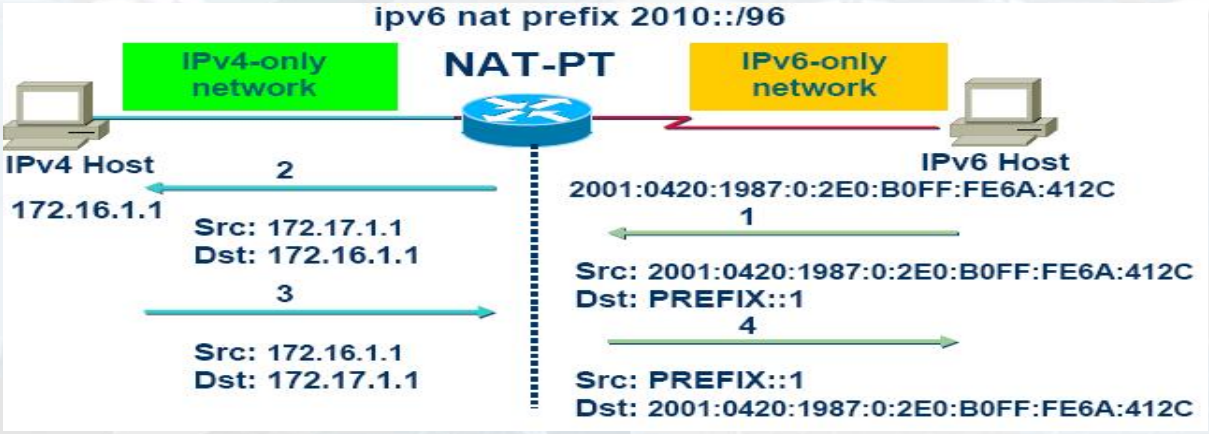
NAT-PT (1/3)

- Allows IPv6-only hosts to talk to IPv4 hosts and vice-versa
- similar to NAT in IPv4 network
- Stateful translation
- Requires at least one IPv4 address per site
- Traditional NAT-PT
  - Sessions are unidirectional, outbound from the v6 network
- Bi-directional-NAT-PT
  - Sessions can be initiated from hosts in v4 network as well as the v6 network
  - A DNS-ALG (application level gateway) must be employed to facilitate name to address mapping

NAT-PT (2/3)

- Limitations
  - all requests and responses pertaining to session should be routed via the same NAT-PT router
  - A number of IPv4 fields have changed meaning in IPv6 and translation is not straightforward
    - Ex. Option headers
  - Applications that carry the IP address in the high layer will not work.
    - In this case ALG need to be incorporated to provide support for these applications.
  - Lack of end-to-end security
  - Bottleneck

NAT-PT (3/3)



NAT-PT的優點：
1.對使用者來說是通透性的，用戶端不需要其他設定
NAT-PT的缺點：
1.同一個Session(連線)的封包必須經過同一個NAT-PT router,
2.所用的protocol translation演算法無法完全地轉換所有的資訊，會造成資訊的流失.
3.應用層若包含IP資訊將無法被轉換，除非透過Application Level Gateway(ALG)

NAT for IPv6之問題與解決現況彙整

代號	問題簡述	過去的解決方案	失敗原因	目前進行中的解決方案
1-a	ALG處理加密資料			• draft-A Scalable IPv4-IPv6 Transition Architecture Need for an address-port-borrowing-protocol • draft-Modified Network Address Translation - Protocol Translation • draft-IPv6 Rapid Deployment on IPv4 infrastructures • draft-Simplified Network Address Translation - Protocol Translation • draft-Carrier Grade NAT Behavioral Requirements • draft-Prefix-specific and Stateless Address Mapping (IVI) • draft-NAT64_DNS64 • draft-NAT for IPv6-Only Hosts • draft-Dual-stack lite broadband deployments post IPv4 exhaustion • draft-IPv4-IPv6 Coexistence and Transition Requirements for solutions • draft-Softwires Network Address Translation (SNAT) • dratf_Shimmed IPv4_IPv6 Address Network Translation Interface (SHANTI)
1-b	不用port number的協定			
1-c	Binding timout問題			
1-d	Header欄位不同			
1-e	分割封包的處理			
1-f	SCTP and multihoming	新增一個transport layer gateway	過於複雜	
1-g	Mobile IP議題	NAT-PT as a proxy	過於複雜	
1-h	處理multicast traffic	Draft: v4-v6 multicast gateway	Obsoleted	
2-a	network topology受限	Draft:NAT-PT DNS ALG solutions	只解決部分問題	
2-b	單點瓶頸與攻擊點	分散式NAT-PT+DNS-ALG	過於複雜	
2-c	Binding timout問題			
2-d	相關DOS攻擊	Draft:NAT-PT DNS ALG solutions	過於複雜	
3-a	Address selection	Draft:NAT-PT DNS ALG solutions	只解決部分問題	
3-b	將Record轉給別的應用			
3-c	要A給AAAA record	Stateless改為Stateful		
3-d	Multi-addressed nodes			
3-e	Secure DNS議題	將DNS-ALG變為DNSSEC server	過於複雜	
4	對應用發展的影響			

Application Layer Gateway

DNS ALG

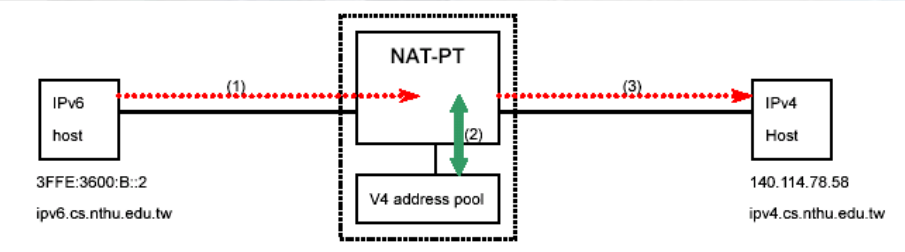
FTP ALG

ALG

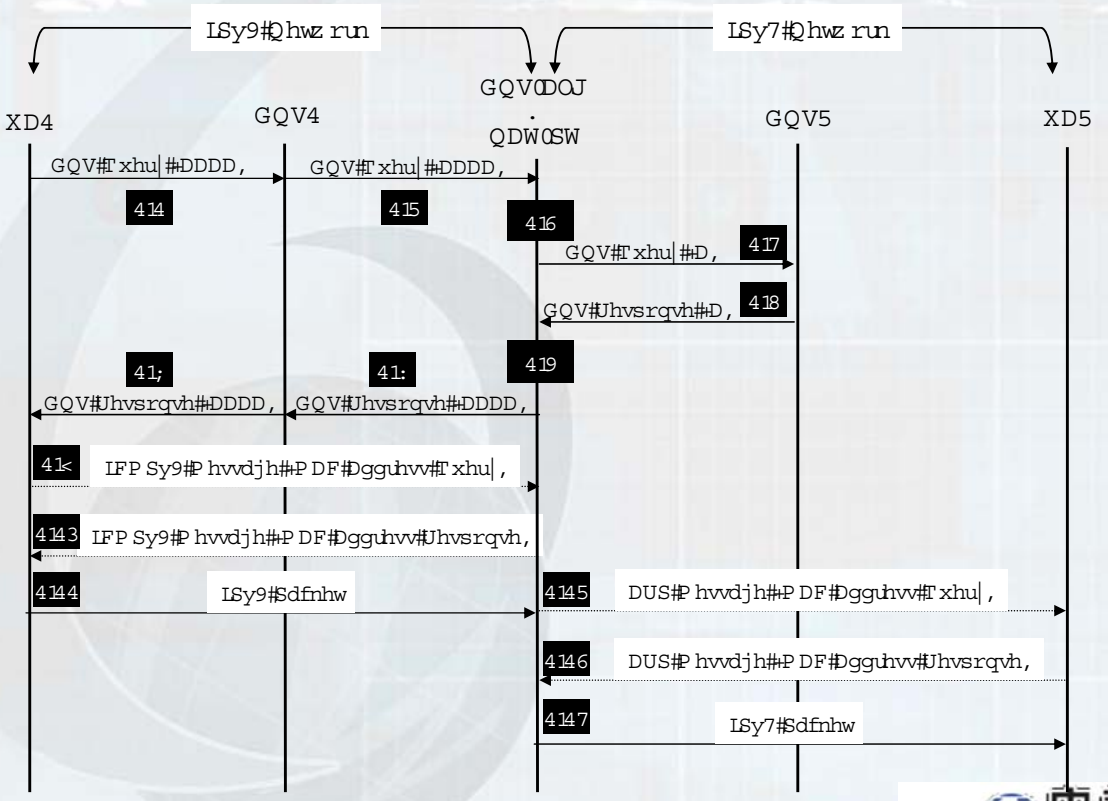
- ALG 是對應於特定應用程式的代理人，用來讓V6 node 可以和V4 node 互相溝通。有些應用程式會把網路位址存在封包的payload 中，可是NAT-PT 本身並無法得知payload 裡存的是什麼。ALG 可以協助NAT-PT 來達到這個功能。

DNS-ALG (1/2)

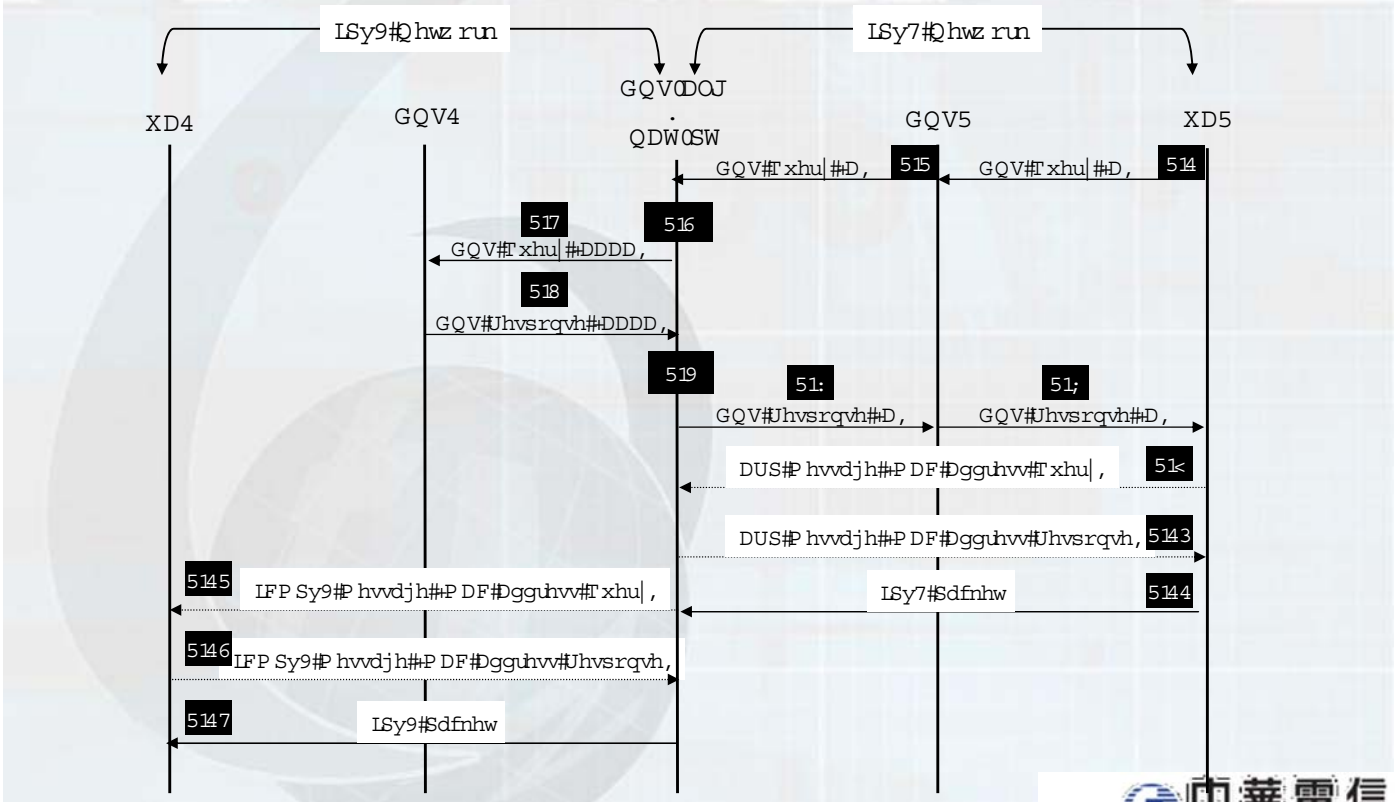
- 在沒有DNS-ALG 的情況下，NAT-PT 只能做到v6 建立連線到v4，v4 無法透過NAT-PT 向v6建立連線。
- V4 to v6 的連線之所以需要DNS-ALG 的協助，是因為一開始，v4 node 並不知道NAT-PT 會給v6 node 的替代v4 address 。



NAT-PT operations with DNS-ALG (IPv6→IPv4)

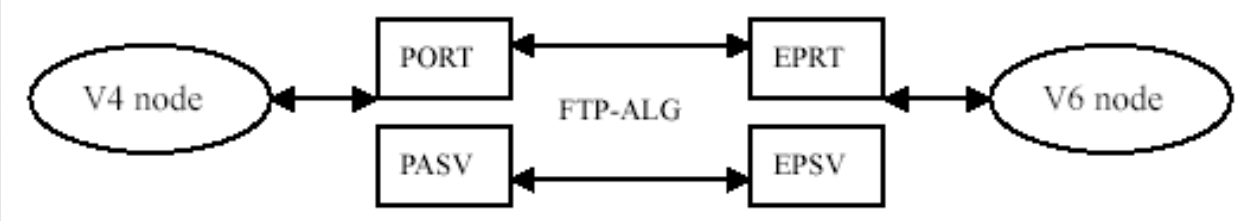


NAT-PT operations with DNS-ALG (IPv4→IPv6)



FTP-ALG

- FTP control message 中會攜帶IP address 以及TCP port 資訊，FTP-ALG 可以支援NAT-PT 使得FTP在application level 的轉換沒有問題。在RFC2428中建議利用EPRT和EPSV兩個指令分別替代PORT和PASV 指令。



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。

穿隧(Tunneling)技術優缺點比較表

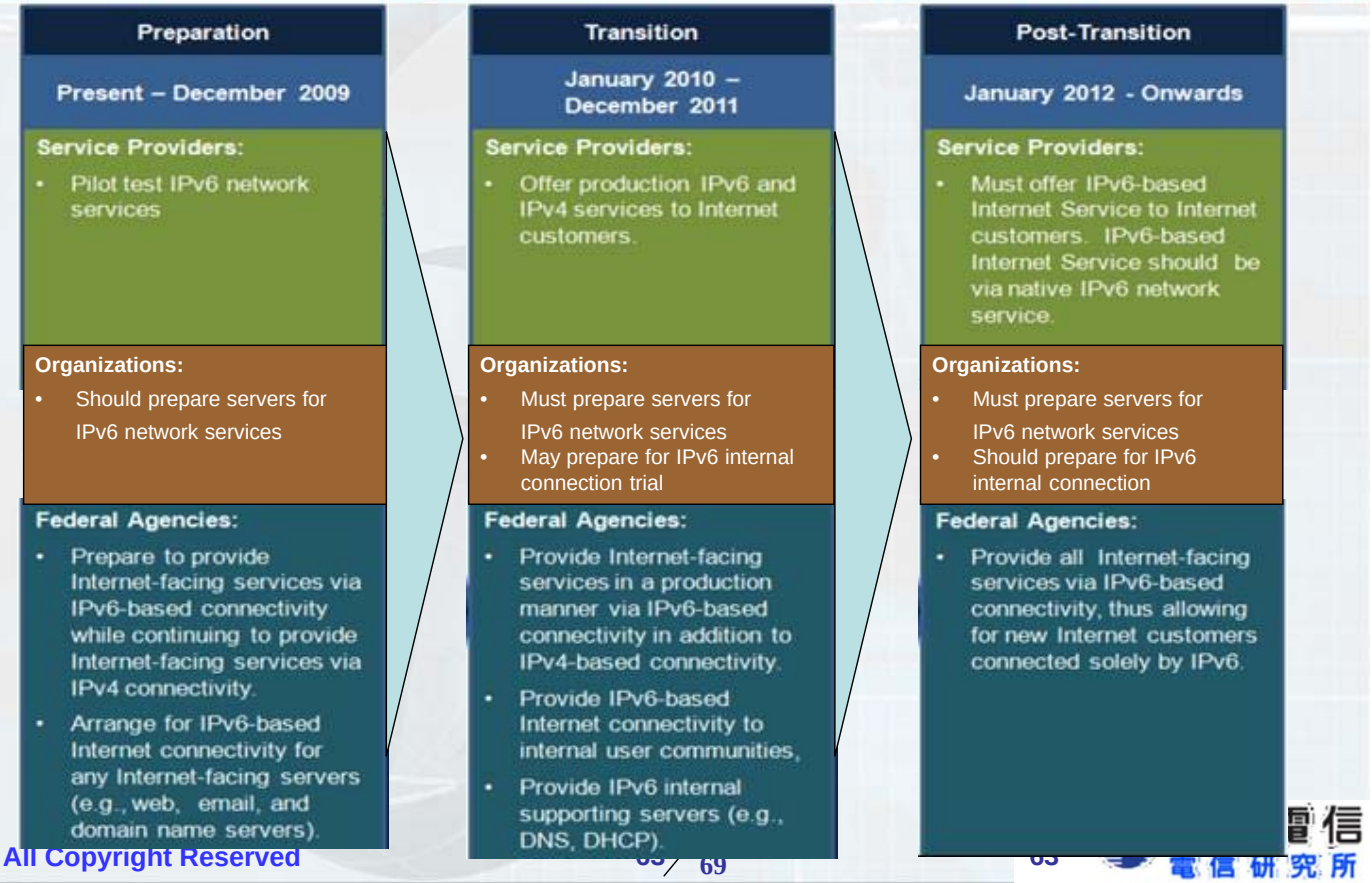
IPv4/IPv6穿隧(Tunneling)轉移技術	
優點	缺點
節點對節點的連線方式未遭破壞。	需要IPv4網路架構。
利用現有IPv4網路，可降低成本。	無法解決IPv4位址不足的問題。
	封裝及解封裝增加網路額外負擔。
	需要人工的設定與維護，增加網管者沈重的工作負擔。

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。

目 錄

RFC 5211 - An Internet Transition Plan



ISP responses to IPv4 exhaustion (1/3)

- 啟動回收機制
  - 優點：當IPv4位址用罄時，或可解決短期需求
  - 缺點：效果可能不佳，依賴此方案將使ISP陷入風險之中，亦無法滿足長期發展之需求
- 建置CGN (Carrier grade NAT) ，雙層NAT
  - 優點：可解決IPv4位址不足問題
  - 缺點：許多應用不適合於雙層NAT；網管/查測不易；CGN易成訊務/資安瓶頸點；擴展性受限；IPv6發展停滯

ISP responses to IPv4 exhaustion (2/3)

- 將網路與服務IP dual stack化
  - 優點：解決IPv4位址不足問題；單一網路與服務同時滿足IPv4 & IPv6用戶，網路與服務共享，整體成本有效降低；
  - 缺點：自然汰舊換新僅能達到點狀分佈，有些環境dual有些沒有，反而增加整體導入複雜度，而一次大規模IP dual stack成本又高；
- 新建IPv6網路，與IPv4網路獨立
  - 優點：不影響既有網路與服務；導入IPv6問題相對單純；IPv6新服務之研發亦不會受到既有IPv4網路之限制
  - 缺點：需同時建置兩套網路與服務平台，導入IPv6成本大幅增加，降低業者導入意願；兩個網路的服務無法直接共享
  - 代表業者: NTT East/West

ISP responses to IPv4 exhaustion (3/3)

- Shared address solution (SAS)
  - “建置CGN，雙層NAT”之改良版，嘗試與IPv6結合，但只用一層NAT即可達到一個public IPv4位址為許多用戶共用的目標
  - 關鍵點：在大部分的proposals中，Port被拿出來作為用戶區別之用
  - 優點：大部分既有適用於單層NAT之應用不受影響；可解決IPv4位址不足問題；與IPv6結合，IPv6發展持續
  - 缺點： 因Port另有用途，將使部分應用受到影響；CGN易成訊務/資安瓶頸點；UPnP應用會受到影響；IPS/IDS機制將受到影響
  - 代表業者：Comcast

Port distribution & reservation

- 因為SAS將Port拿出來作為用戶區別之用，因此用戶及應用不能再隨意的使用port number，而須由ISP來管控與分配
- How long an application session is ongoing and requiring port stability?
- 統計發現，一個用戶使用的port number範圍遠高於平均使用的port number數目
- ISP如何管控、分配與保留Port給用戶將是Shared address solution的成敗關鍵

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