『前瞻及完整之 IPv6 生態系推動方案』

附錄二
『ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練』教材

目錄

一、 第一場教材


ICP IPv4/IPv6
雙協定網路安全防護
技術人才培訓
教育訓練
點進網域新視界！
國立虎尾科技大學 電機工程系
蘇暉凱 副教授
hksu@nfu.edu.tw
1


TWNIC
財團法人
台灣網路資訊中心
簡介
點進網域新視界！

- 財團法人台灣網路資訊中心(TWNIC)是一個非營利性之財團法人機構，在交通部電信總局及中華民國電腦學會的共同捐助下，TWNIC於民國88年12月29日完成財團法人設立登記事宜，『財團法人台灣網路資訊中心』正式成立

- 主管機關乃為交通部，民國106年12月22日完成主管機關變更為國家通訊傳播委員會。捐助章程中規定TWNIC為我國國家級網路資訊中心(National Network Information Center)

3

服務宗旨如下：

- 非以營利為目的，以超然中立及互助共享網路資源之精神，提供註冊資訊、目錄與資料庫、推廣等服務。
- 促進、協調全國與國際網際網路(Internet)組織之間交流與合作，並爭取國際網路資源及國際合作之機會。
- 協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換。
- 協助或支援政府辦理各項事務，並推動網路資訊相關公益事務。

4

- TWNIC是目前國內唯一統籌網域名稱註冊及IP位址發放之超然中立之非營利性組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。

- 期盼更多人的參與及不斷檢討改進，為我國網際網路事業提供最佳服務，是TWNIC成立為財團法人之最大目的。希望各界也能不斷給予TWNIC更多的支持予鼓勵，使我國網際網路事業能更健全、更快速的發展。

5

- TWNIC是目前國內唯一統籌網域名稱註冊及IP位址發放之超然中立之非營利性組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。

- 期盼更多人的參與及不斷檢討改進，為我國網際網路事業提供最佳服務，是TWNIC成立為財團法人之最大目的。希望各界也能不斷給予TWNIC更多的支持予鼓勵，使我國網際網路事業能更健全、更快速的發展。

5


第32屆TWNIC IP
政策資源管理會議
「第32屆TWNIC IP政策資源管理會議」歡迎您踴躍報名參加！
2019-04-30 | 活動訊息
.tw To the World
泰文.tw 邁向域名國際化
泛用型網域名稱新增泰文IDN註冊公告事項
2019-05-17 | 中心公告
韓文.tw
邁向域名國際化
泛用型網域名稱新增韓文IDN註冊公告事項
2019-05-17 | 中心公告
2019 網路治理研習營
「2019 網路治理研習營」開放報名!
2019-05-08 | 活動訊息
「網路社群與數位合作」專家座談會
2019-05-06 | 活動訊息
ICANN APAC-TWNIC
ICANN與TWNIC共同在台北舉辦網路論壇
2019-04-18 | 活動訊息
7


IP/DNS 論壇
IP / DNS 論壇
@IPv6up.tw
首頁
貼文
關於
已說讚
追蹤中
分享
傳送訊息
IP / DNS 論壇
域名之友
@twnicNEWS
首頁
貼文
影片
讚
追蹤
分享
傳送訊息
Marco TeaLand
竹籃裡的山茶園
8

點進網域新視界！

IPv4/IPv6雙軌運作概念介紹

什麼是IP?

IP (Internet protocol) 電腦在網際網路上用來辨認溝通彼此的方法， IP位址就像是每家都有的門牌地址。

當我們上網或送email時，所打的網域名稱(如www.twnic.net.tw)會轉換成210.17.9.228網址，根據這個網址，網際網路就可以將訊息送到指定的主機。

10

IP的角色

網路的門牌號碼：IP address

位於網路堆疊的中心位置，兼容不同的網路介面

對 Transport Protocol 或 Application

提供統一的通訊方式。

11

擁擠的IPv4網路世界！？

目前分配給電腦的位址稱為IPv4位址
其位址格式是由4組 0~255的數字排列組成的
210.130.1.1

算算看，總共有2的32次方個位址可以使用
4,294,967,296看起來很多嗎?

新的電腦就再也擠不進網路世界了?

12

IP位址分配的組織

以紐約的IANA為中心（現委由ICANN管理）
其下再依區域分成五個區域註冊中心(Regional Internet Registries)

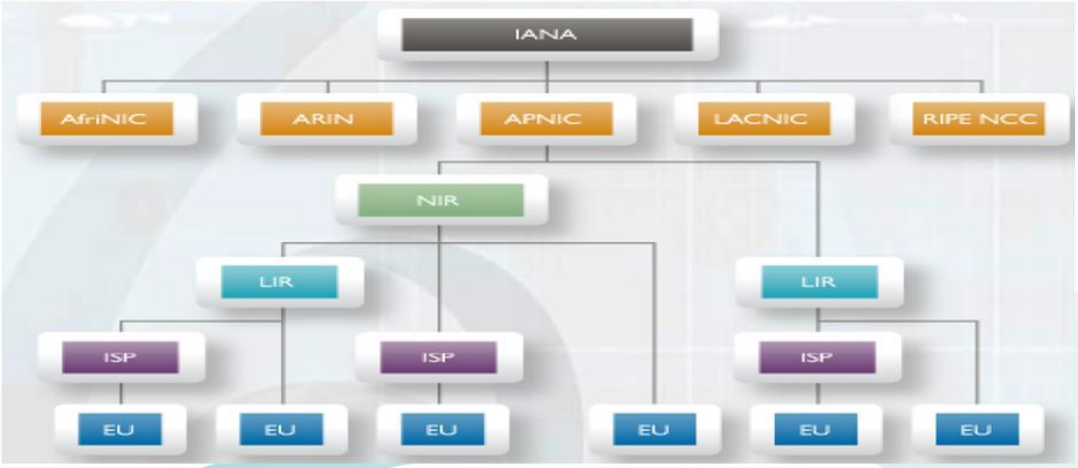
–歐洲地區：RIPE NCC
　　Réseaux IP Européens Network Coordination Centre
–北美地區：ARIN
　　American Registry for Internet Numbers
–亞太地區：APNIC
　　Asia Pacific Network Information Centre
–拉丁美洲：LACNIC
　　Latin American and Caribbean Internet Addresses Registry
–非洲: AfriNIC
　　Africa Network Information Centre

13

全球網際網路號碼管理架構

14

位址指派機構之階層式架構圖



以亞太地區來說，可透過 NIR (National Internet Registry) 將資源發放給LIR (Local Internet Registry，一般皆為ISP) ，LIR 再將資源指定分發給其客戶。

如此階層式的組織不但使得資源分配及管理更有效率
可避免資源過度集中，避免不公平的資源分配

15

IPv4 位址定址方式

1994年以前 Classful

分類網路（Classful Addressing）或稱「分級式定址」，是在 1993年左右用於描述網際網路的網路體系的一個術語。 它將IPv4的IP位址分成五個類別

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

1994年以後 Classless

16

IPv4 位址的分配類別

類別	網路位址	主機位址	最多主機數量	可分配的組織數
A	8位元	24位元	16,777, 214	128
B	16位元	16位元	65,534	16,384
C	24位元	8位元	254	2,097,152

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

17

IPv4位址枯竭影響與衝擊

- 影響
  - 無IPv4位址來提供新型態網路服務
  - 既有網路服務無法擴展
- 衝擊
  - 將造成網際網路發展停滯
- 解決方案
  - 使用NAT技術
  - IPv4 to IPv6位址移轉技術
  - 回收未使用的IPv4位址
  - 全面佈署IPv6
  - 其他

18

IPv4位址枯竭因應措施

- 開源
  - 開放保留的IP位址
  - IP位址的移轉或交易
  - IP位址的回收等等
- 節流
  - 調整現行的IP位址發放原則
  - 使用NAT相關技術延緩
- 進行IPv6的佈署
  - 分階段實行

19

IPv4位址枯竭因應建議策略

因應措施	開源(回收、移轉)	節流(使用NAT)	部署IPv6
優勢 (Strengths)	無技術門檻與實施費用	屬於現有成熟技術，可大量節省IP位址的使用，花費比部署IPv6相對便宜	擁有大量的位址，可根本解決位址不足問題
劣勢 (Weaknesses)	無確實可行的方法(回收或移轉均無好的實行經驗)，也非長期可行政策	NAT本身對一些應用的連線所有限制、每一個網路使用者需要的連線數正快速增加中，減少可共享一個IP的使用者數	對於大量實施在一些技術上仍有顧慮(如設備能力不足、安全性尚未完整考量)且部署費用相對較高

20

IPv4位址枯竭因應建議策略

因應措施	開源(回收、移轉)	節流(使用NAT)	部署IPv6
機會 (Opportunities)	有不少可回收位址(約有50個/8未出現在BGP routing table中、36個/8是歷史或特殊用途位址)	短期內有可能是唯一便宜可行的技術	唯一長期的解決方案，極有可能是未來會被全面採用的協定
威脅 (Threats)	合法擁有的IP位址要回收不容易，需擁有者願意配合	非長期解決方案且對於大量的使用者、電信等級的NAT均仍有待市場考驗	尚無明顯看到IPv6使用者市場，讓大部份的公司採觀望態度

21

IPv4所遭遇的挑戰

- IP位址有限，多人(戶)共用一個位址

- NAT雖可減緩位址之消耗，但是
  - 終究抵擋不住新興市場需求(如金磚四國)爆發性需求。
  - 2010年全球上網人口約16.9億　仍迅速增加中！

- 行動上網需要更多IP位址及行動能力(Mobility)支援
  - IPv4位址不足外，Mobility支援能力先天不足。

- 資源分配不均
  - 2010年1月底美國上網人口2.2億，擁有超過50%以上之IP位址
  - 2010年1月底中國上網人口3.6億，僅擁有不到6%的IP位址

22

IPv4技術本身的缺陷

- 數目限制：
  - IPv4的網路位址只有32位元
  - 採用Class的方式劃分區域較缺乏彈性
- 效能問題：
  - 在IPv4上面實做「QoS」服務極為困難。
  - CIDR的出現導致網路管理上的困難。

23

IPv4技術本身的缺陷

- 安全問題：
  - IPv4無法在基本網路層提供安全的加密通訊
- 組態設定：
  - DHCP伺服器安裝、設定、維運不易
  - 全自動化的組態設定

24

IPv4技術本身的缺陷

IPv4不只無法支應快速成長的位址需求
它的缺點是無法支援網路安全及國際漫遊的能力

IPv4 需要利用網路位址翻譯器
(Network Address Translator；NAT)

對經營者而言，它就增加了成本及管理上的負擔

25

為何需要IPv6？

解決 IPv4 的問題

–發生 IPv4 位址不足
–NAT 的應用增加
–對等式 (Peer-to-Peer) 網路技術問題
–行動設備的支援性

26

為何需要IPv6？

下一代 Internet 的標準

–IETF 已完成 IPv6 核心網路的標準
–全球將邁入 IPv6 新世紀 (例如：4G、 5G)
–行動裝置、 P2P 軟體應用
–IPv6的安全性

27

為何需要IPv6？

IPv6與物聯網社會

–P2P通信、無國界通信
– End2End security
–與雲端運算特性結合
–利用IPv6實現物聯網服務與應用

28

IPv6的發展 (1/2)

1992年，IETF之IPv4的Address空間不足的問題開始被檢討

1994年，下一代的網際網路協定開始被提案，包括三項
CATNIP (Common Architecture for the Internet)
TUBA (TCP/IP with Bigger Addresses)
SIPP (Simple Internet Protocol Plus)

1995年，SIPP被更名為IPv6
IPv6的規範將被RFC1752公開
(The Recommendation for the IP Next Generation Protocol)

29

IPv6的發展 (2/2)

1998年，IPv6之位址架構與通訊協定之規範分別在RFC2373 (IP Version 6 Addressing Architecture)與RFC2460 (Internet Protocol Version 6(IPv6) Specification)公開。

1999年，全球第一個業界團體(共有42個單位加盟)成立了「IPv6 Forum」。ARIN 將全球第一個之IPv6 Prefix：2001:400::/35授予給 Esnet (能源科學網)。

2002年，全球各區域性的Internet Registry RIR(Regional Internet Registries)實施新的「IPv6 Address Allocation and Assignment Global Policy」

30

IPv6之優點與支援狀況

- IPv6 發展之優勢(相對於IPv4)
  - 足夠的位址空間
  - 彈性的聯網機制 (Plug & Play)
  - 安全機制
  - QoS功能增強
  - 強化的 Mobility 與 Multicast 能力等

31

IPv6之優點與支援狀況

- 標準已臻完備

  2007年底止 IETF通過191項RFC標準，幾乎涵蓋所有IPv4既有標準。

- 軟硬體設備支援已漸成熟

  各式作業系統皆支援IPv6

32

IPv6之優點與支援狀況

•尚未蓬勃發展的主要因素

–IPv4位址尚未迫切短缺，普遍以不變應萬變
–發展期過長，不斷在IPv4技術上尋求解決方法
–許多IPv4 applications均將NAT issue考慮在內

–尚無法找到有明確利基的IPv6 Business Model
(IPv6 應該是標準，而不是應用)

33

什麼是IPv6?

v = version= 版本
IPv6 就是第六版的IP規範

IPv6總共有2的128次方個可以使用，IPv6位址寫法為八組四個位數，每位數是由16進位的0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f 所組成，中間用冒號分隔 2001:0c50:ffff:0001:02e0:18ff:fe95:b229

34

什麼是IPv6?

別擔心這麼一大串背不起來

我們日常上網還是以使用網域名稱

例如 www.twnic.net.tw

系統會自動轉換網域名稱為IPv6位址

所以一般使用者不需要直接輸入IPv6位址

35

IPv6 位址表示法

IPv6使用128 Bit的位址空間

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

用以下位址為例

20030000000000B30000000000001234

(太長容易記錯)

36

IPv6 位址表示法

>2003:0000:0000:00B3:0000:0000:0000:1234

(分為八段，以冒號分隔)

簡寫規則:

1.每 32 Bit 如開頭之 4bit 表示為 0，即可省略

2.若 32 Bit 全為 0，則可簡寫為0

3.若連續完整之 32Bit 段落皆為 0000，則可全省略，簡寫為::，但以一次為限

>2003:0:0:B3::1234 (簡寫)

37

IPv6 位址表示法

請還原

2001:e09:6910:100::1

請用簡寫寫法表示

2001:0f08:5800:0009:0052:0000:0000:0101

38

IPv6位址範例

www.ipv6.hinet.net
  2001:b000:180:3::5
  202.39.224.5

www.twnic.net.tw
  2001:c50:ffff:1::9999
  124.9.9.9

39

使用IPv6的理由

- 提供更多的IP位址空間
  - 滿足未來IPv4可能不足的危機。
- 更好的資料傳送品質管理(QoS)
  - 對於多媒體影音有更好的QoS支援。
- 更契合無線行動通訊的協定
  - 利用Mobile IPv6協定，增加IP定址的便利性與縮短資料傳送延遲的時間。
- 強化的安全機制(IPSec)
  - 確保End-to-End(端點到端點)的安全。

40

IPv6的五個主要優點

1. 數量多，非常多
2. 服務品質保證(QoS, Quality of Service)
3. 隨插即用
4. 點對點傳輸
5. 使用更安全

41

優點一：數量多，非常多

• IPv6位址總共有2的128次方個可以使用，也就是有340282366920938463463374607431768211456個IPv6位址可以使用

•一平方公尺能有多少IPv6的位址呢？以地球總面積來算算看，地球總面積約5億1仟萬平方公里，每平方公尺將有655570793348866943898599個IPv6的位址(約有6仟5佰萬兆個)

42

優點二：服務品質保證(QoS)

•QoS是一種控制機制，傳統的IPv4 網路並未提供完整的QoS機制，訊息的傳遞未被分類，全部擠在網路上爭先恐後是造成網路擁塞的主因之一。

•IPv6的應用主要特色有：提供順暢、有秩序的網路傳輸將網路資源分級與分類，通過流量控管保持網路傳輸的順暢。

43

優點二：服務品質保證(QoS)

•這就像車輛走在道路上，不同的車種走不同的通道，快速而有秩序的通過以保待通道的順暢性。提供特定標籤給特殊需求者優先的服務權，如緊急醫療服務系統、119、110…等社會緊急資源的應用。

•透過IPv6與建全的QoS機制能確保即時線上的連線、防止服務中斷以及提高網路的效能，讓訊息傳輸達到一定的水準。

44

IPv6優點三：隨插即用

•在未來世界裡具有IPv6功能的家電及設備，只要啟動開關立即可變成IPv6網路的一員。

• IoT 的大量運用

45

IPv6優點四：點對點傳輸

在IPv6的世界裡，每個上網的人都有專屬的位址，這使得點對點的運用變得更便利，如網路電話、視訊傳輸，可即時快速的傳送給對方。

46

IPv6優點五：使用更安全

IPSec是過去為了解決IPv4的安全性問題所產生的IP安全協定

IPv6將IPSec納入其架構中

讓IPSec直接可以鑲嵌在IPv6的封包中

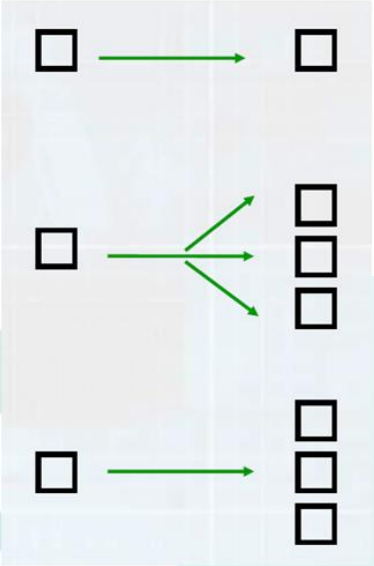
47

Basic Address Types

•Unicast (點對點傳輸)

•Multicast (群播傳輸)

•Anycast (多點備援傳輸)



48

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

49

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

```
|          n bits          | 64-n bits |        64 bits              |
+--------------------------+-----------+-----------------------------+
| global routing prefix    | subnet ID |        interface ID         |
+--------------------------+-----------+-----------------------------+
```

50

Network ID 設定與配送機制

1.採用Neighbor Discovery (ND)指派 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)

51

Interface ID

- Unique to the link
- Identifies interface on a specific link
- Can be automatically derived
  - IEEE addresses use MAC-to-EUI-64 conversion
  - Other addresses use other automatic means
- Can be used to form link-local address
- Can be used to form global address with stateless autoconfiguration

52

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)

53

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 02C0:3FFF:FEBB:9391

54

Global Unicast Address

•Global routing prefix: The global routing prefix is designed to be structured hierarchically by the RIRs and ISPs.

•Subnet ID: An identifier of a link within the site. The subnet field is designed to be structured hierarchically by site administrators.

•Interface ID: Identify interfaces on a link. They are required to be unique within a subnet.

```
|          n bits          |   m bits  |        128-n-m bits          |
+-------------------------+-----------+-----------------------------+
| global routing prefix   | subnet ID |        interface ID          |
+-------------------------+-----------+-----------------------------+
```

```
|          n bits          | 64-n bits |        64 bits               |
+-------------------------+-----------+-----------------------------+
| global routing prefix   | subnet ID |        interface ID          |
+-------------------------+-----------+-----------------------------+
```

55

Global Unicast Address 分配表(部份)

Prefix	說明
2001::/16	IPv6 Internet, ARIN, RIPE NCC, LACNIC
2002::/16	6to4 Tunnel 專用
2003::/16	IPv6 Internet RIPE NCC
2400:0000/19 2400:2000::/19 2400:4000::/21	IPv6 Internet APNIC

56

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

57

IPv4 vs. IPv6

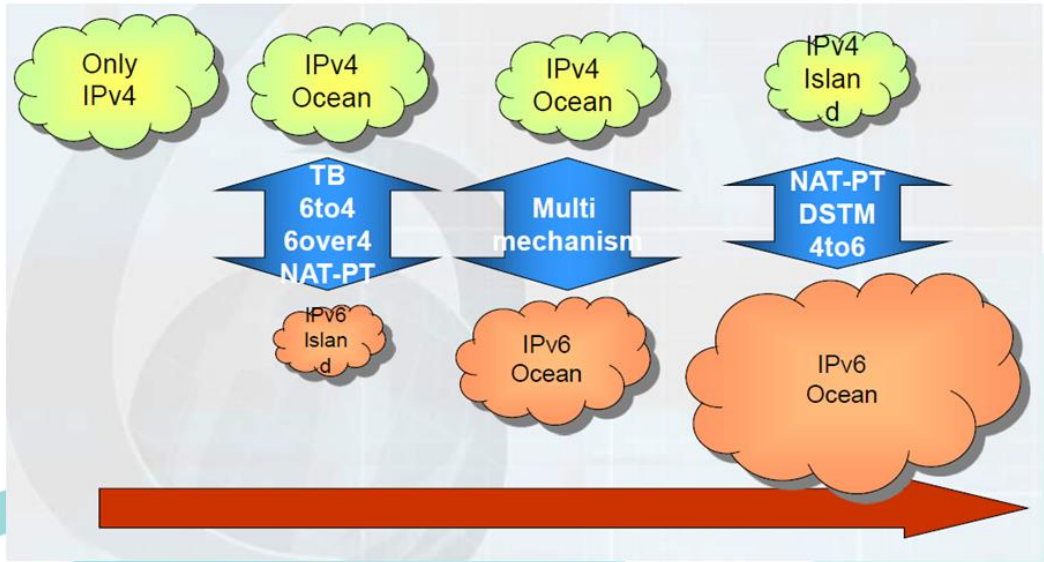
Version	IPv4	IPv6
位址空間	2^32 ＝4,294,967,296	2^128 ≒3.4*10^38
ICMP發放方式	以廣播(Broadcast)方式	以群播(Multicast)方式
QoS策略	推測遺失資料與暫存器	資源保留與優先等級
協定的可擴充性	沒有彈性(最多提供1個Option欄位的擴充)	較有彈性(具有延伸標頭)
IPSec的支援	本身沒有支援，需額外設定	將IPSec納入本身協定中
Plug and Play	需透過DHCP分配IP	具有Statefull (透過DHCPv6)與Stateless (自動組態)分配IP
繞回位址	127.0.0.1	::1
表示方式	十進位表示，以點分隔	十六進位表示，以冒號分隔

58

點進網域新視界！

IPv4/IPv6雙軌環境建置概述

轉型趨勢



60

現有IPv4服務環境的限制

- 無法提供目前網際網路連線所需要的位址空間
- 依靠Broadcast的機制，對網路及伺服器效能產生Overhead
- 沒有普遍被公認而應用於網路設備及應用系統的Quality of Service管理機制。
- 在傳輸時的資料安全性不足

61

現有IPv4服務環境的限制

以上所提之限制，只包含了IPv4缺點之一部份

但已足夠說明IPv4是一個無法滿足現在與未來

網際網路需求的通訊協定

IPv6對於以上的缺點，均內建了解決方案。

62

IPv6可解決的問題

- 在技術問題上，可消除IPv4位址不足，移動性不足的限制，並使用QoS及IPSec的機制提高重要服務的傳輸品質與資料傳輸安全。
- 在經營問題方面，可降低ISP業者的營運成本與克服NAT障礙而產生的技術成本，並可為使用者創造新的服務。

63

IPv6可解決的問題

使用IPv6來解決目前IPv4所產生的問題

會比研發IPv4的新技術來解決IPv4的問題

採用 IPv6 會更為有效

並對ISP業者的投資更有保障

64

三大類過渡技術

1. IPv6/IPv4 Dual Stack

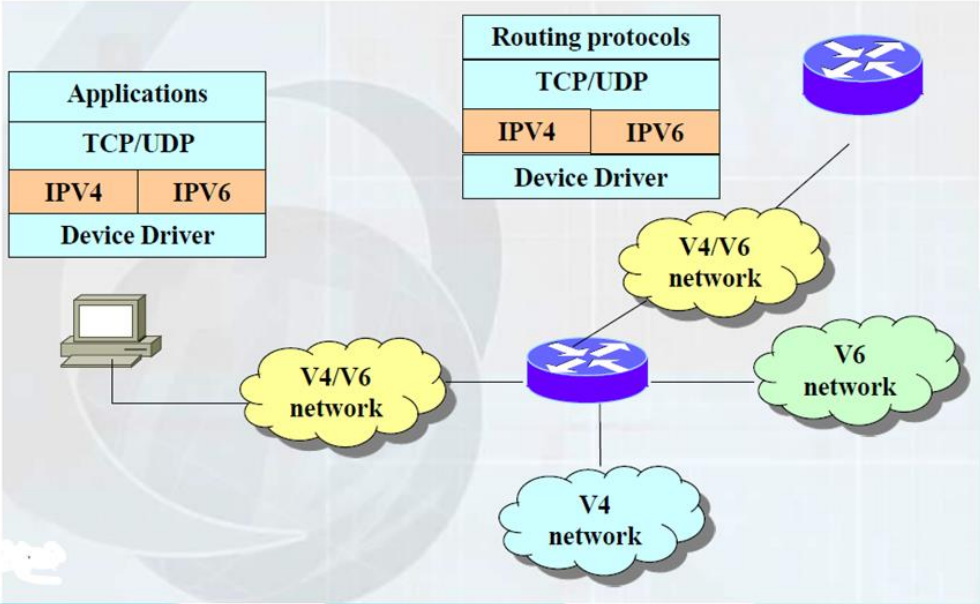
即在同一條線路上

同時提供IPv6及IPv4的通訊協定

最為推薦的方案

65

Dual Stack Mode 示意圖



66

三大類過渡技術

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

67

Tunneling 系統的元件

Tunnel 大致包含了下列元件

- Tunnel Server: 提供Tunnel 服務之局端設備
- 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
- 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

68

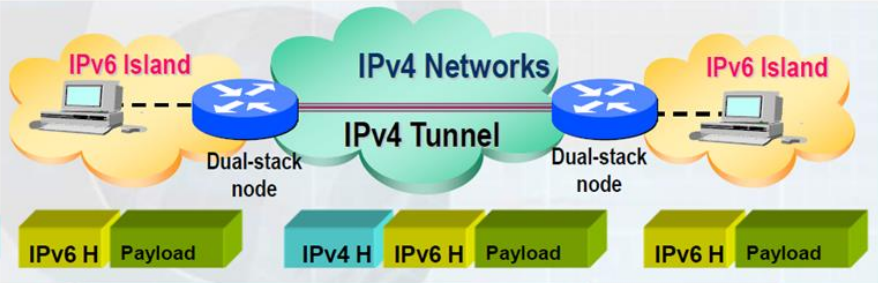
Tunnel 的種類(一)

• Configured Tunnel: 手動設定之Tunnel

適用於ISP與企業用戶間的IPv6 Tunnel連線

優點:安全性高，可支援IPv6 Multicast

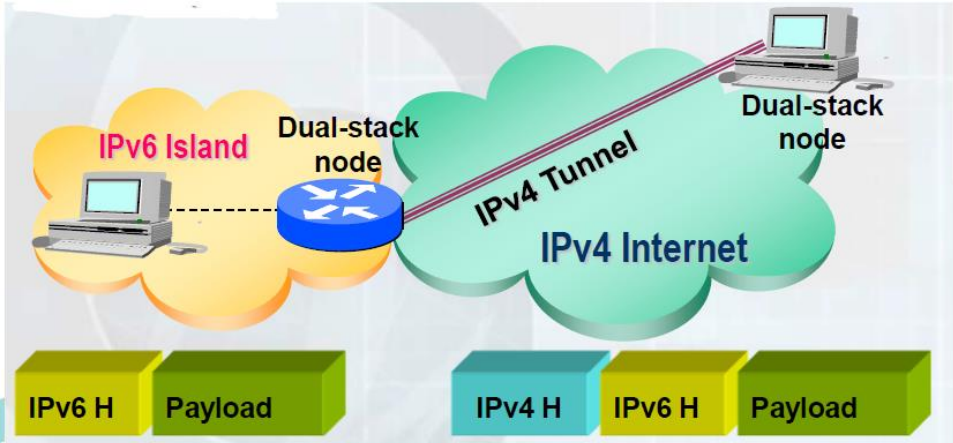
缺點:設定之工作負擔很重



69

Tunnel 的種類(二)

• Automatic Tunnel



70

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部署。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。

71

Tunnel Broker System

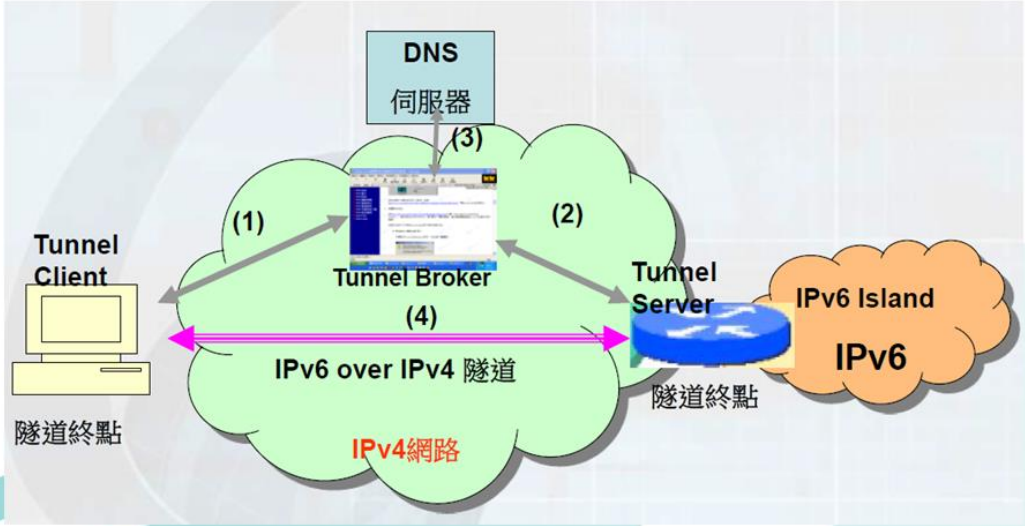
由於Automatic Tunnel 無法有效進行安全管控，而Configured Tunnel 需要太多的手動設定。

而造成ISP不願意提供IPv6 Tunneling Service. Tunnel Broker 可為Configured Tunnel及網管人員提供較佳的管理方式，使IPv6 Tunneling Service 的商業化提供了可行的途徑。

但對一般使用者而言，仍然不夠方便

72

Tunnel Broker 系統示意圖



三大類過渡技術

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

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

75

Translator 技術之限制

事實上，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。

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

76

點進網域新視界！

IPv4/IPv6雙軌網路環境建置

Router, Firewall, Load Balance

第一部分

DHCP

IPv4網路位址指派方式主要有
固定位址指派及動態位址指派兩種

固定位址配置需要手動設定，主要應用於伺服器主機及網路設備，動態位址配置大多透過 DHCP 協定 (Dynamic Host Configuration Protocol)

由 DHCP 伺服器進行位址指派。

78

IPv6同樣提供固定位址指派
在自動位址指派的作法上則有三種方式

- 無狀態位址自動指派
  (Stateless Address Autoconfiguration, SLAAC)
- 無狀態
  DHCPv6(Stateless DHCPv6)
- 全狀態
  DHCPv6(Stateful DHCPv6)。

79

在實際運用上，辦公室環境建議使用Stateful DHCPv6，對資訊安全可以得到最佳管控

家用網路則建議使用Stateless DHCPv6，系統簡化又符合使用需求，純粹的物件感測網路則可以使用SLAAC，設定最為簡單

針對各種不同的IPv6位址指派技術進一步說明

80

人工指派位址

與IPv4網路設定固定位址的做法相同，逐台主機人工指派IPv6位址、預設閘道與DNS伺服器位址

一般而言，路由器與DMZ伺服器的IPv6位址建議採用人工指派，以方便於防火牆設定資安政策，IPv6位址尾碼可以選擇與IPv4位址相同，便於管理及記憶

在使用固定位址的DMZ網段，建議要關閉RA (Router Advertisement)的發送，以避免成為資安漏洞。

81

SLAAC或SLAAC+RDNSS

無狀態位址自動指派(Stateless Address Auto-configuration, SLAAC)

做法是路由器會透過 Multicast 定期發出路由公告 (Router Advertisement) 的封包給用戶端主機，RA的資訊包含 /64 Prefix (Network ID) 及Default Gateway的資訊，主機收到Prefix會與自行產生的Host ID(主機識別碼)組合成為該主機的IPv6位址

82

SLAAC或SLAAC+RDNSS

由於位址指派後即不再持續管理這個位址的使用情形，所以稱為「無狀態」。

上述提到的主機識別碼(Host ID)有兩種產生方式，一種是使用EUI-64運算法，從主機的MAC address轉換而來，另一種是使用亂數法產生

83

SLAAC或SLAAC+RDNSS

早期SLAAC不支援指派DNS伺服器位址

後來的標準解決了這個問題

稱為SLAAC + RDNSS

84

Stateless DHCPv6

這個做法是結合 SLAAC 及 DHCPv6 指派DNS的功能，進行無狀態位址自動指派，以解決前述無法獲得DNS資訊的問題。

在分工上 SLAAC負責 IPv6 位址及 Default Gateway指派，DHCPv6則提供DNS伺服器位址及其他資訊，如NTP

85

Stateless DHCPv6

實作上是透過設定RA封包的一個控制位元(稱為O-bit)來協調用戶端主機的作業。

如果主機收到O-bit為0的RA，就是前述SLAAC的作法；如果O-bit為1，用戶端主機就會再向DHCPv6伺服器請求指派DNS伺服器位址。

86

Stateless DHCPv6

透過SLAAC指派IPv6位址時，並不會進行IPv6位址的定時更新維護及使用追蹤，所以稱為無狀態DHCPv6位址自動指派

在資安管理上不易由IPv6位址追蹤到使用者，因此比較適合不須嚴格進行資安查核管理的場所使用，例如私人家裡。

87

Stateful DHCPv6

在這個做法裡RA只負責提供Default Gateway，而IPv6位址(包括Prefix、Host ID)及DNS伺服器位址的指派均由DHCPv6負責，實作上是透過RA封包的兩個控制位元進行協調。

當用戶端主機收到M-bit及O-bit均為1的RA，主機就會再向DHCPv6伺服器請求指派IPv6位址及DNS伺服器位址。

88

Stateful DHCPv6

由於經由DHCPv6指派IPv6位址時會記錄IPv6位址與MAC位址的對應表，並經由定期更新位址以維護使用紀錄，所以稱為全狀態DHCPv6位址自動指派，對於需要嚴格進行資安查核管理場所是比較恰當的做法。

由於DHCPv6無法指派Default Gateway的資訊，所以Stateful DHCPv6仍需要與RA配合運作，將來DHCPv6可能會發展出提供Default Gateway的機制，這樣就不需要RA的協助。

89

派址方式	預設閘道	Prefix 指派	Host ID 指派	DNS 位址指派	說明	適用環境
人工配置位址	手動設定	手動設定	手動設定	手動設定	穩定可靠、較無資安疑慮，但無彈性、設定麻煩	伺服器及網路設備
SLAAC + RDNSS	RA 指派	RA 指派	EUI-64 或亂數法自動產生	RA 指派	簡單方便，但無法管理位址指派原則及使用紀錄，但大部分作業系統尚未支援 RDNSS	物件連網應用服務
Stateless DHCPv6	RA 指派	RA 指派	EUI-64 或亂數法自動產生	DHCP 指派	簡單方便，但無法管理位址指派原則及使用紀錄，另外，Windows XP 不支援 DHCPv6(可外掛)	家用網路環境
Stateful DHCPv6	RA 指派	DHCP 指派	DHCP 指派	DHCP 指派	可管理位址指派原則及使用紀錄，但 Prefix 與 Gateway 分由 DHCP 及 RA 指派，增加偵錯難度，另外，Windows XP 不支援 DHCPv6(可外掛)	辦公室網路環境

90

點進網域新視界！

IPv4/IPv6雙軌網路環境建置

Router, Firewall, Load Balance

第二部分

防火牆升級IPv6

網際網路的盛行，越來越多的攻擊技術也不斷的產生，如何有效的阻隔外在的威脅，「防火牆」便是一個重要的基本資安元件

「防火牆」(Firewall)是指架設在不同網路之間（例如需要保護的內部網路和公共的網際網路之間）的一系統設備，可能是硬體式的或軟體防護式的安裝於提供服務的設備上。

92

防火牆升級IPv6

在功能上，防火牆可有效地監控內部網路和網際網路之間的任何活動，提供基本的內部網路安全防護

通過監測、限制、更改要通過防火牆的「封包」或「Packet」，屏蔽內部需要受保護的網路資訊、結構和運行狀況，防止資訊洩露，以此來保護網路的安全

93

(一) 防火牆的基本原理

IP位址好比是電腦的「門牌號碼」，一部電腦便可比喻成一棟大廈，連接埠就像這大廈不同的入口，負責各種不同的業務，住戶，行人訪客，駕車的住戶或訪客，以及送貨的貨車等各有不同入口

所有的連接埠都會按通訊協定，被賦予不同編號，防火牆的功能就像大門的警衛保安員，監視進出大廈的訪客，禁止可疑人或物通過

94

(一) 防火牆的基本原理

最基本的防火牆型態是僅由單一的封包過濾器組成，防火牆網路外部的使用者在透過防火牆的封包過濾之後，才能接觸到網路內部的網際網路伺服器。

這種配置下，防火牆管制必須非常嚴格，只讓已經對外開放服務的流量通過，如對電子郵件傳遞，公司公開網站的存取等，合理安全的訪問才能進入防火牆所保護的內部網路系統，而一些危險性較高，不必要的服務如遠端載入等可阻檔在外，並且可以根據可疑份子建立黑名單，禁止這些可疑份子或是 IP address 的封包加以攔阻，不得通過

95

(二) 防火牆的重要性

常有人問「安裝了防毒軟體，還需要加裝防火牆嗎？」其實，防毒軟體與防火牆是相輔相成的

諾大的電腦網路就如同我們生活的國度，防火牆便如同在電腦系統執勤的海關人員，所有入境者，包括惡意程式想透過外部網路侵入內部系統，都要先經過防火牆的查驗，這也是防止駭客的基本防務

96

(二) 防火牆的重要性

防毒軟體其功能就像是機場內的緝毒犬以及操作X光機的檢驗人員，各司其職，構成雙重的保護網，希望能夠有效防止駭客的惡意病毒程式，達到

- 機密性(Confidentiality)
- 完整性(Integrity)
- 可用性(Availability)

避免境內的電腦或資料受到損傷。新型病毒為達到擴散的目的，也經常利用隱藏的連線來感染系統，所以正確設定防火牆也能有效地阻止病毒的攻擊

97

(三) 防火牆的限制

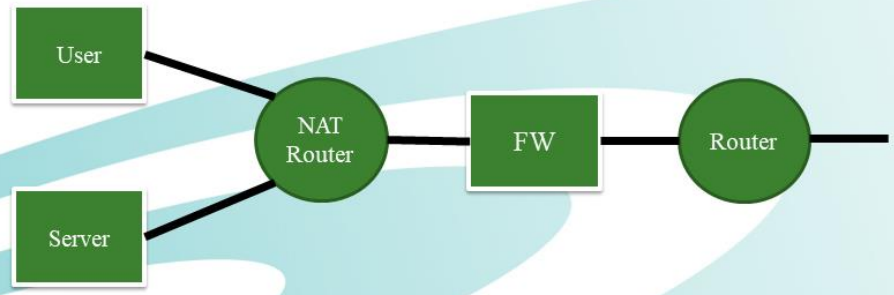
防火牆無法抵擋所有型態的訪問與攻擊，尤其傳統的防火牆運作在網路的第三層與第四層為主，對於應用層的攻擊或是session layer的攻擊往往需要搭配其它資安設備與策略進行防堵

新型態防火牆 Layer 7 Application Firewall

98

(一) 透通模式Transparent Mode

機關IPv4防火牆位置如設置於ISP 路由器與內部NAT路由器之間，並採用Transparent 透通模式進行運作，內部路由器最少有三個介面，一個與防火牆介接，一個與內部一般使用者連接，一個與伺服器區塊連接



99

(一) 透通模式Transparent Mode

採用本架構可以限制外來的訪客對於內部網路的存取，並且在不改變內部原有的設備設定，以提供內部使用者安全的IPv4/IPv6對外存取服務。

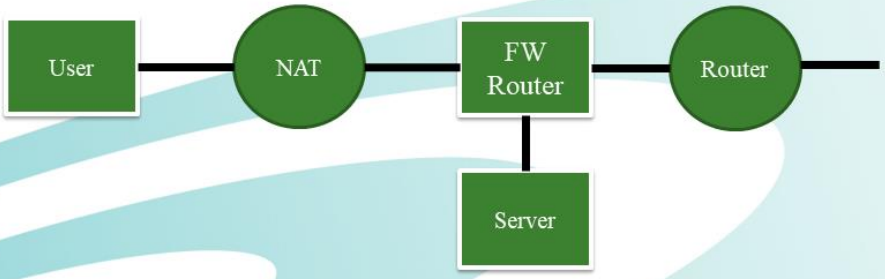
內部使用者若採用IPv6 Public IP address，不再經由NAT或PAT位址轉換，可直接提供IPv6接取服務。

防火牆可抵擋外部IPv4/IPv6對於內部使用者的所有連線訪問。

100

(二) 路由模式Route Mode

機關IPv4防火牆位置如設置於ISP 路由器與內部路由器之間，並採用Route Mode路由模式進行運作，防火牆最少有三個介面，一個與外部ISP業者介接，一個與內部路由連接，一個與DMZ伺服器區塊連接



101

(二) 路由模式Route Mode

採用本架構可以限制外來的訪客對於內部網路的存取，並且限制DMZ區對於內部使用者的存取，可以提供內部使用者安全的IPv4/IPv6對外存取服務。

內部使用者若採用IPv6 Public IP address，不再經由NAT或PAT位址轉換，可直接提供IPv6接取服務。

防火牆可抵擋外部IPv4/IPv6對於內部使用者的所有連線訪問。

102

點進網域新視界！

網路升級流程
步驟和檢查項目清單

網路升級流程步驟和檢查項目清單

升級清查目的在針對各項網路應用服務系統進行IPv6支援能力調查，藉以評估網路升級需進行之工作內容、作業程序及時程規劃。

升級清查作業從服務系統角度出發，逐一填寫對外提供服務的應用服務系統，其次應依據各服務系統逐一清查相關之軟硬體設備，包括伺服器、服務系統或軟體、基礎網路設備及其他相關設備等，參考步驟如下。

104

(一) 評估現有網路環境

網路設備種類甚多，唯有釐清設備功能，才能規劃IPv6升級優先順序，其中需調查項目如下：

- 技術人員IPv6相關能力調查
- 資訊應用服務系統(自行開發、委外設計或市購套裝軟體)
- 網路架構圖(區域網路、DMZ、連外網路、接取網路、核心網路、機房等)
- 硬體設備(使用年限與IPv6支援程度)
- 評估現有網路設備之屬性

105

大多數網路設備可分類成下列四項

1. 主機(Host)

2. Layer 2 交換器

3. Layer 3 網路設備

4. 網路安全防護設備

106

1. 主機(Host)：

單埠接收與傳送IPv6封包

個人電腦、筆記型電腦、伺服器

平板、手機

以下分類不屬於 Host

Layer 2交換器

Layer 3網路設備

網路安全防護設備

107

2. Layer 2交換器：

根據網路封包的Layer 2標頭執行網路封包交換技術，大多數設備不需要進行IPv6升級，亦即無需更換或進行韌體升級，如消費者等級Layer 2交換器和企業等級Layer 2交換器等。

但是部分企業/ISP等級Layer 2交換器功能較強，仍會偷偷看到網路封包的Layer 3標頭處理，如網管IP、Multicast Snooping或Protocol-Based VLAN等，亦需將此類設備納入IPv6升級考量。

108

3. Layer 3網路設備：

根據網路封包的目的位址欄位進行IPv6封包轉送處理之節點，例如：

路由器Router

Layer 3交換器

此為提供IPv6網路運作的基礎

109

4. 網路安全防護設備

此為選擇性地攔阻威脅性之網路封包或者限制網路流量的IPv6節點，例如：

防火牆(Firewall)

入侵偵測系統(IDS)

入侵防護系統(IPS)

110

(二) 規劃IPv6升級策略

根據上述調查結果，可大致掌握現有網路設備特性與屬性。接著需制定IPv6導入之網路範疇與時程，本步驟僅提供3個升級重要參考指標，作為規劃參考依據：

1. 降低導入成本：網路設備升級至IPv6非一蹴可幾，礙於導入預算成本之限制，需針對現有網路設備規劃階段性的升級工作

111

(二) 規劃IPv6升級策略

2. 規劃重要網路應用服務升級：

網路管理員可針對網路流量大或重要之網路應用服務，調查其服務之主要網路傳輸設備，並評估運作模式是否與IP層有關，以作為未來導入IPv6首要升級重點

3. 規劃升級時程與順序：

有些重要的網路設備，流量雖不大，但是卻有立即性的升級需求，如IDC機房的服務，因IPv4位址已經用鑿，且此類型服務大多直接提供對外服務，因此較有機會進行，則規劃上建議優先考量此設備

112

(三) 評估重要依據

建議以雙協定(Dual Stack，同時支援IPv4與IPv6)為首要目標，IPv6部署先由骨幹單一網路節點下手，逐步擴增支援IPv6功能的網路節點，最後連接成IPv4/v6網路，並達到全面性的IPv6網路佈建。

113

(三) 評估重要依據

下列提供三種主要準則
作為網路設備升級模式之參考：

準則1：

原有網路設備已內建支援IPv6功能，網路管理員需要執行基本IPv6指令，如設定、啟動與測試等步驟。此升級方式成本較低廉，技術人員僅需熟悉IPv6設定，即可達到IPv6之目的。

114

(三) 評估重要依據

準則2：

原有網路設備未支援IPv6，但透過官方所釋出之新版本韌體，僅需根據官方標準升級程序，更新升級後即支援IPv6。

115

(三) 評估重要依據

準則3：

原有網路設備未支援IPv6，且未來新版也不支援IPv6；可採取下列步驟：

(1) 要求網路設備廠商修改程式碼以支援IPv6

(2) 找尋其他的替代網路設備

116

經由詳細評估後，應明訂硬體設備與資訊應用服務系統支援IPv6所需工作項目，例如

- 韌體升級
- 硬體更換
- 修改網路架構
- 軟體修改
- 重購軟體

並進行軟硬體升級之經費估算。

117

網路應用服務清查表

服務系統編號	1
服務 類別	DNS
服務系統名稱	DNS
服務內容說明	提供DNS解析服務
網站名稱(URL)	dns.info.gov.tw
重要國際服務	N
具指標性服務	Y
行動服務應用	N
服務使用率高	Y
年度規劃改版	N
主/次要服務	主要
負責 單位	資訊中心
負責 人員	XXX
建議升級年度	2019年

118

服務系統編號
軟硬體編號
品名
硬體廠牌型號或軟體供應商
作業系統/ 軟體版本
距離報廢/授權年限
已內含IPv6能力
已導入IPv6
建議升級年度
硬體升級方式
軟體升級方式

119

網路升級檢測

網路除錯通常使用 ping6 與 tracert6

如要進行此類測試，應事先檢查網路上相關設備是否已開放此類封包訊息傳送，如路由器、防火牆、伺服器、終端電腦等

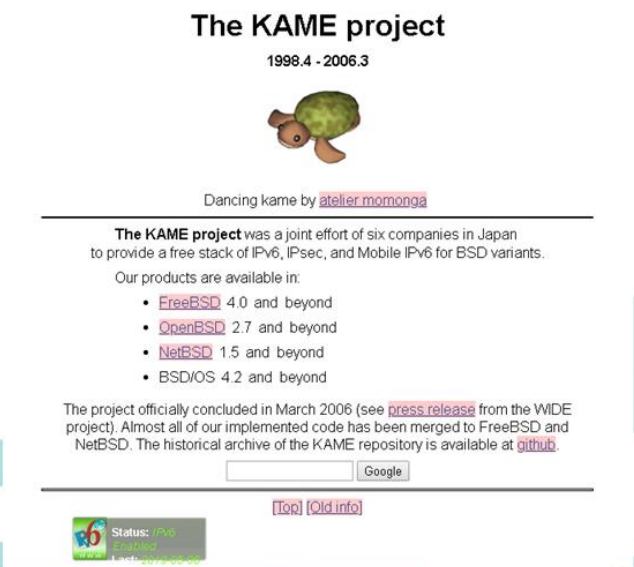
如無法排除封包阻擋的問題，可以改用應用服務層協定(如port 80)進行測試

以下提供檢測IPv6能力的測試網站：

120

https://www.ipv6.hinet.net/

http://www.kame.net/

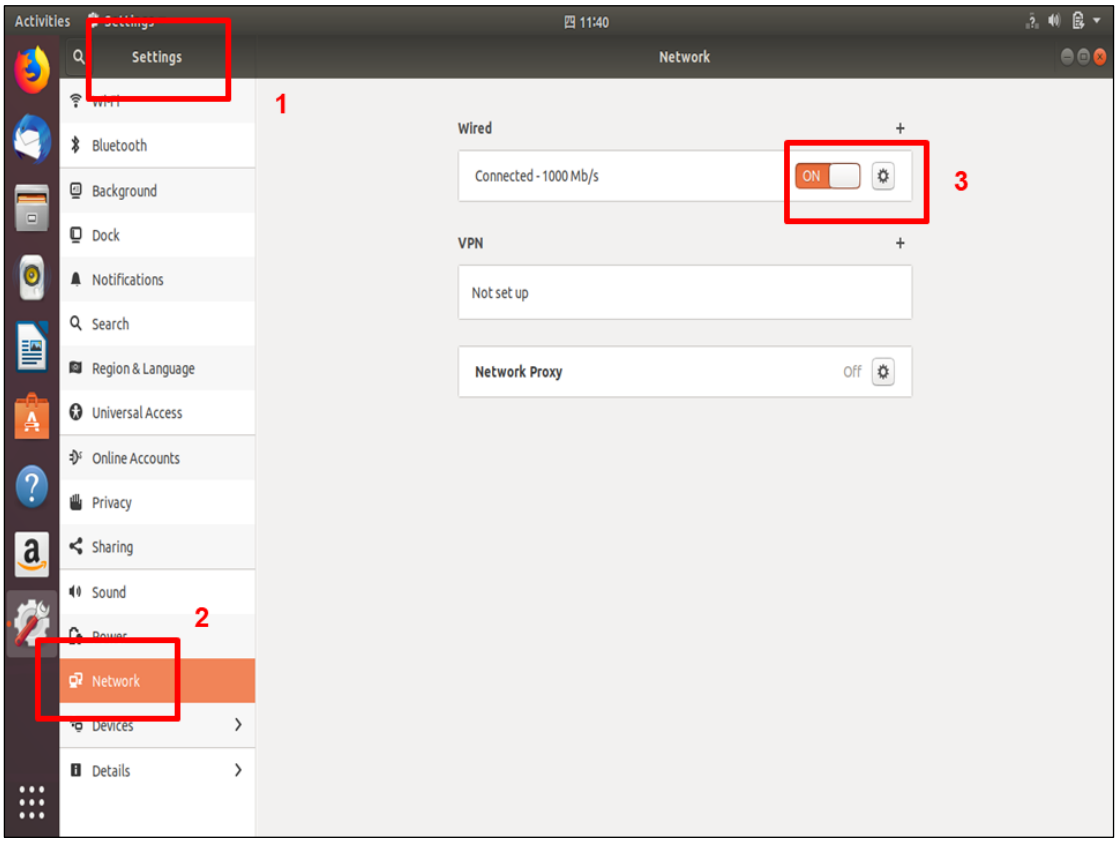


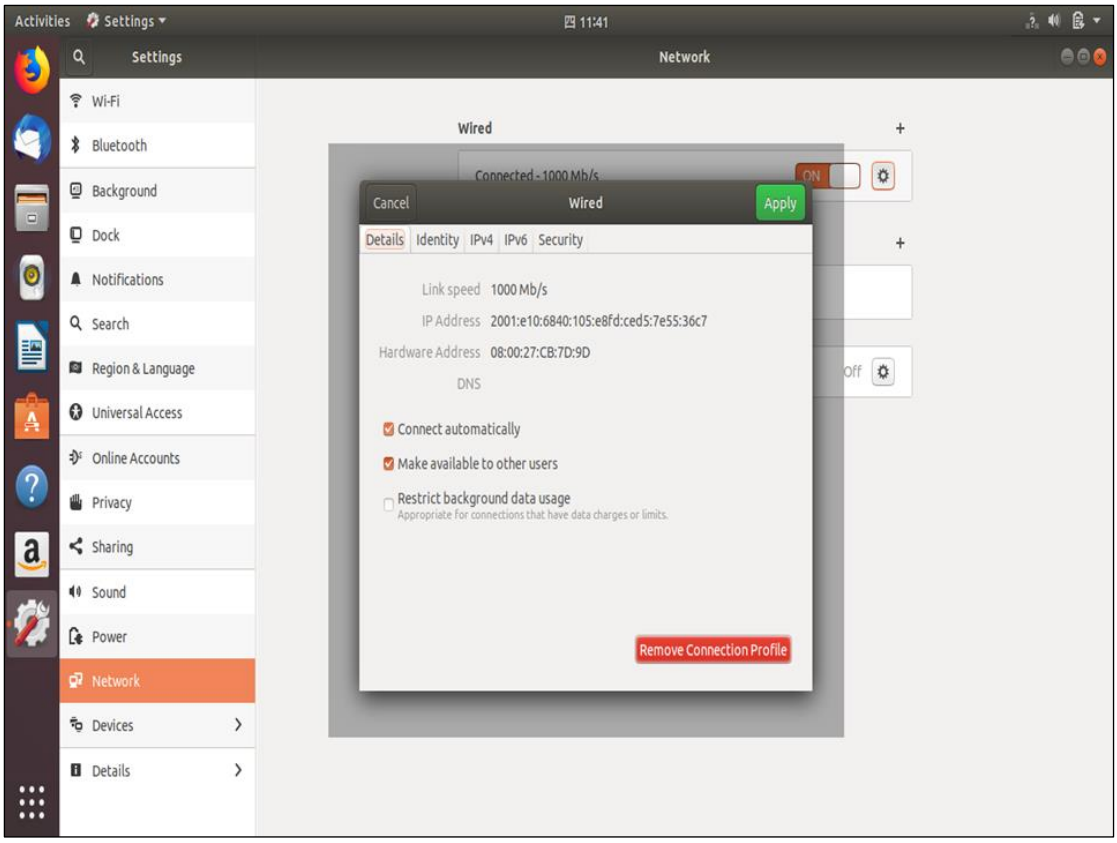
Chrome瀏覽器-擴充功能

行動網路IPv6設定

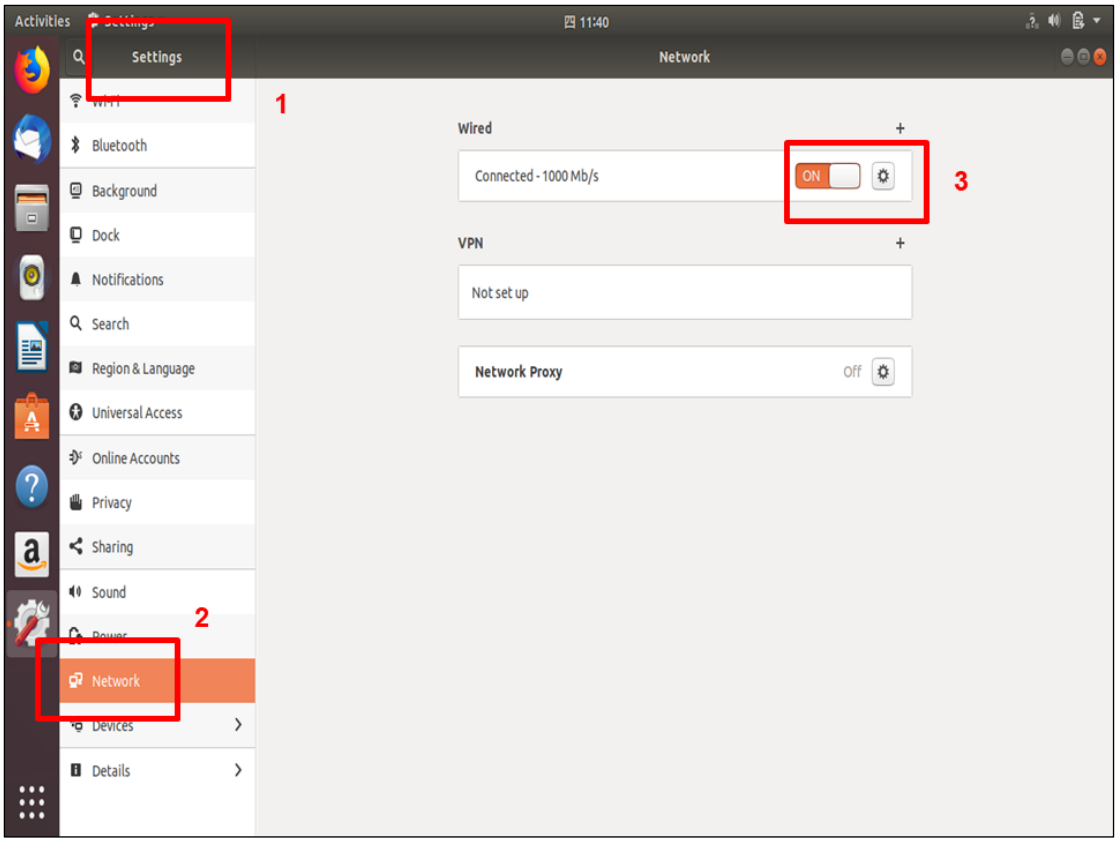
- 手機網路設定說明

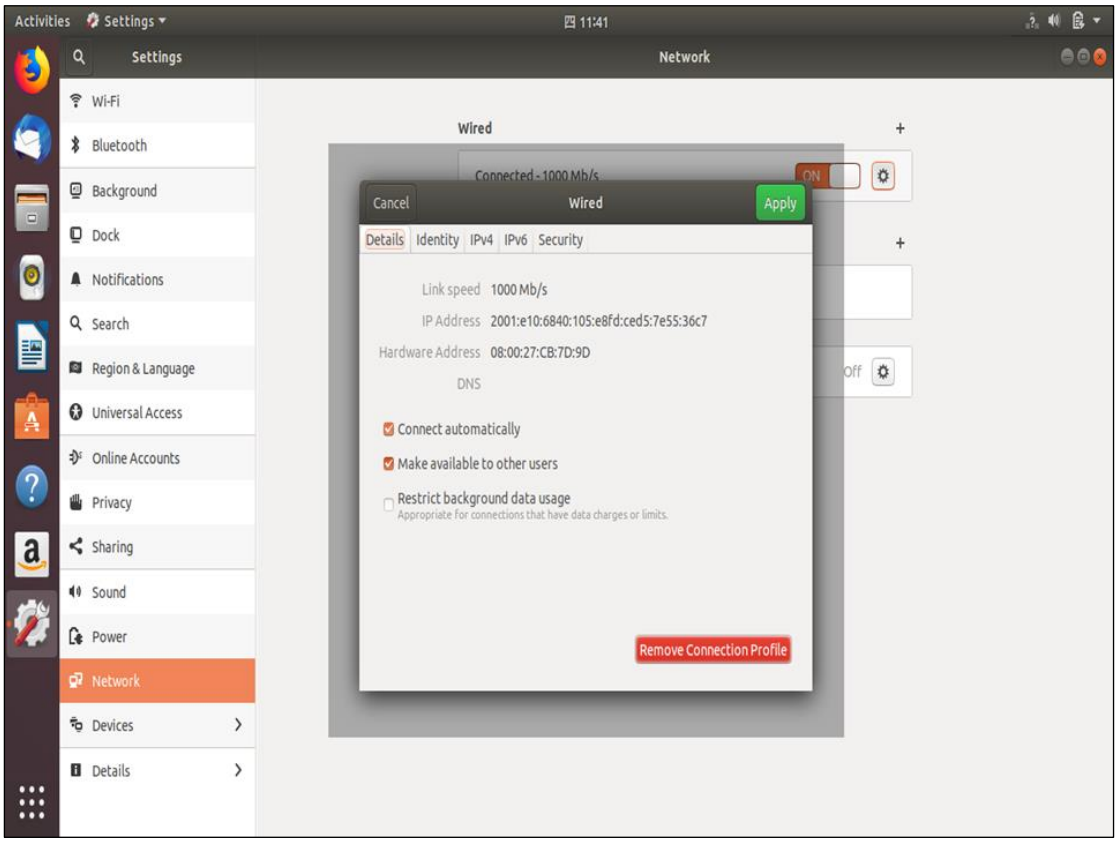

點進網域新視界！
IPv6建置示範
Ubuntu
作業系統

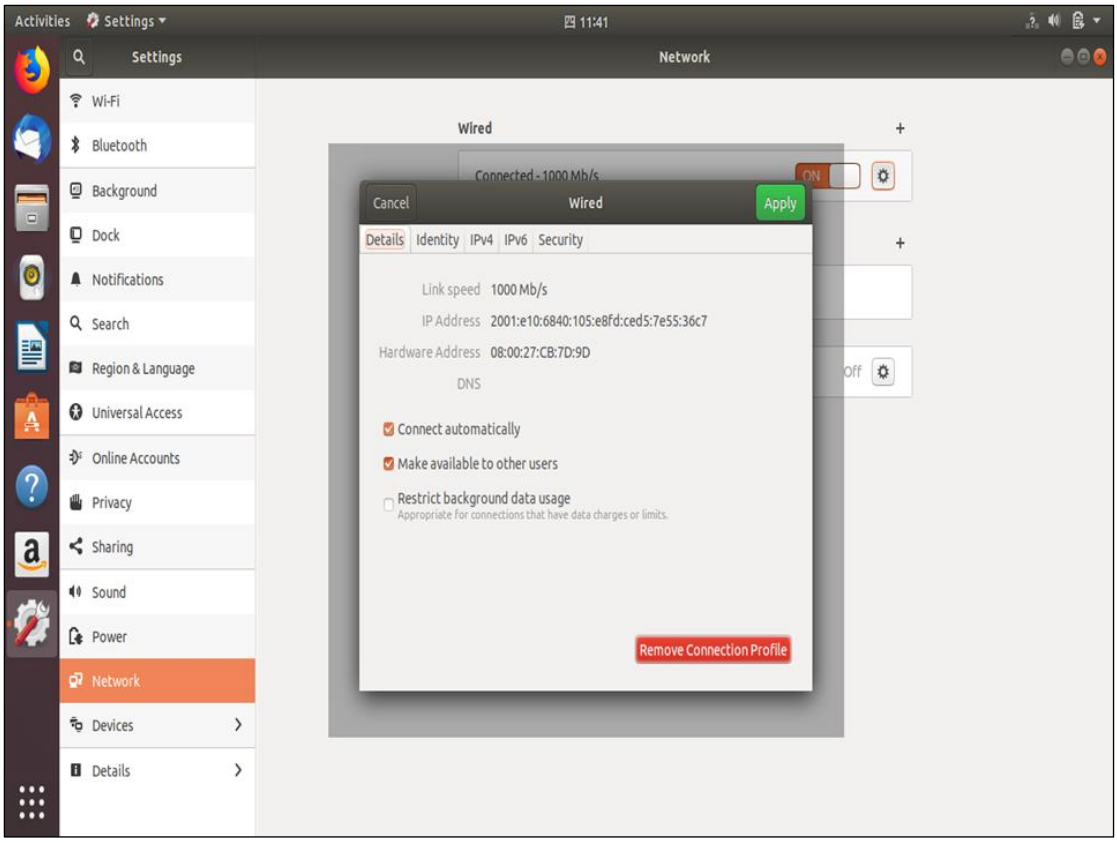

Activities
11:40
Settings
Network
1
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
2
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
3
VPN
Not set up
Network Proxy
Off

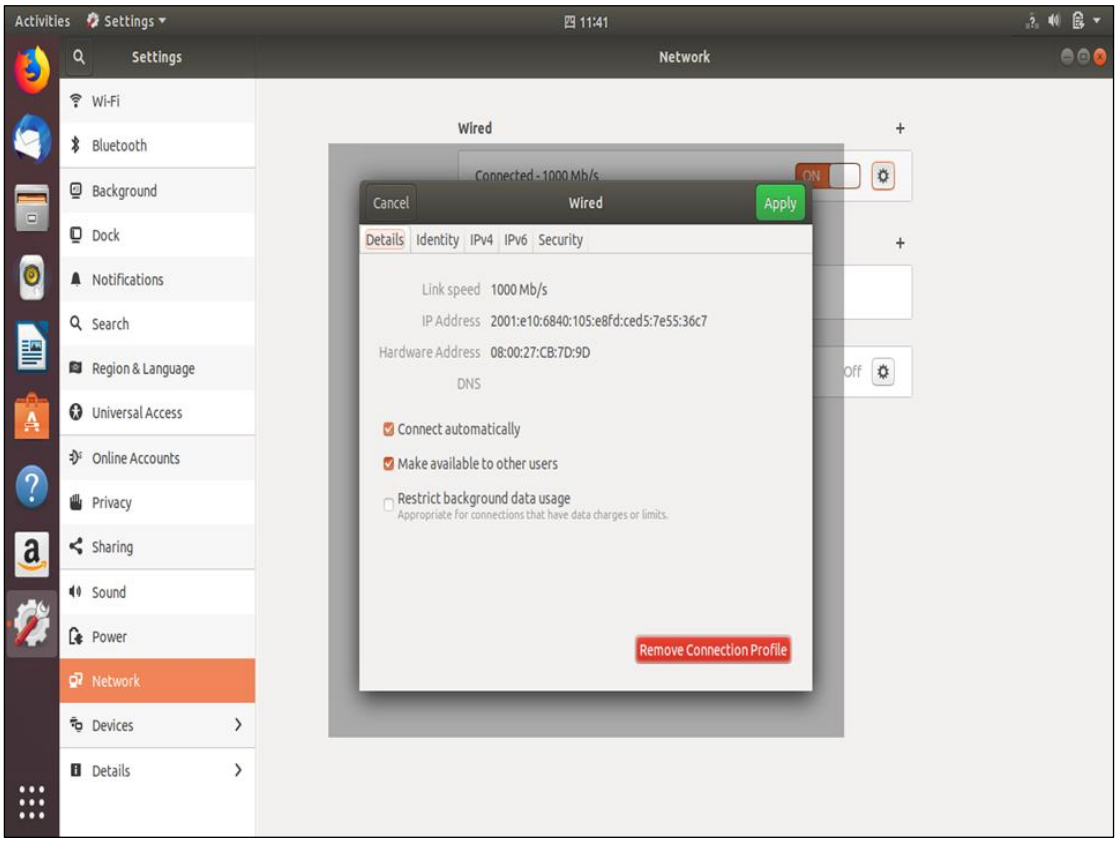

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile
Off


點進網域新視界！
IPv6建置示範
Ubuntu
作業系統

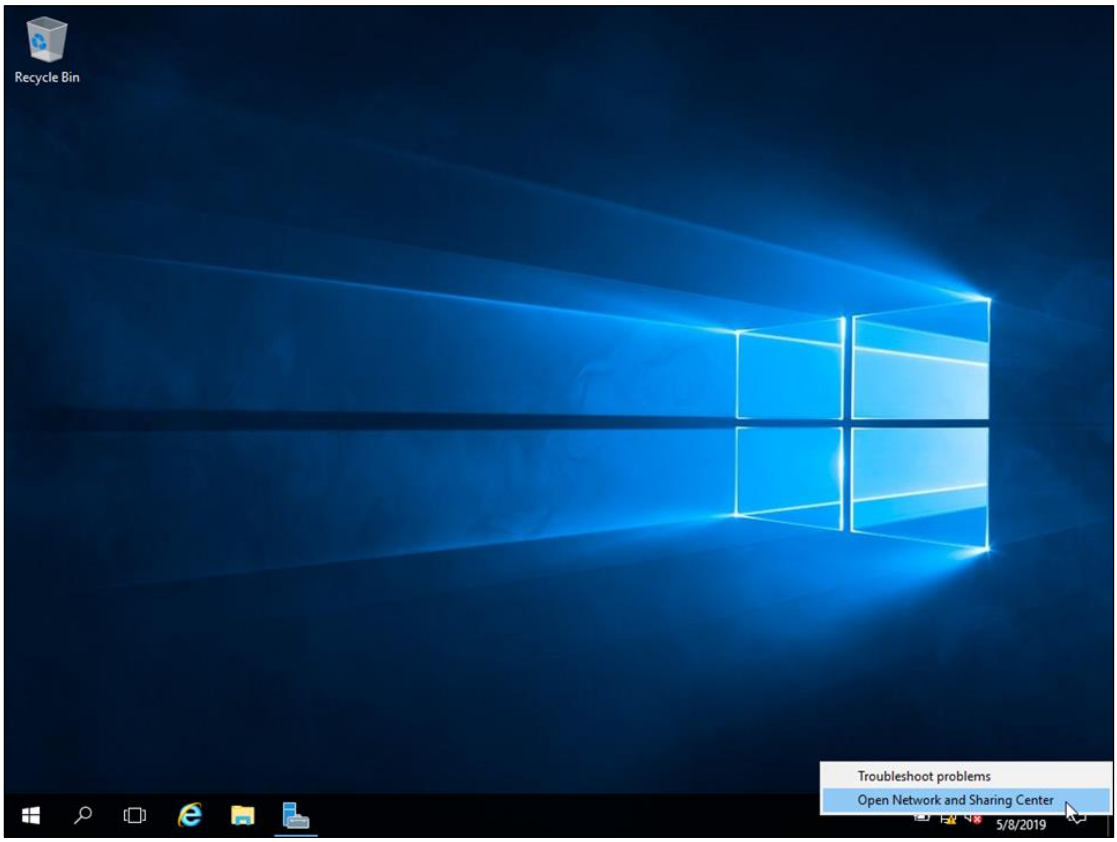

Activities
11:40
Settings
Network
1
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
2
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
3
VPN
Not set up
Network Proxy
Off

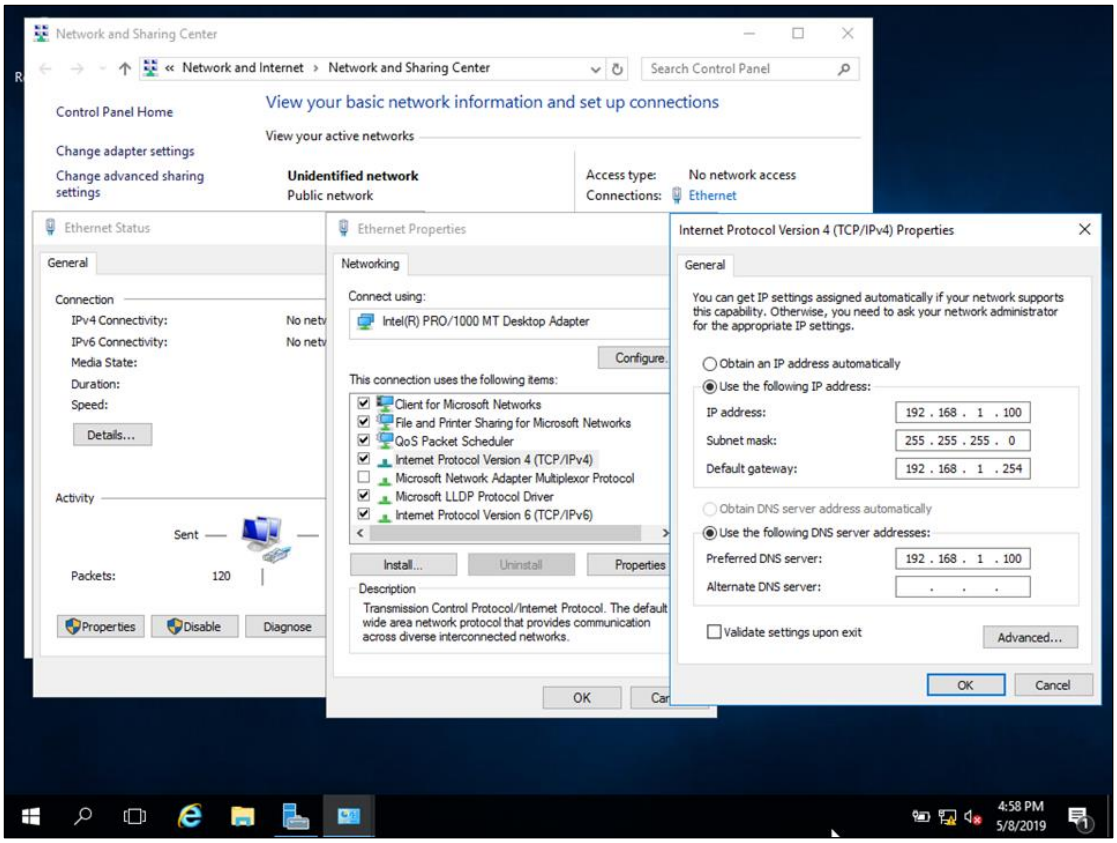

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile
Off

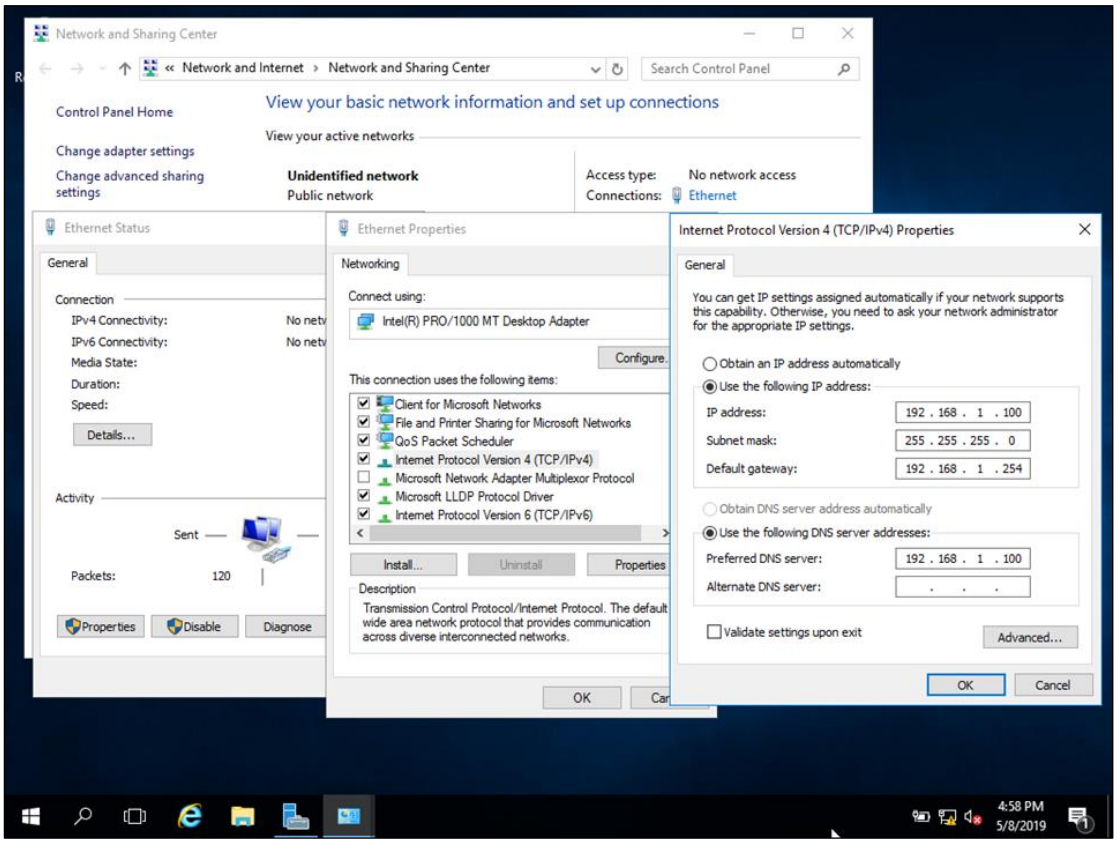

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Off
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile


Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Off
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile

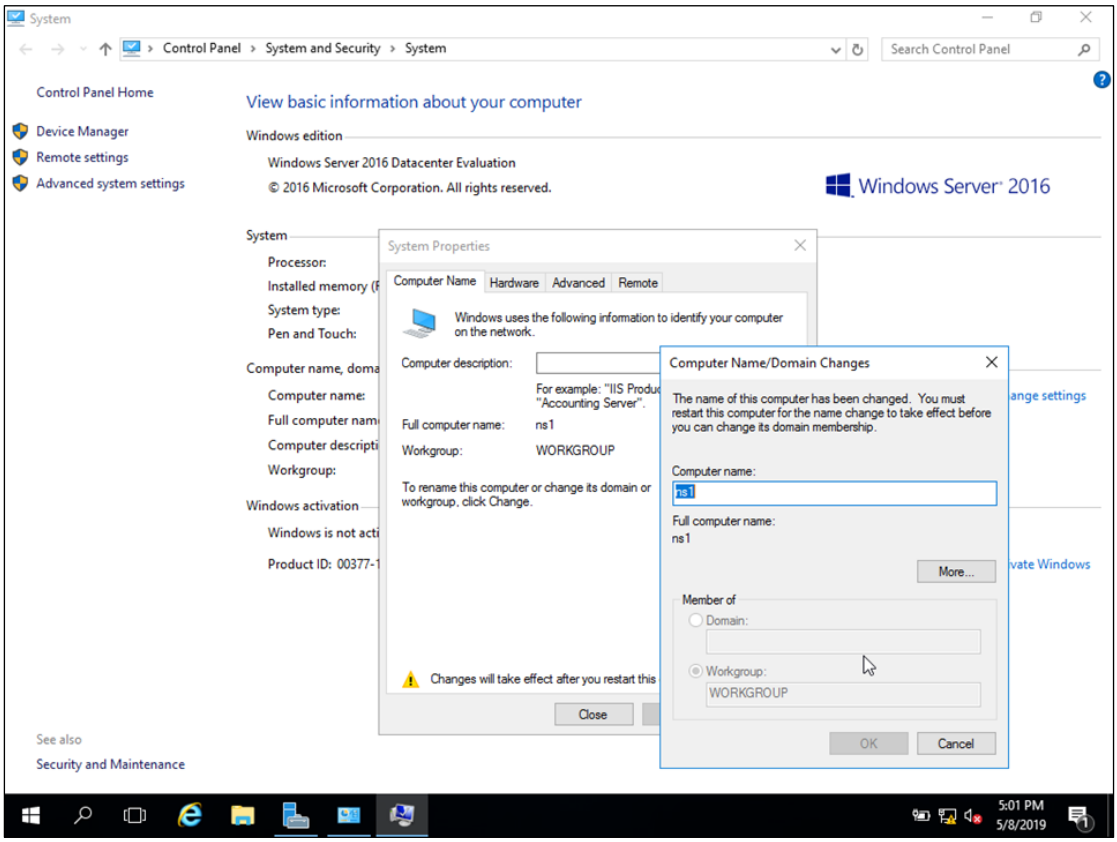

點進網域新視界！
IPv6建置示範
Windows server 2016
作業系統

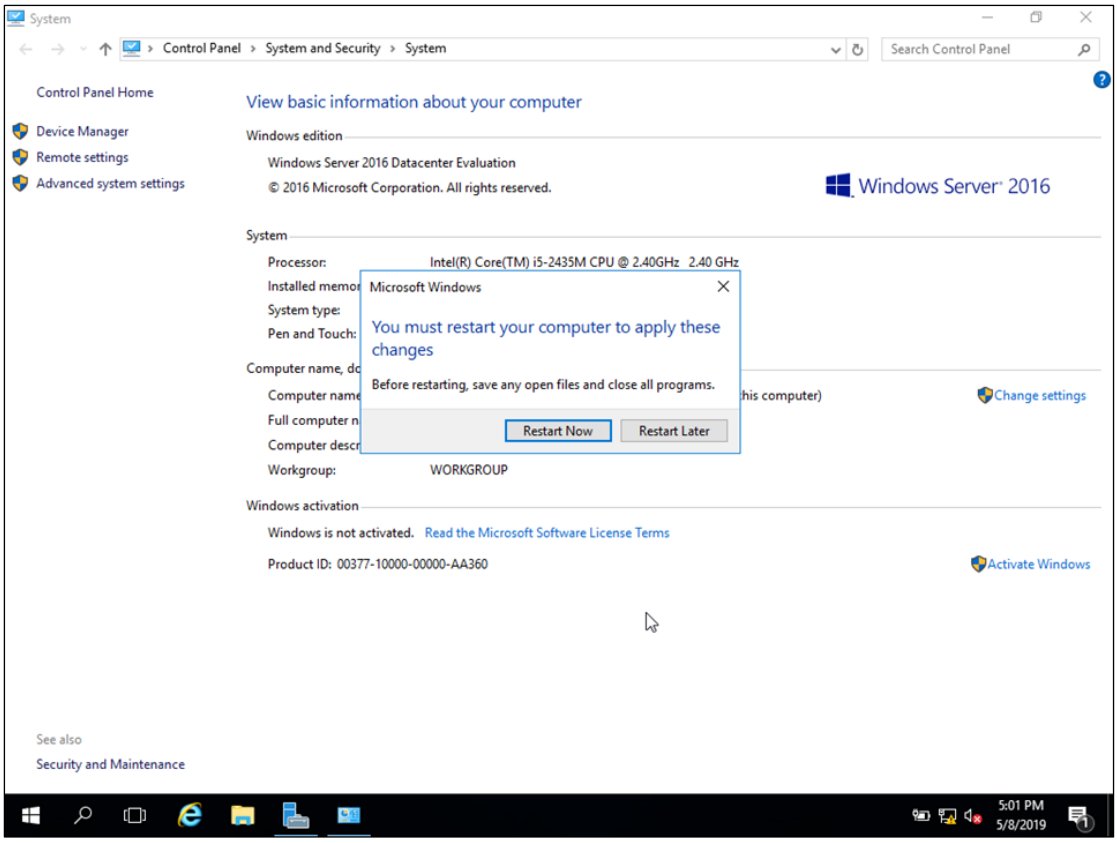

Recycle Bin
Troubleshoot problems
Open Network and Sharing Center
5/8/2019

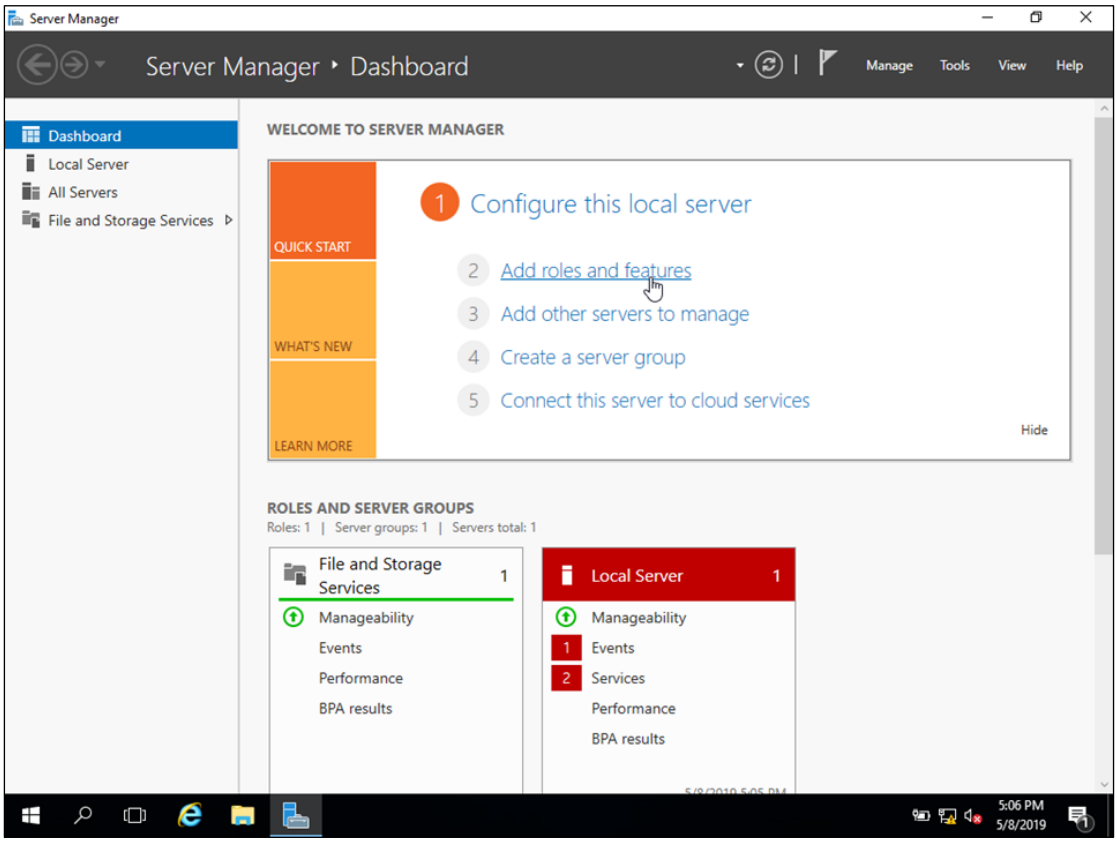

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
4:58 PM
5/8/2019

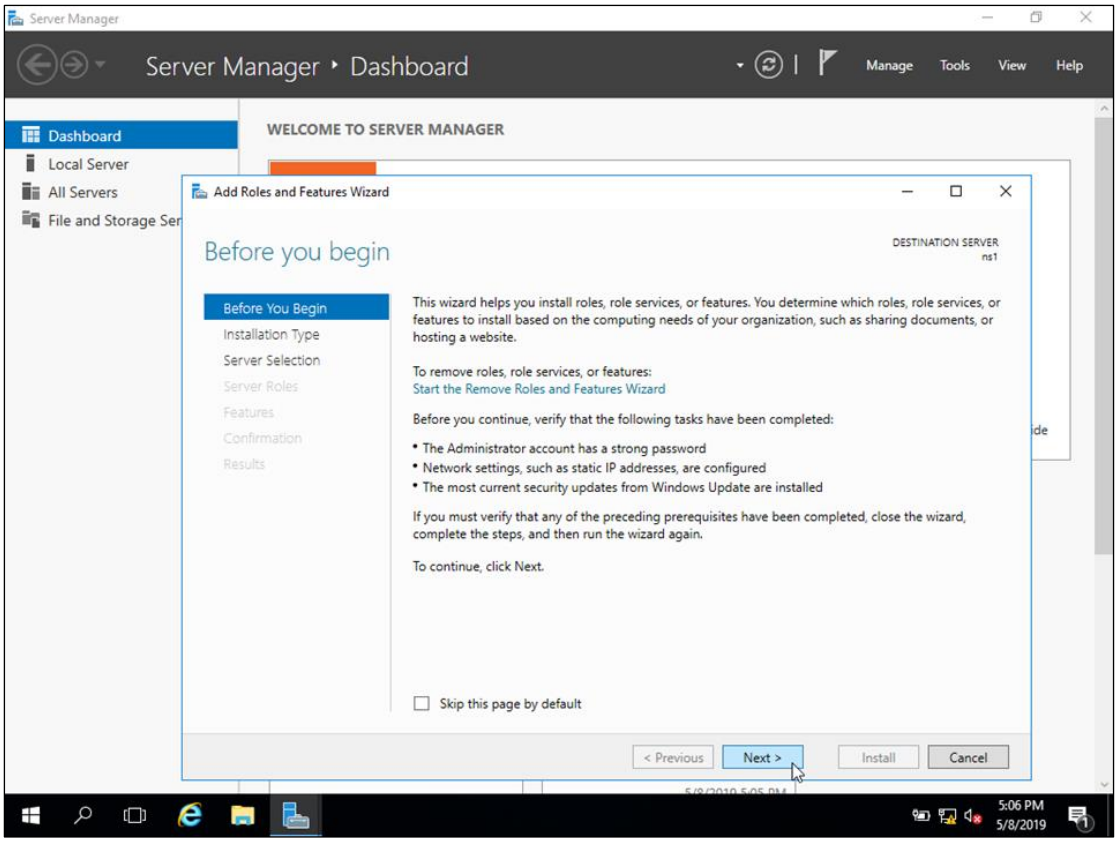

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
4:58 PM
5/8/2019

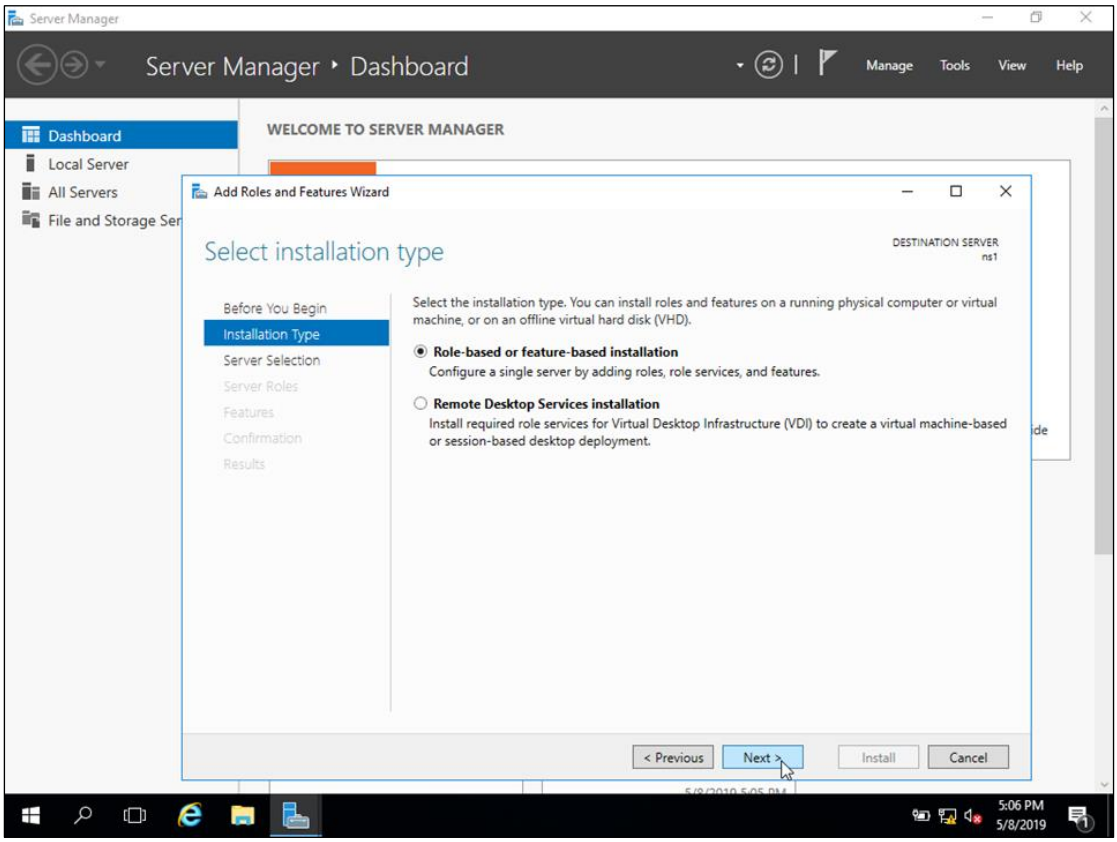

點進網域新視界！
IPv6建置示範
DNS Server

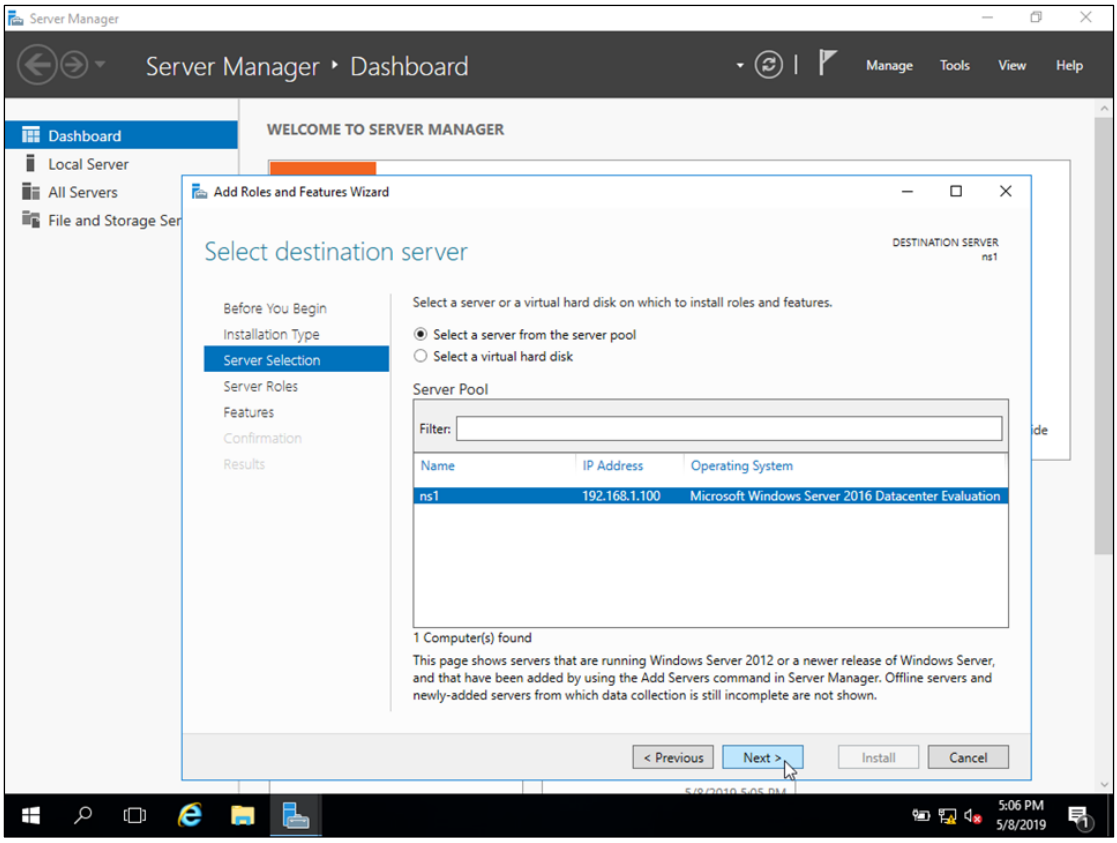

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
View basic information about your computer
Device Manager
Remote settings
Advanced system settings
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor:
Installed memory (
System type:
Pen and Touch:
Computer name, doma
Computer name:
Full computer nam
Computer descripti
Workgroup:
Windows activation
Windows is not acti
Product ID: 00377-1
System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Produc "Accounting Server".
Full computer name: ns1
Workgroup: WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Changes will take effect after you restart this
Close
Computer Name/Domain Changes
The name of this computer has been changed. You must restart this computer for the name change to take effect before you can change its domain membership.
Computer name:
ns1
Full computer name:
ns1
More...
Member of
Domain:
Workgroup:
WORKGROUP
OK
Cancel
See also
Security and Maintenance
5:01 PM
5/8/2019

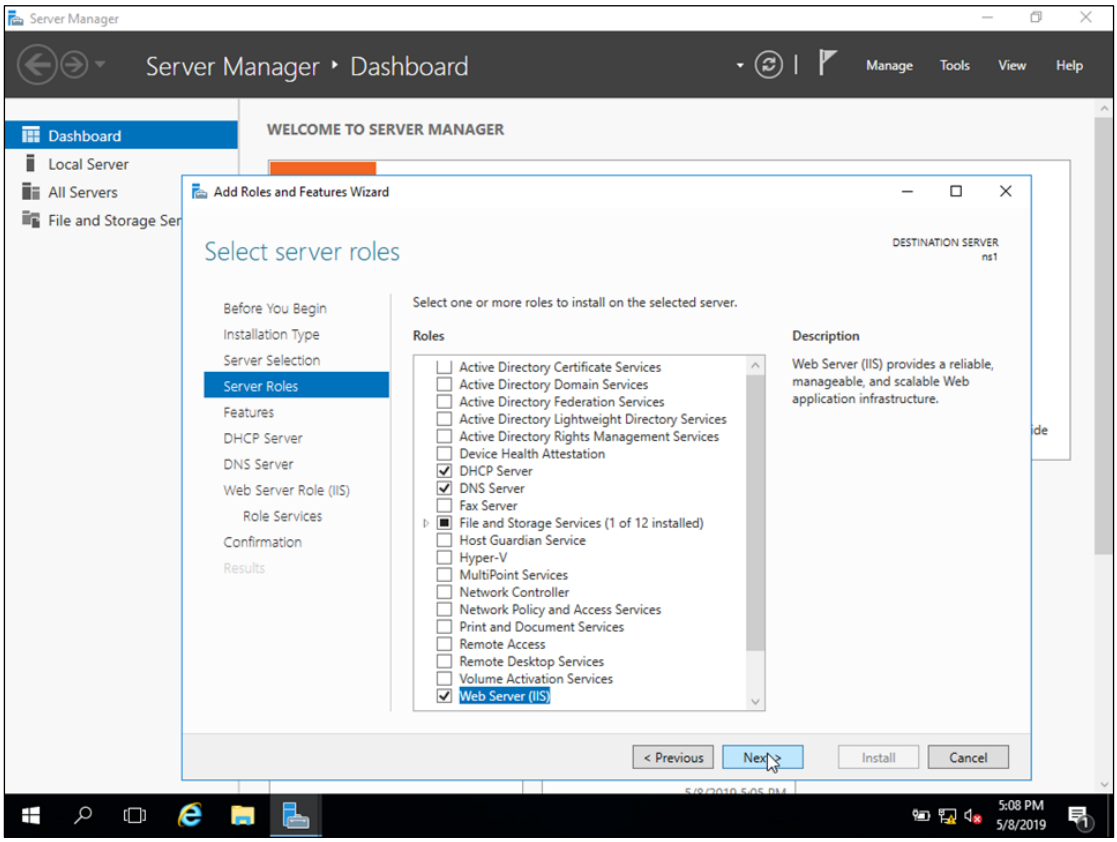

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor: Intel(R) Core(TM) i5-2435M CPU @ 2.40GHz 2.40 GHz
Microsoft Windows
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
Restart Now
Restart Later
Change settings
Workgroup: WORKGROUP
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-10000-00000-AA360
Activate Windows
See also
Security and Maintenance
5:01 PM
5/8/2019

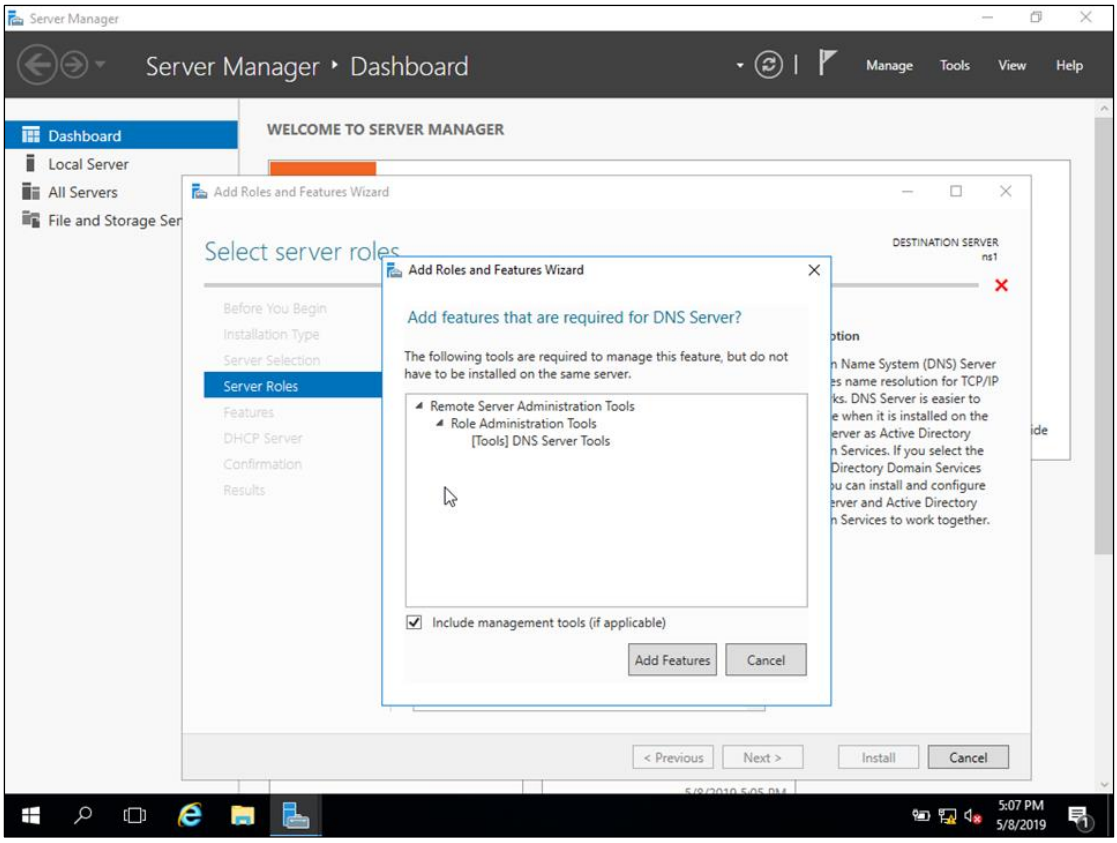

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
1 Events
2 Services
Performance
BPA results
5:06 PM
5/8/2019

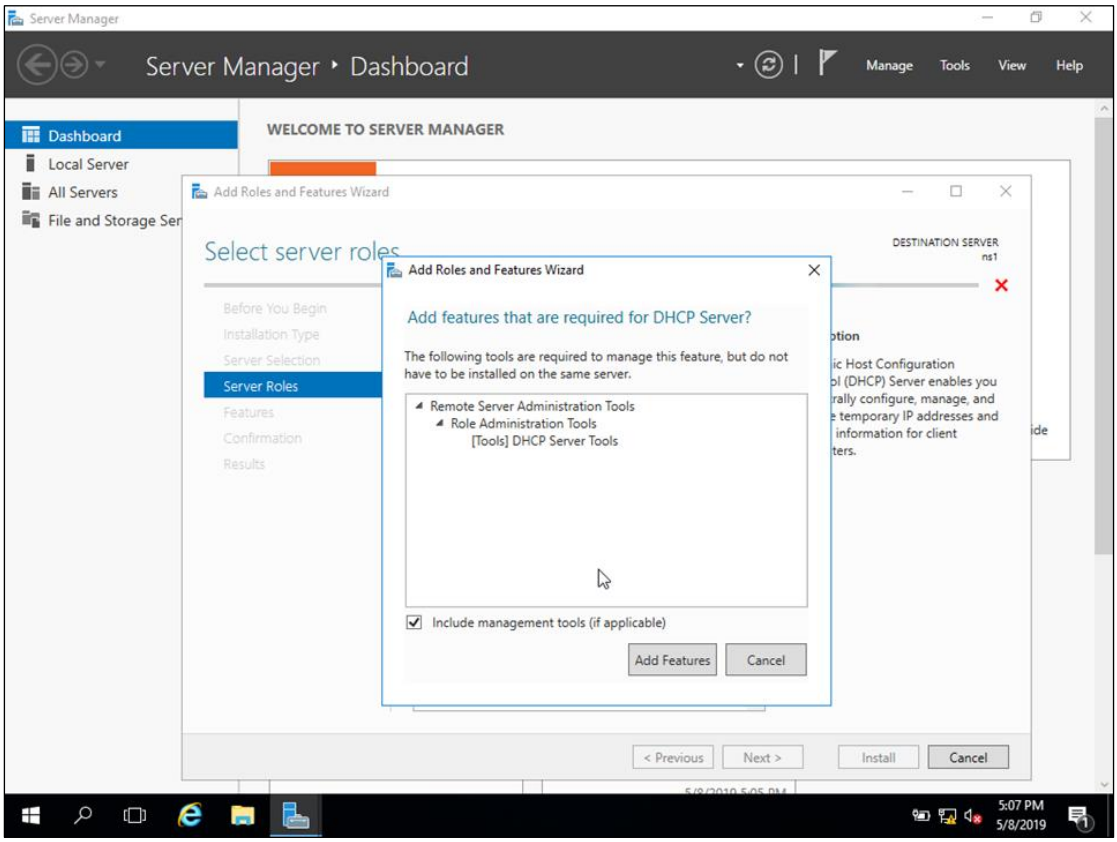

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

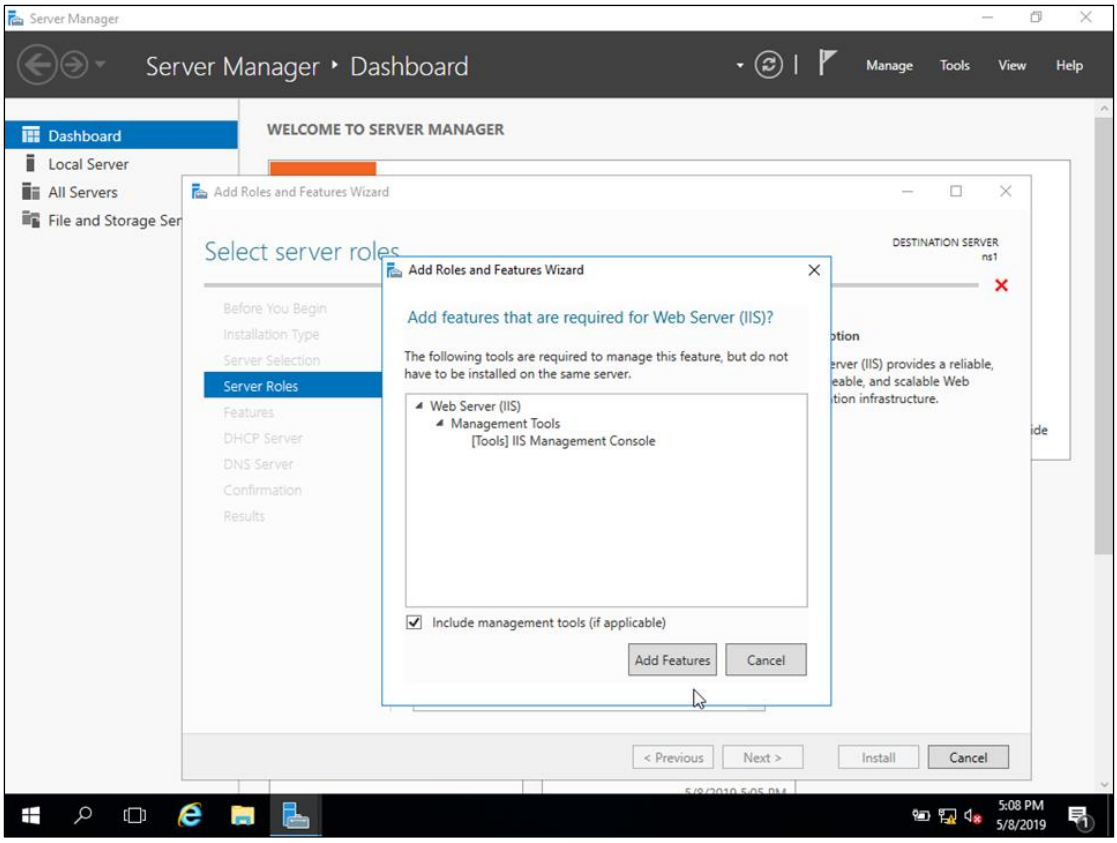

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

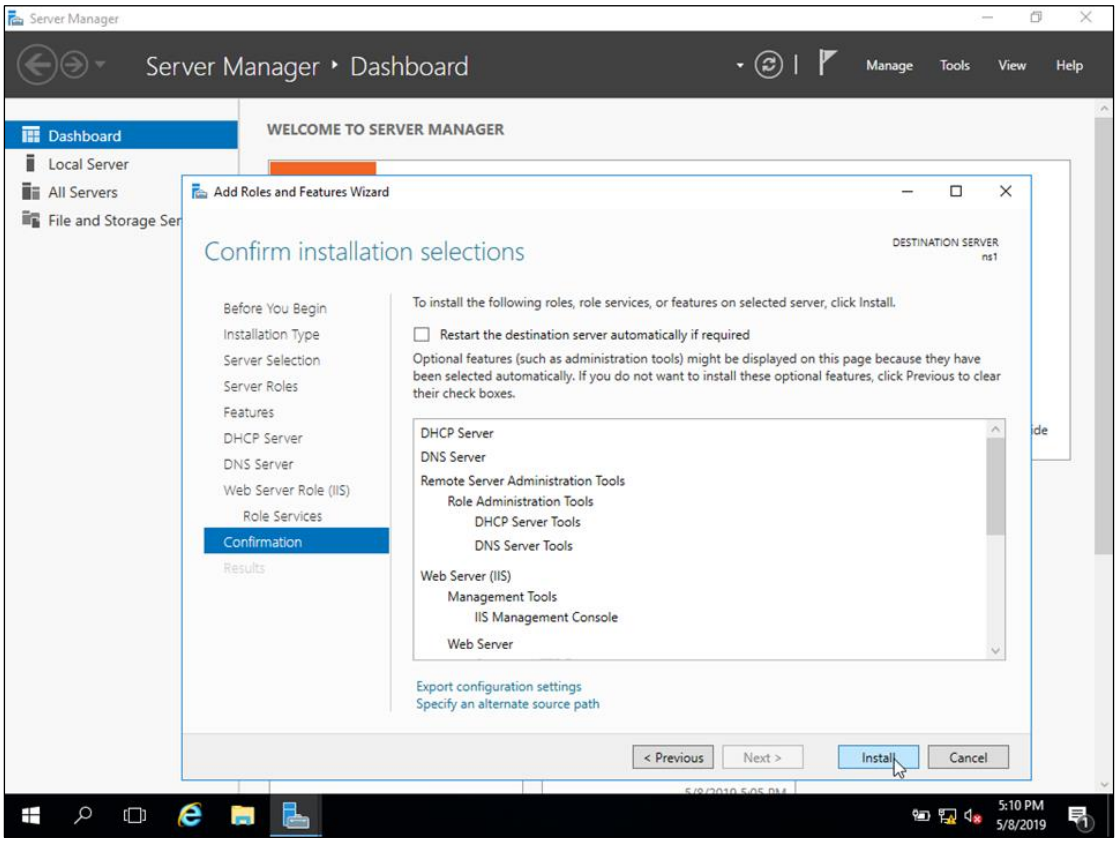

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
ns1
192.168.1.100
Microsoft Windows Server 2016 Datacenter Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

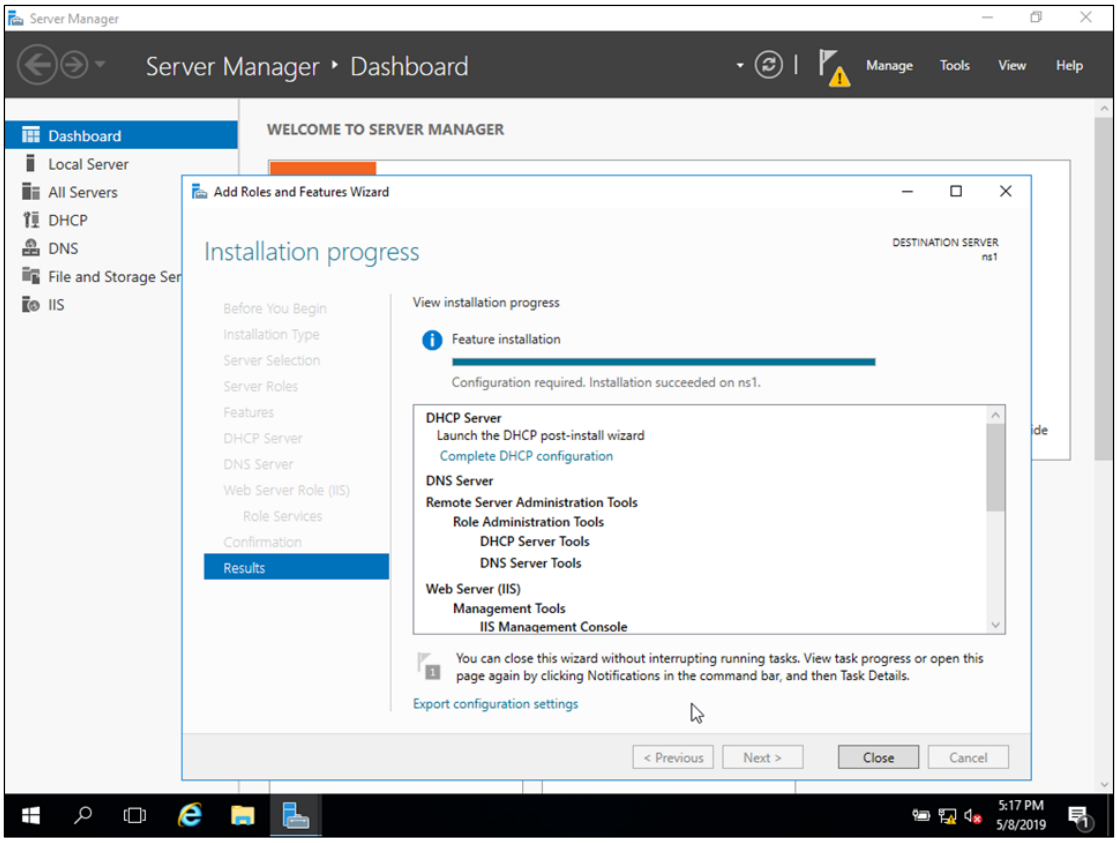

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

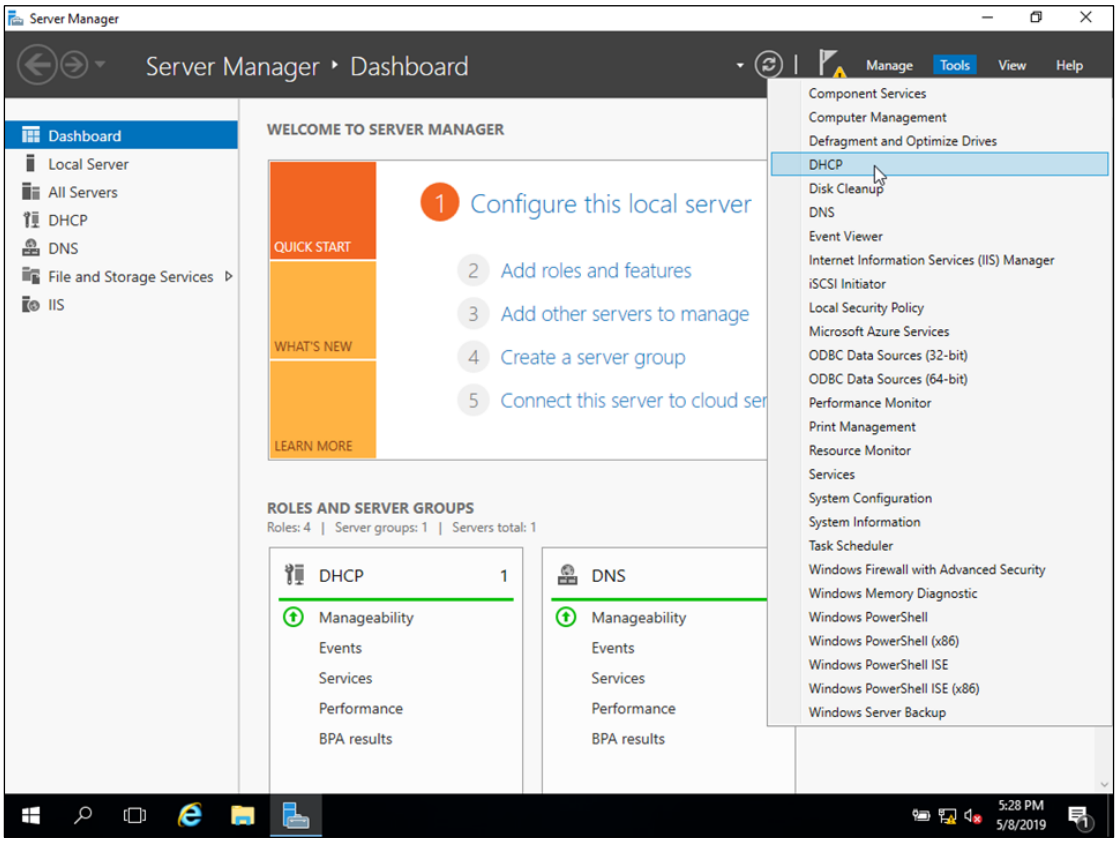

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

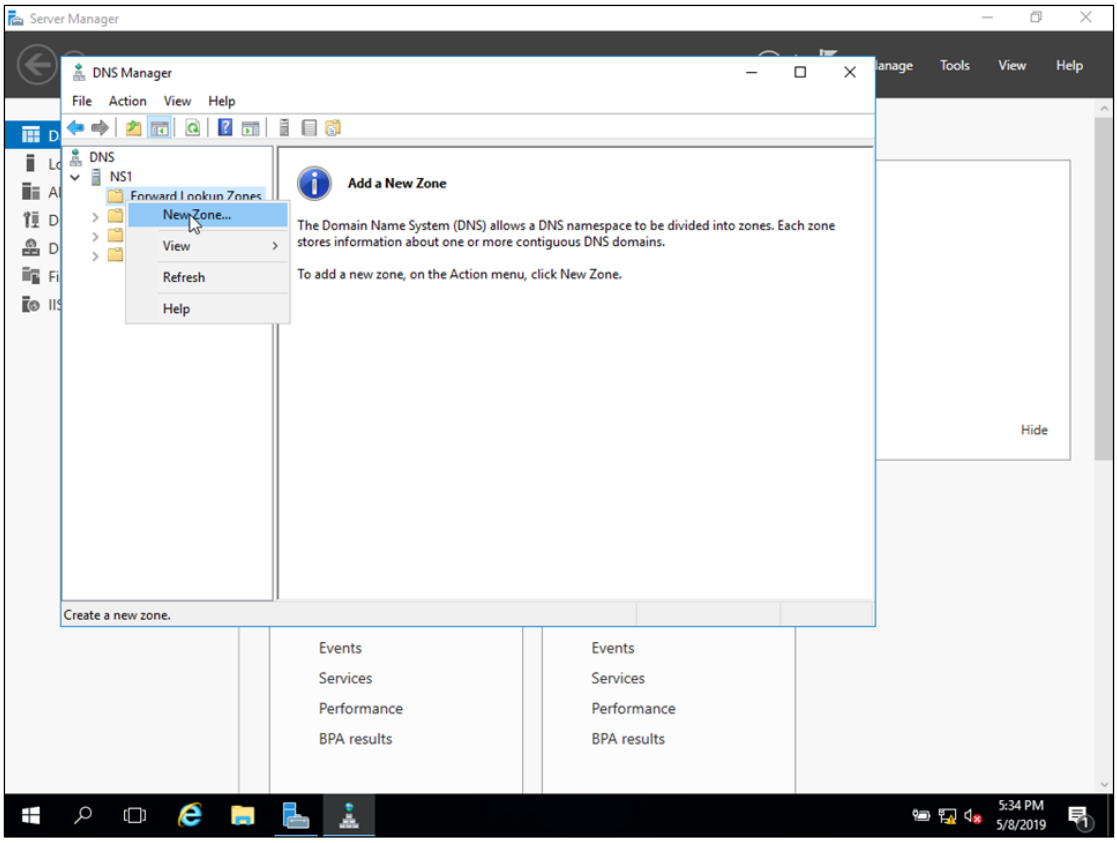

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

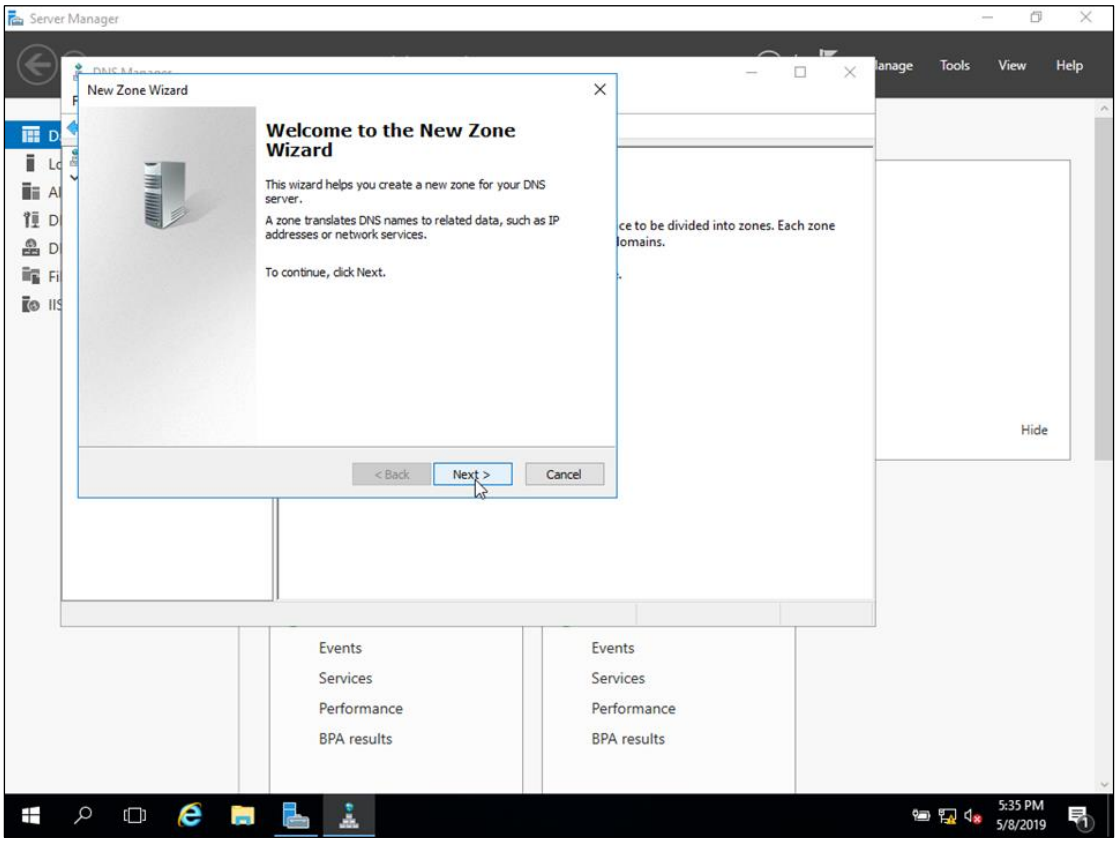

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

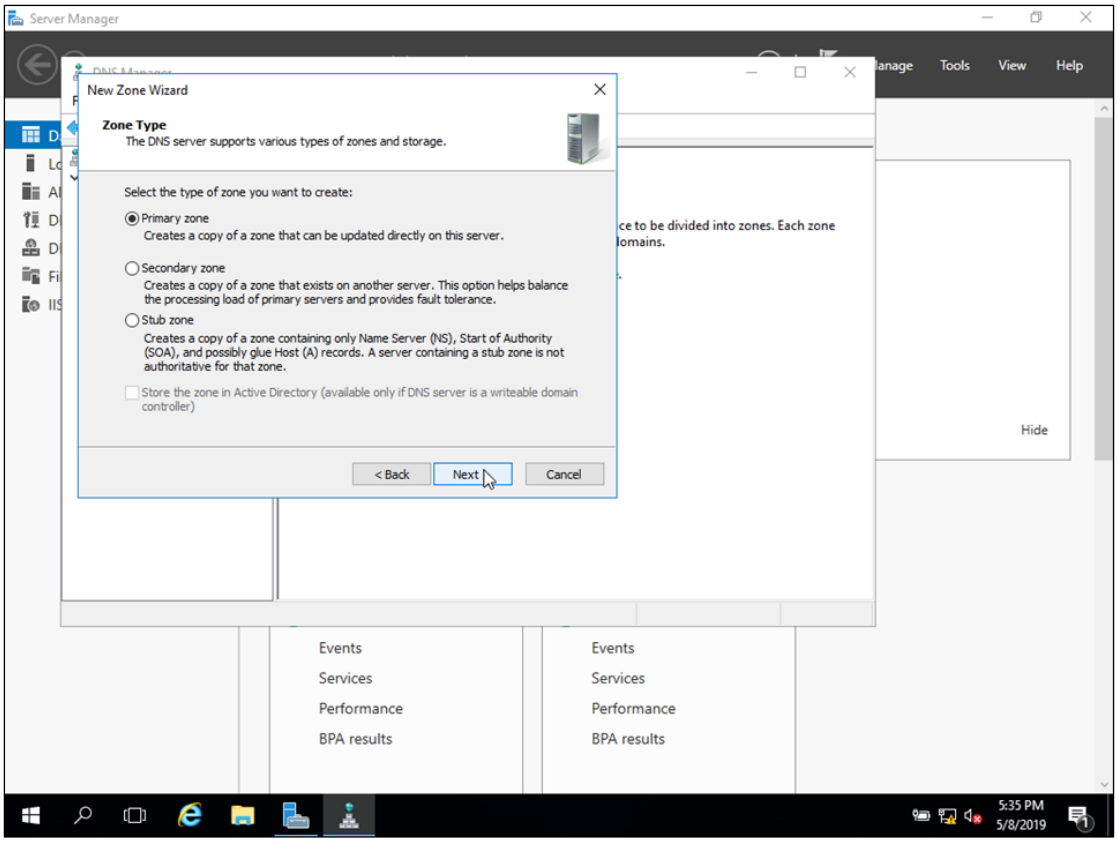

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
DHCP Server
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
5:10 PM
5/8/2019

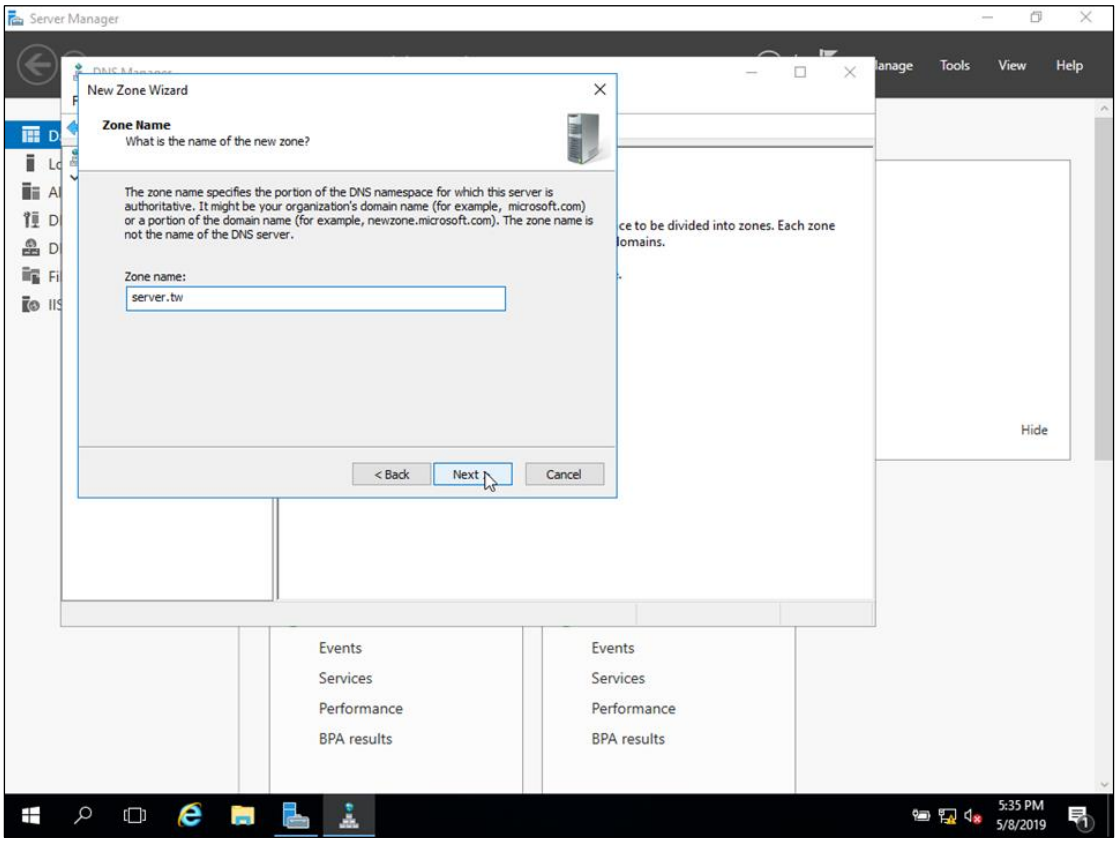

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Ser
IIS
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on ns1.
DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
5:17 PM
5/8/2019

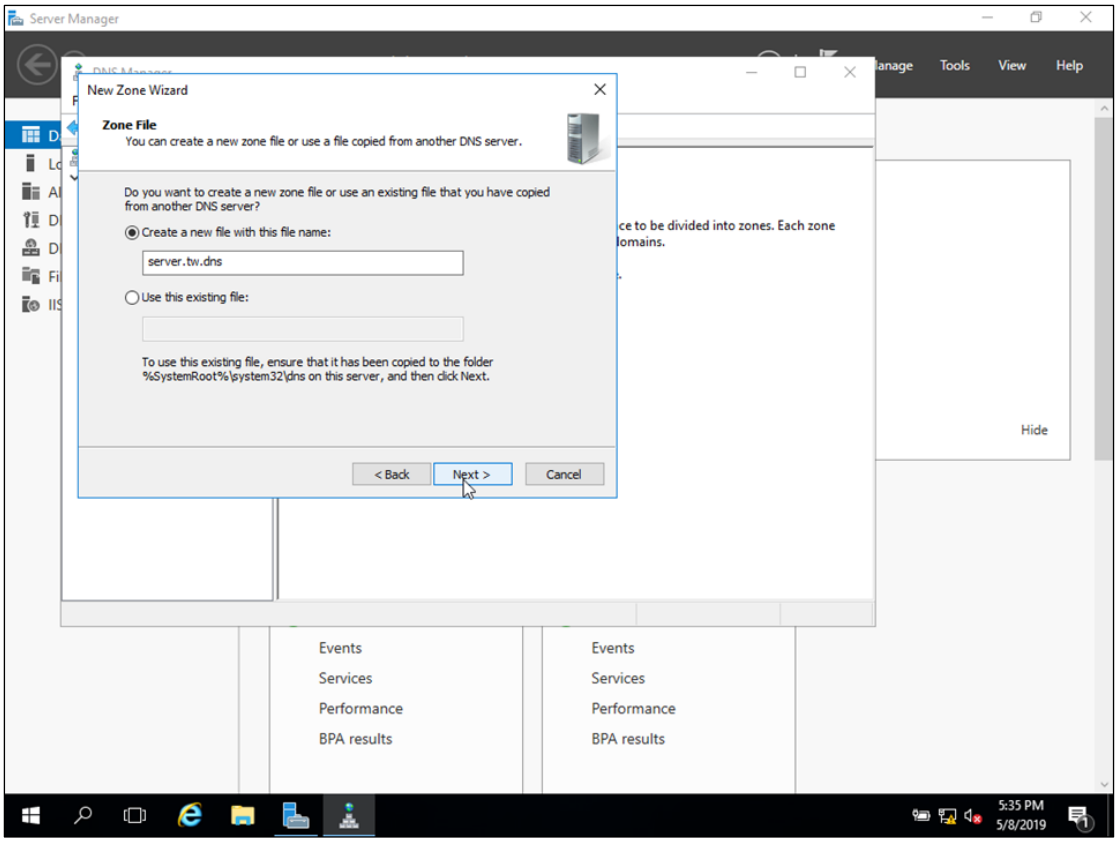

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud ser
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
DHCP 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
5:28 PM
5/8/2019

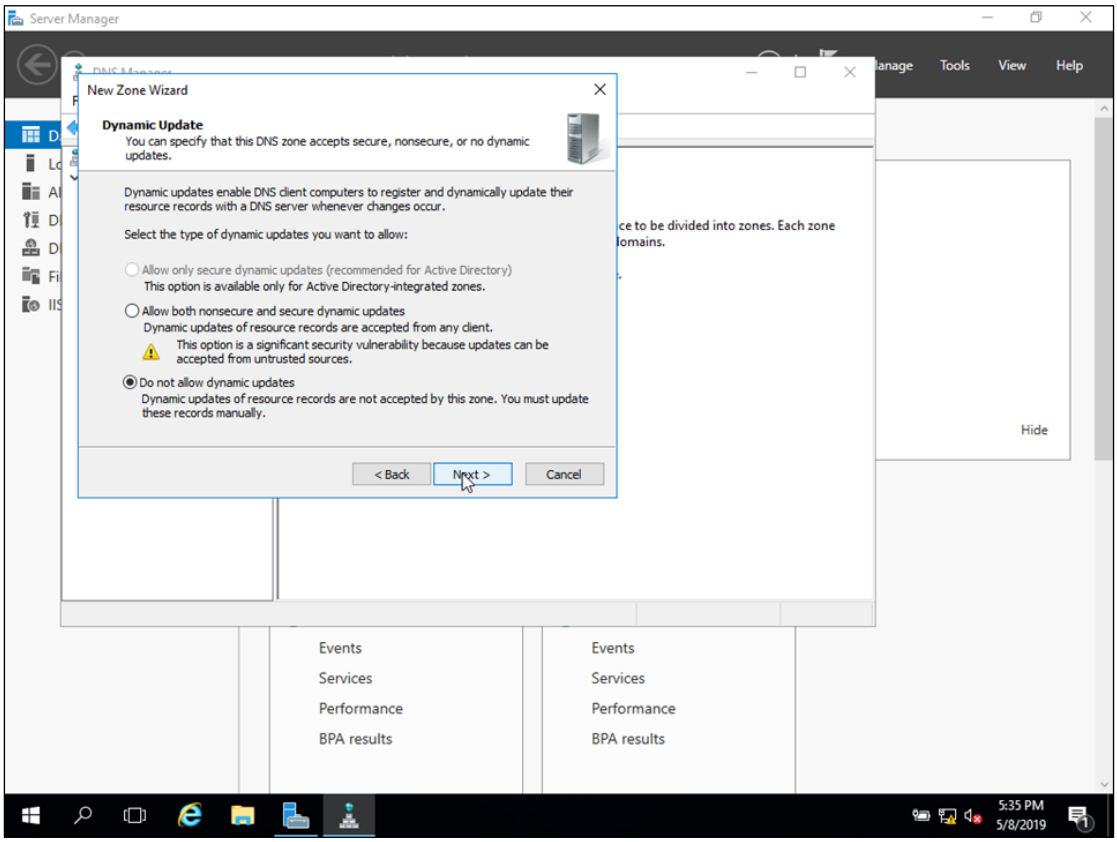

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
To add a new zone, on the Action menu, click New Zone.
Create a new zone.
Tools View Help
Hide
Events
Services
Performance
BPA results
5:34 PM
5/8/2019

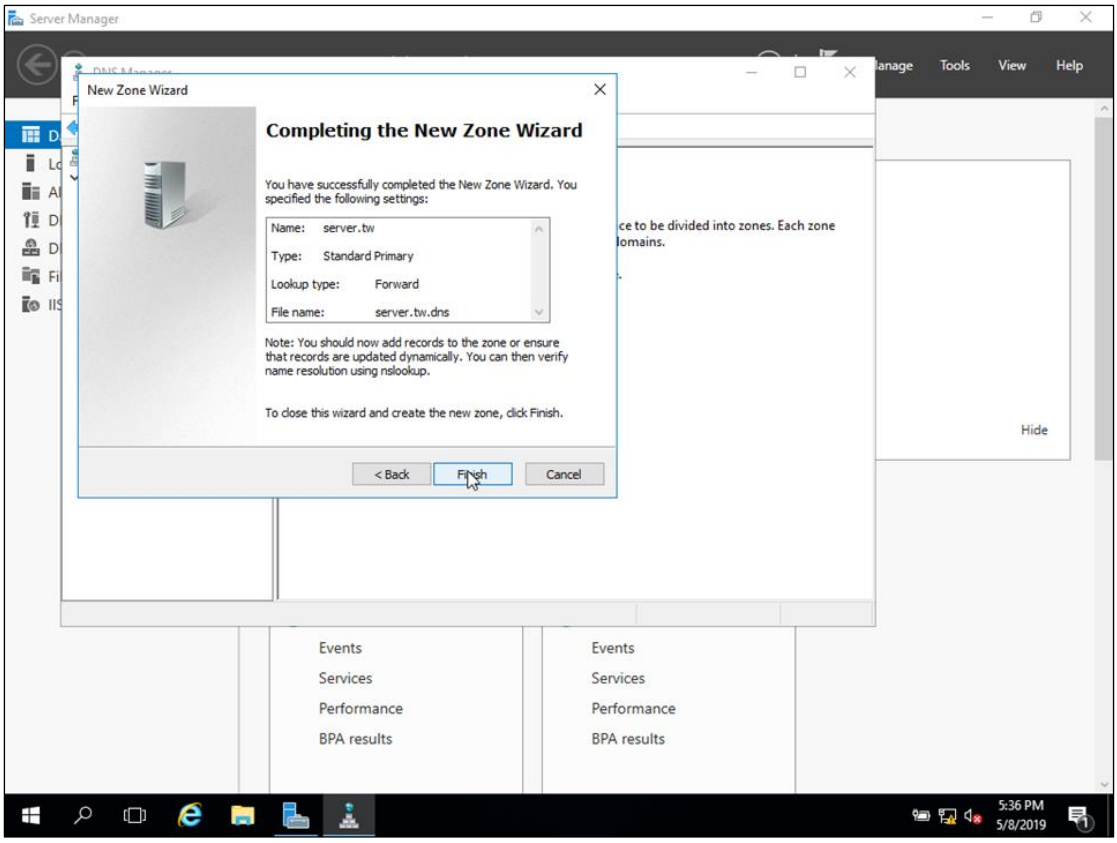

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Tools View Help
Hide
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

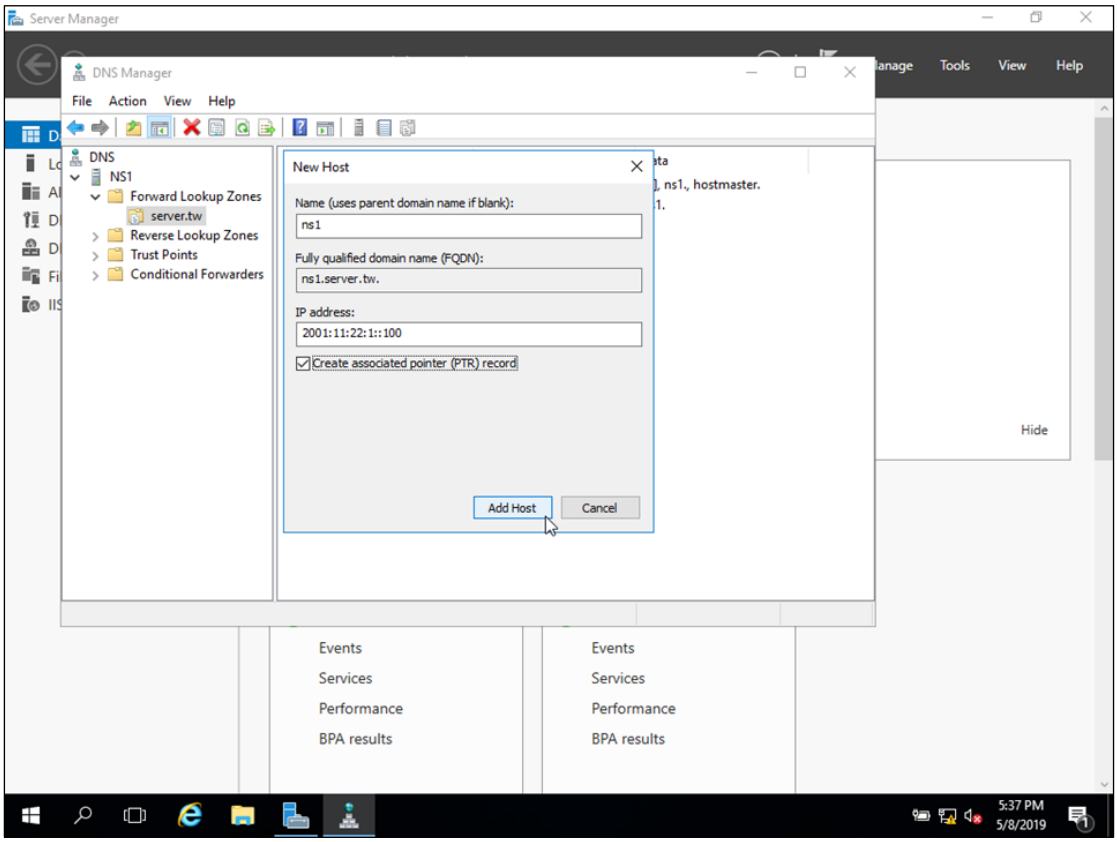

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

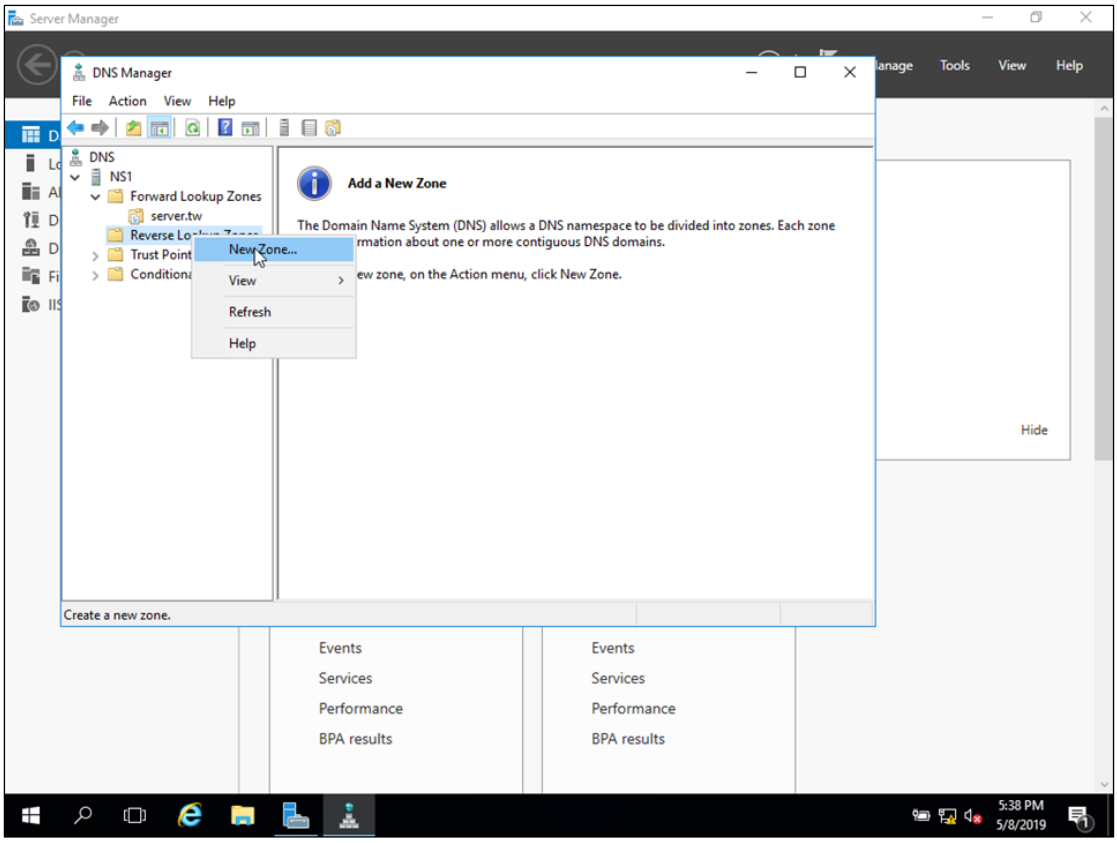

Server Manager
Tools
View
Help
New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
server.tw
< Back
Next
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

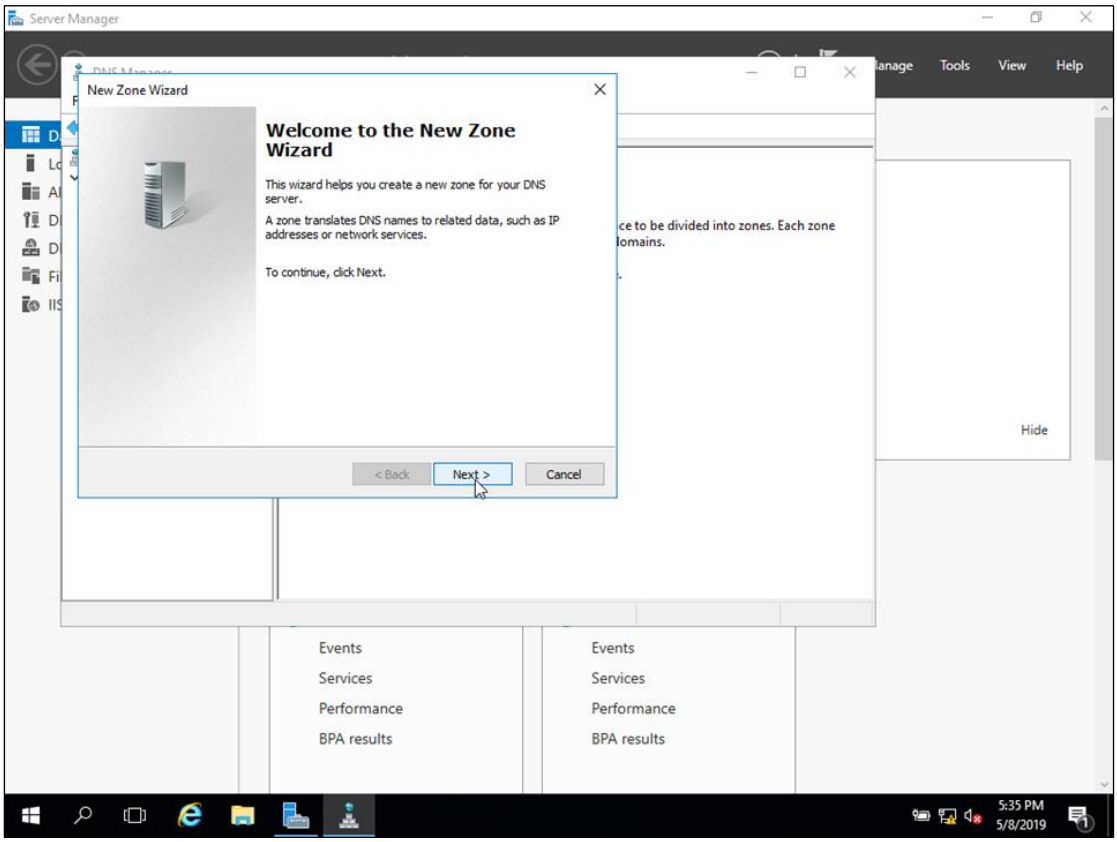

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
server.tw.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

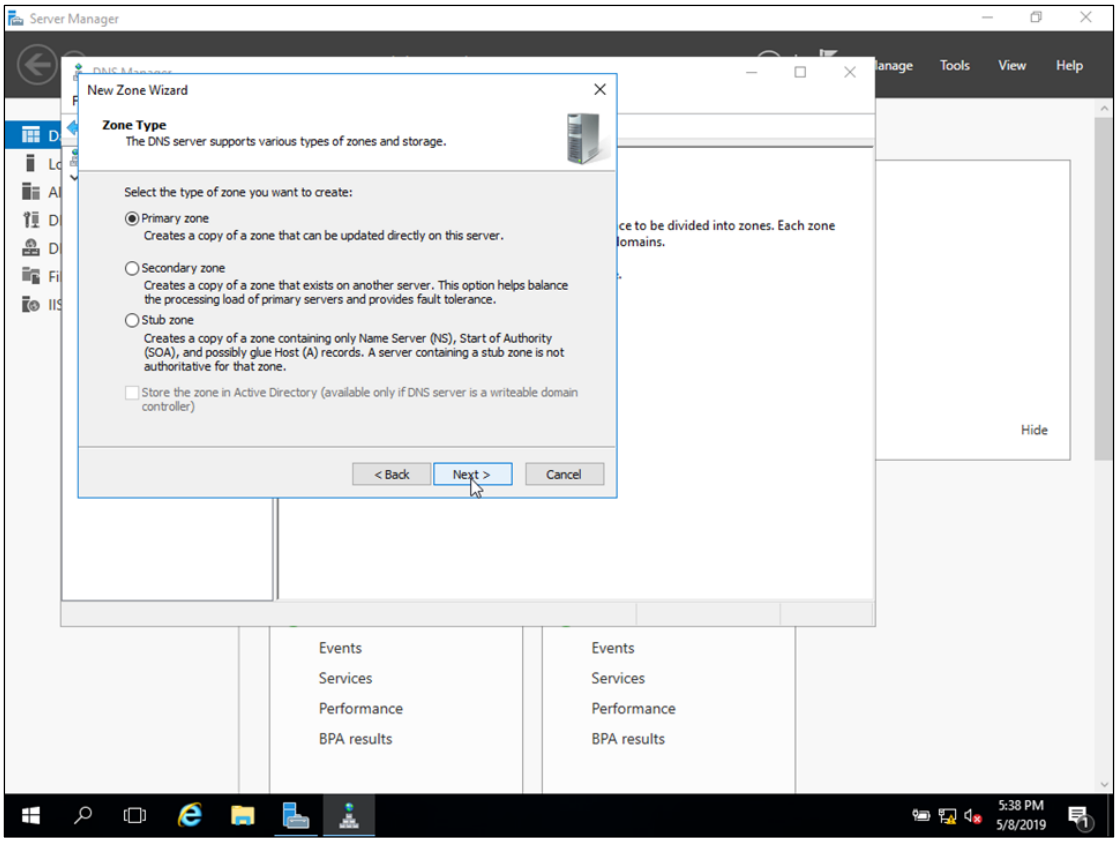

Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

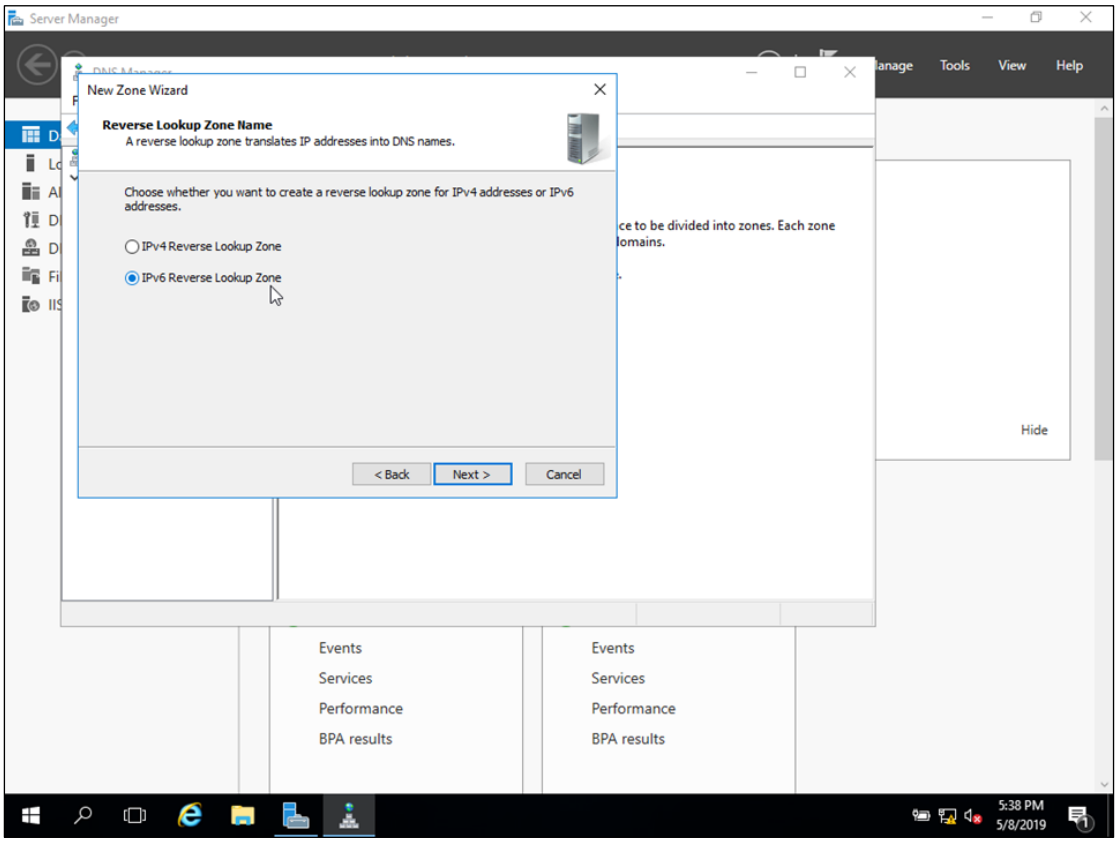

Server Manager
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

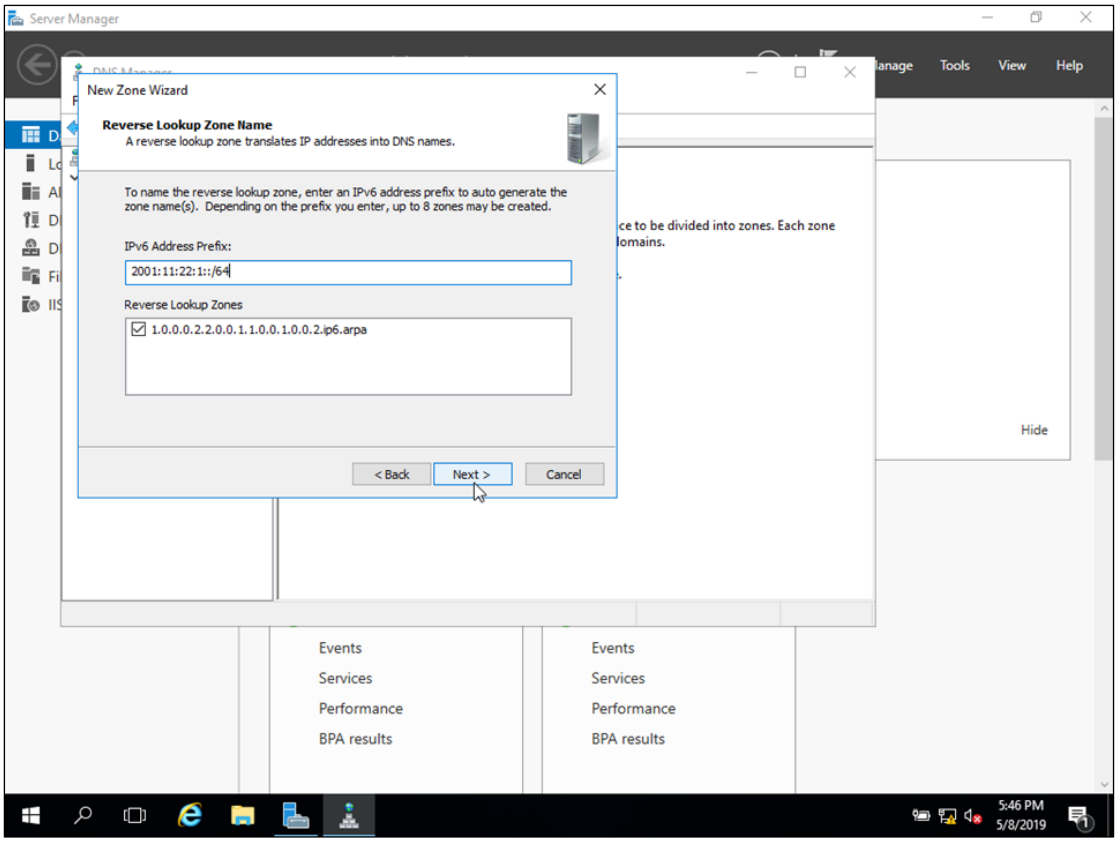

Server Manager
DNS Manager
File
Action
View
Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
Trust Points
Conditional Forwarders
New Host
Name (uses parent domain name if blank):
ns1
Fully qualified domain name (FQDN):
ns1.server.tw.
IP address:
2001:11:22:1::100
Create associated pointer (PTR) record
Add Host
Cancel
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:37 PM
5/8/2019

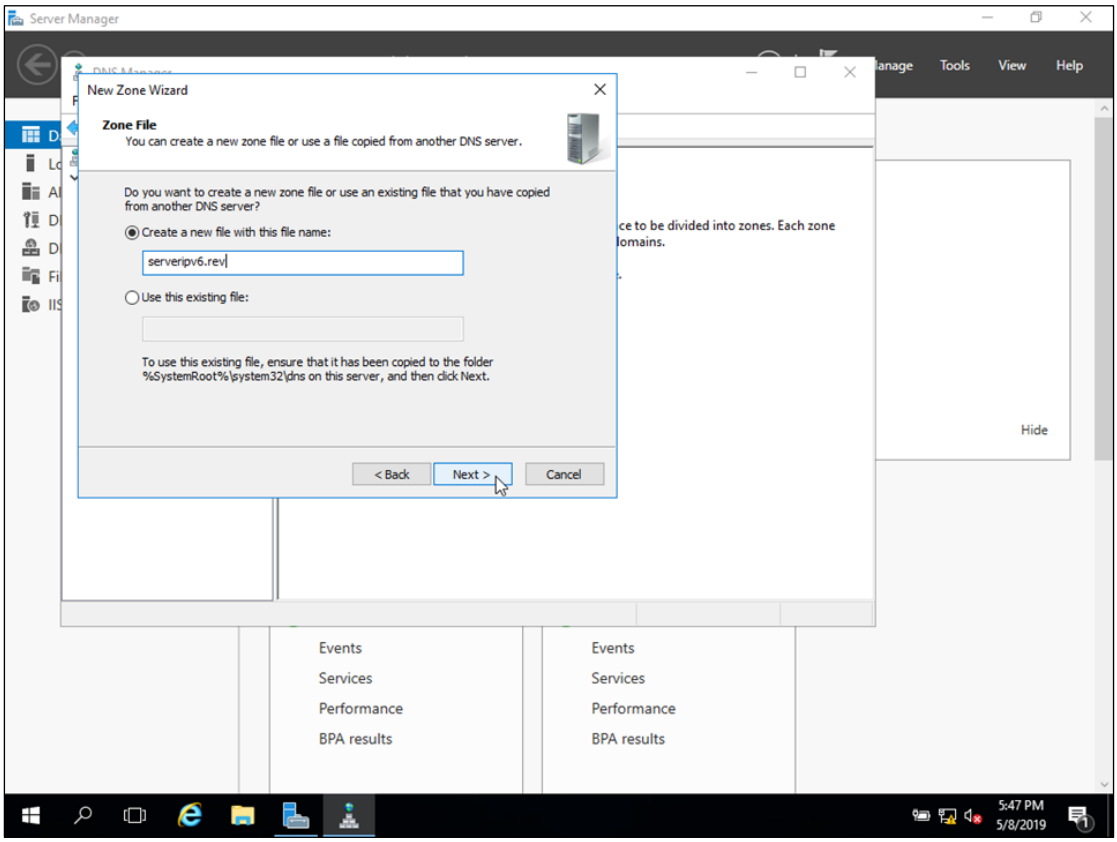

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lo
Trust Point
Conditiona
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone
rmation about one or more contiguous DNS domains.
ew zone, on the Action menu, click New Zone.
Create a new zone.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

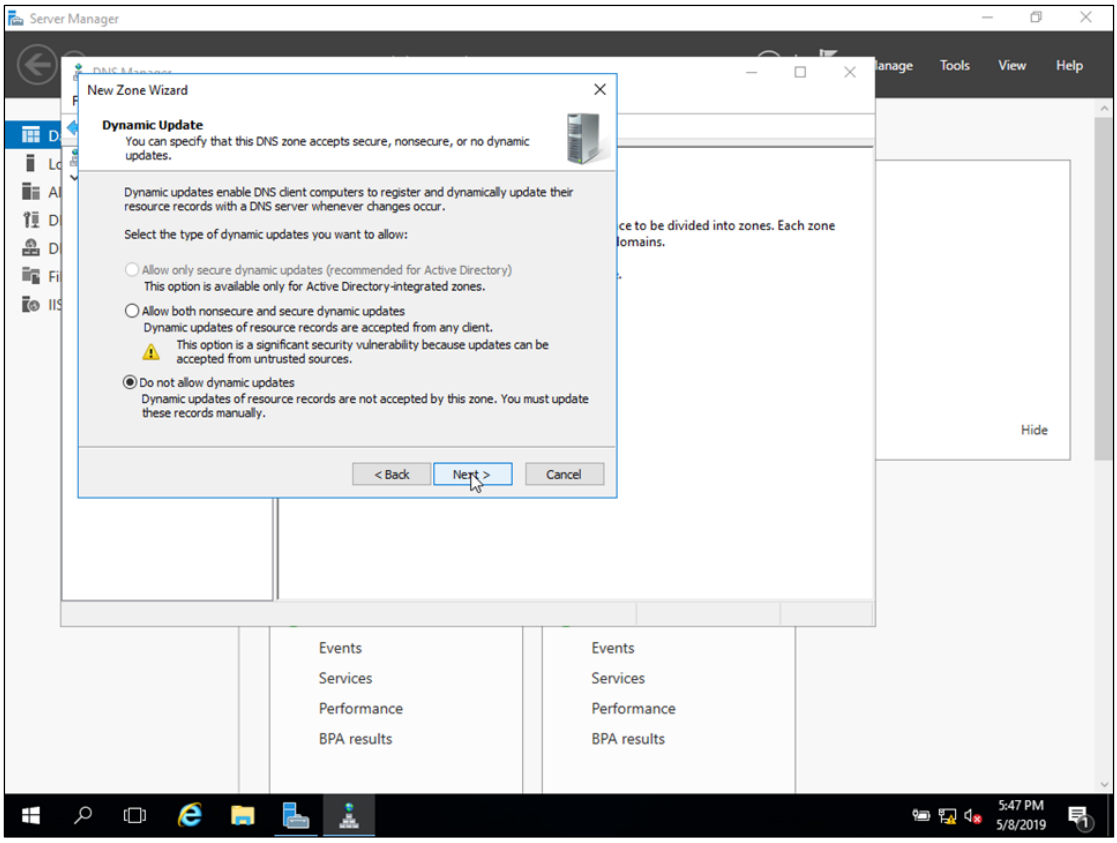

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
ce to be divided into zones. Each zone
omains.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

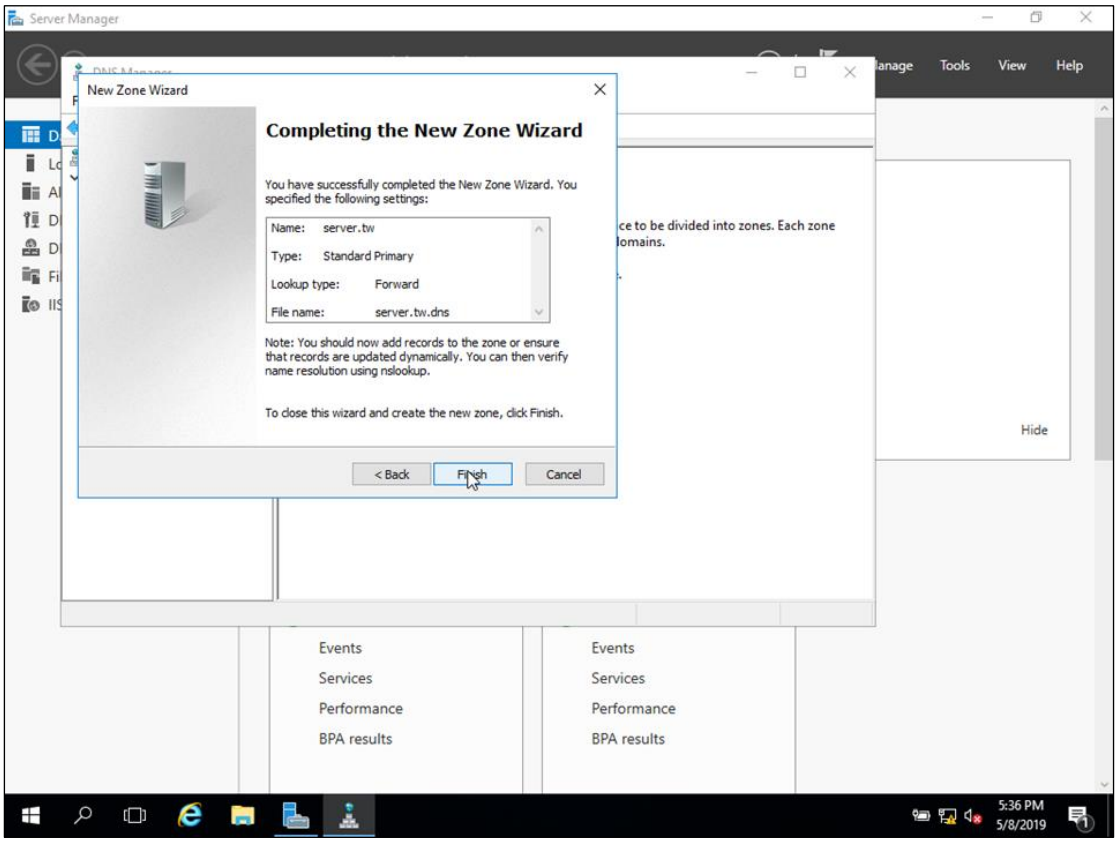

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

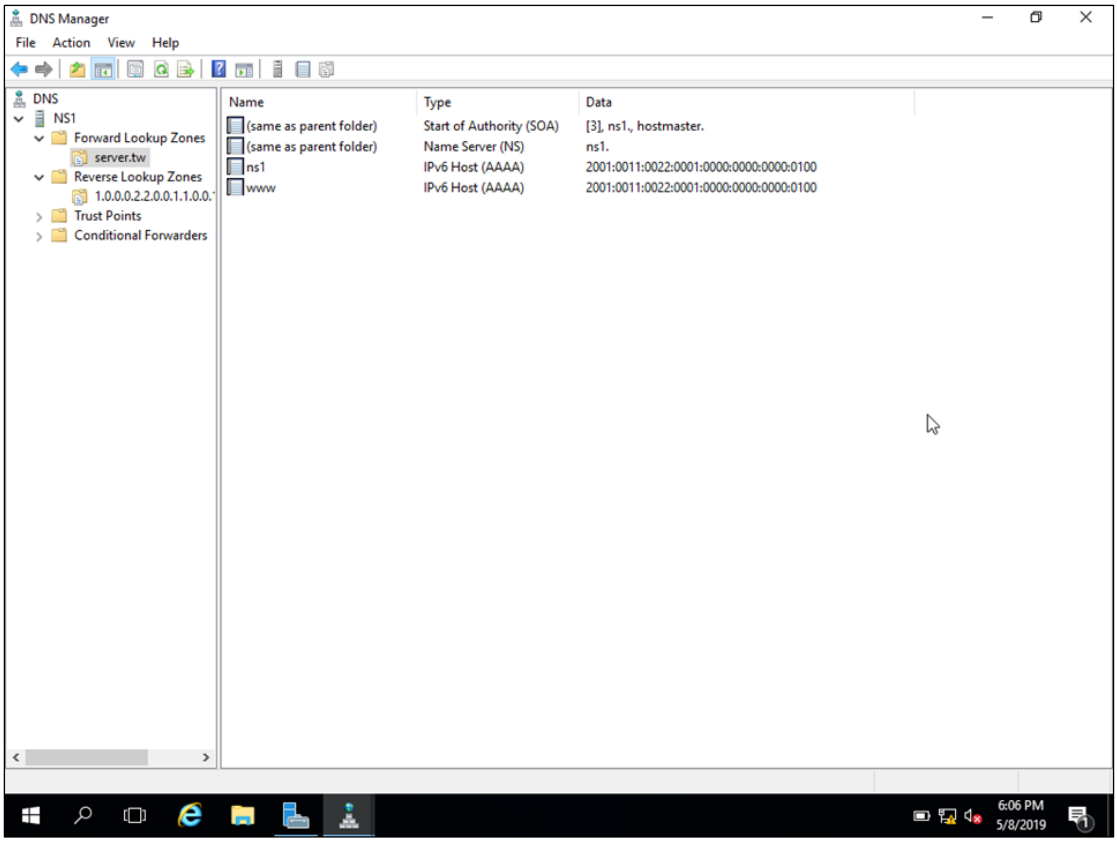

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.
IPv4 Reverse Lookup Zone
IPv6 Reverse Lookup Zone
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

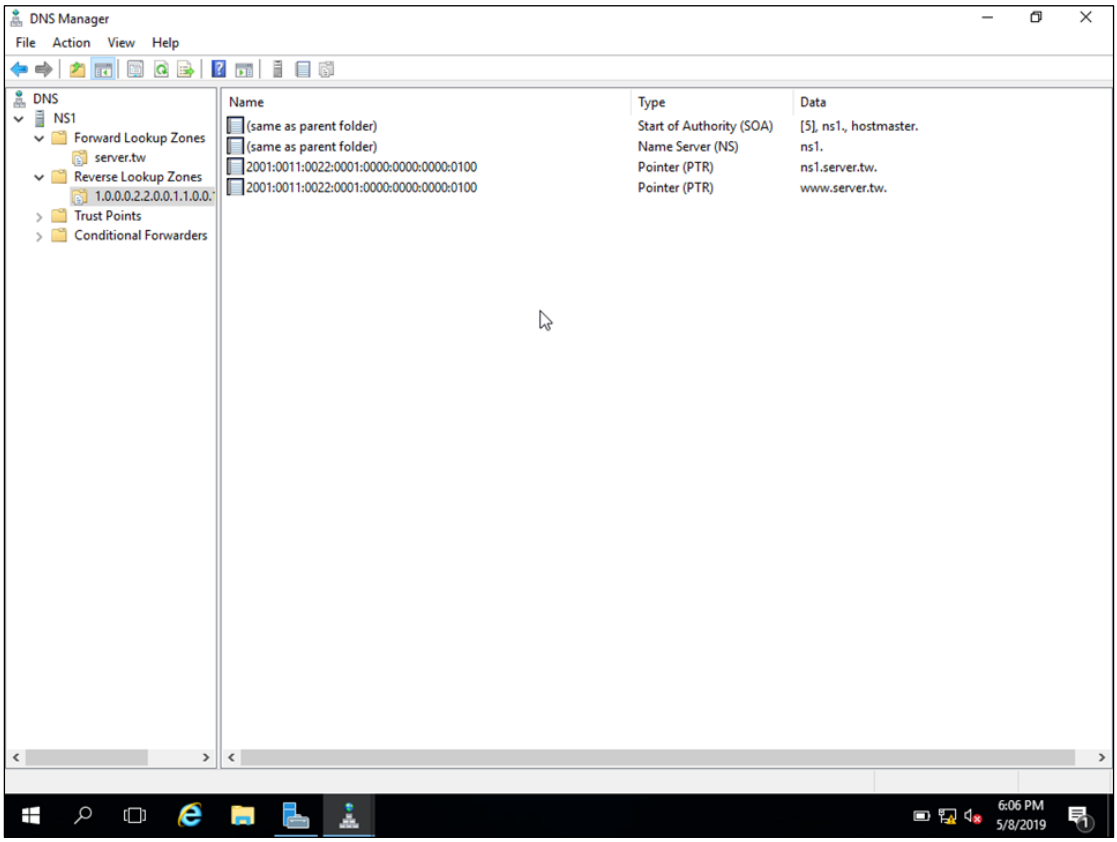

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.
IPv6 Address Prefix:
2001:11:22:1::/64
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.1.0.0.2.ip6.arpa
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:46 PM
5/8/2019

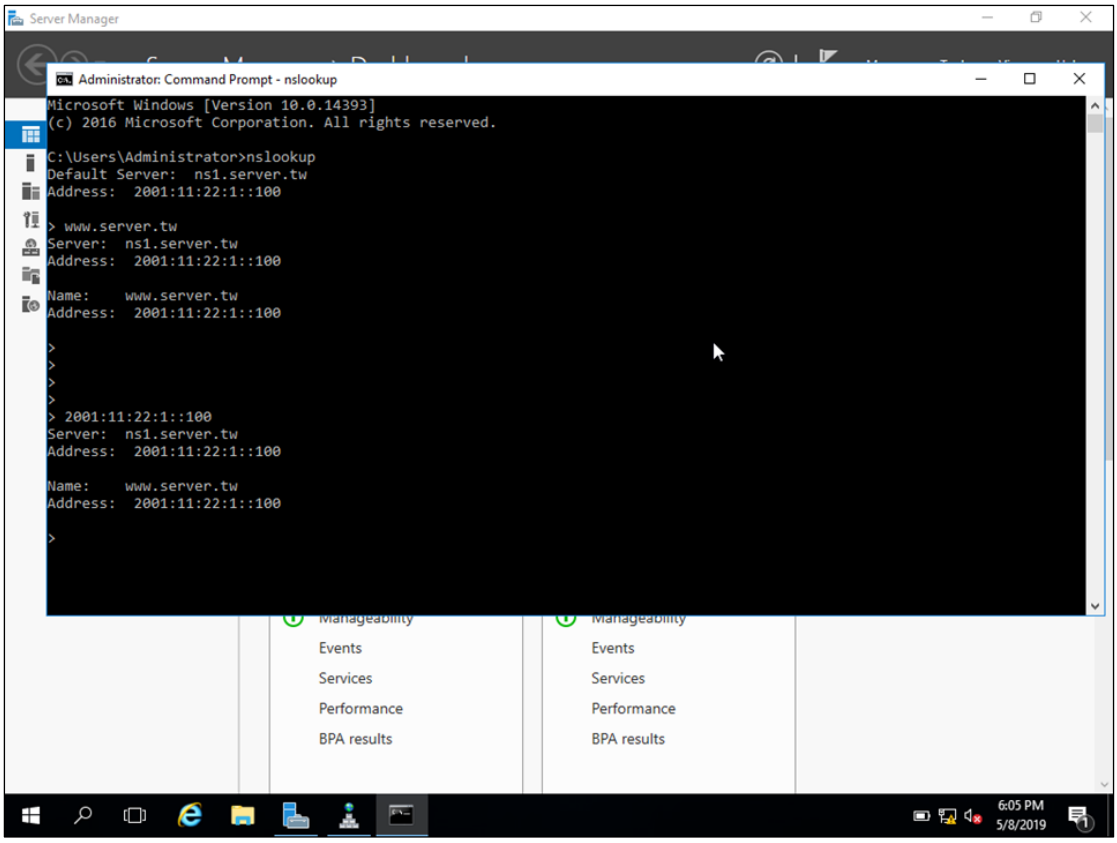

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
serveripv6.rev
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:47 PM
5/8/2019


Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:47 PM
5/8/2019

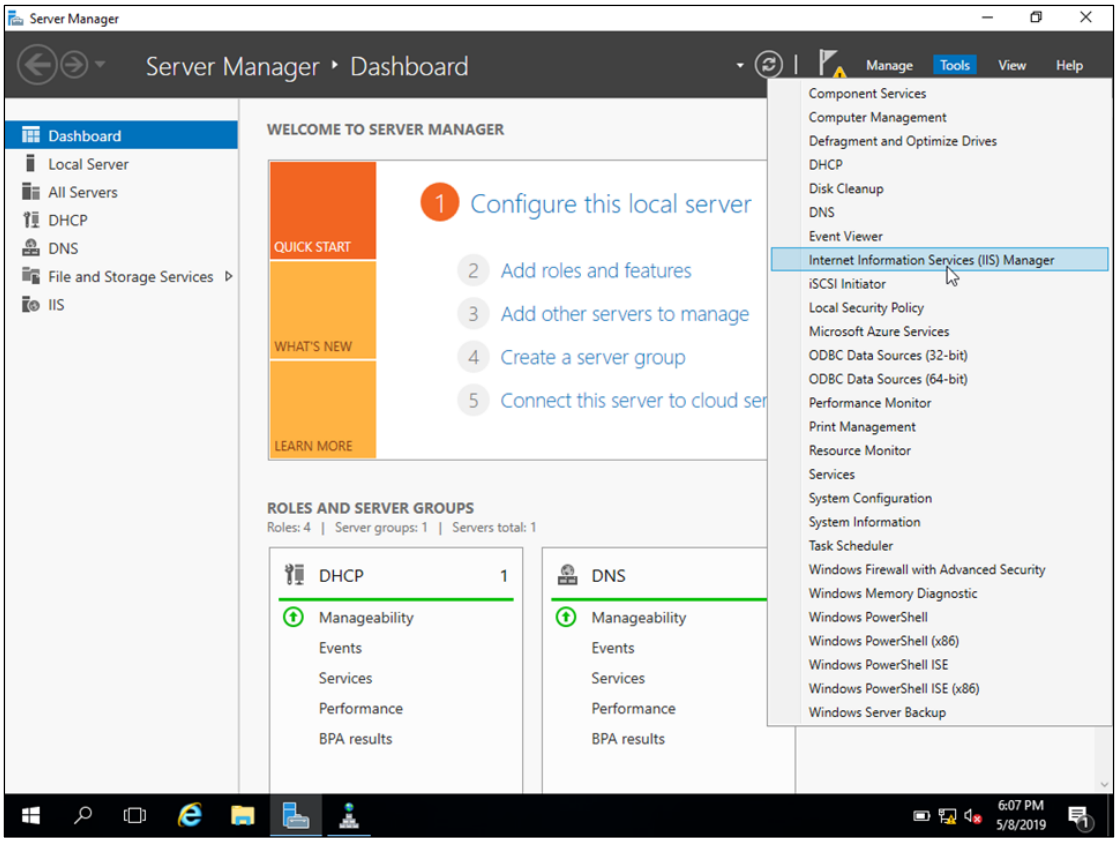

Server Manager
Tools
View
Help
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

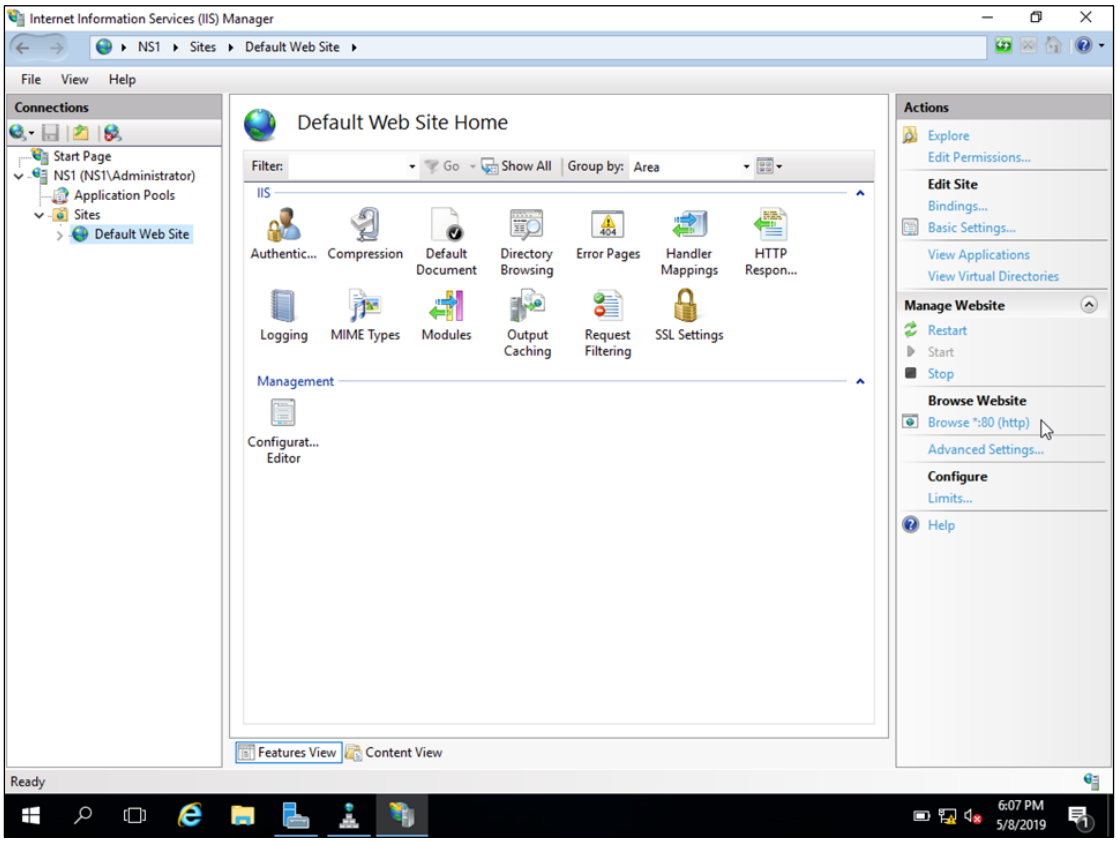

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[3], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
ns1
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
www
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
6:06 PM
5/8/2019

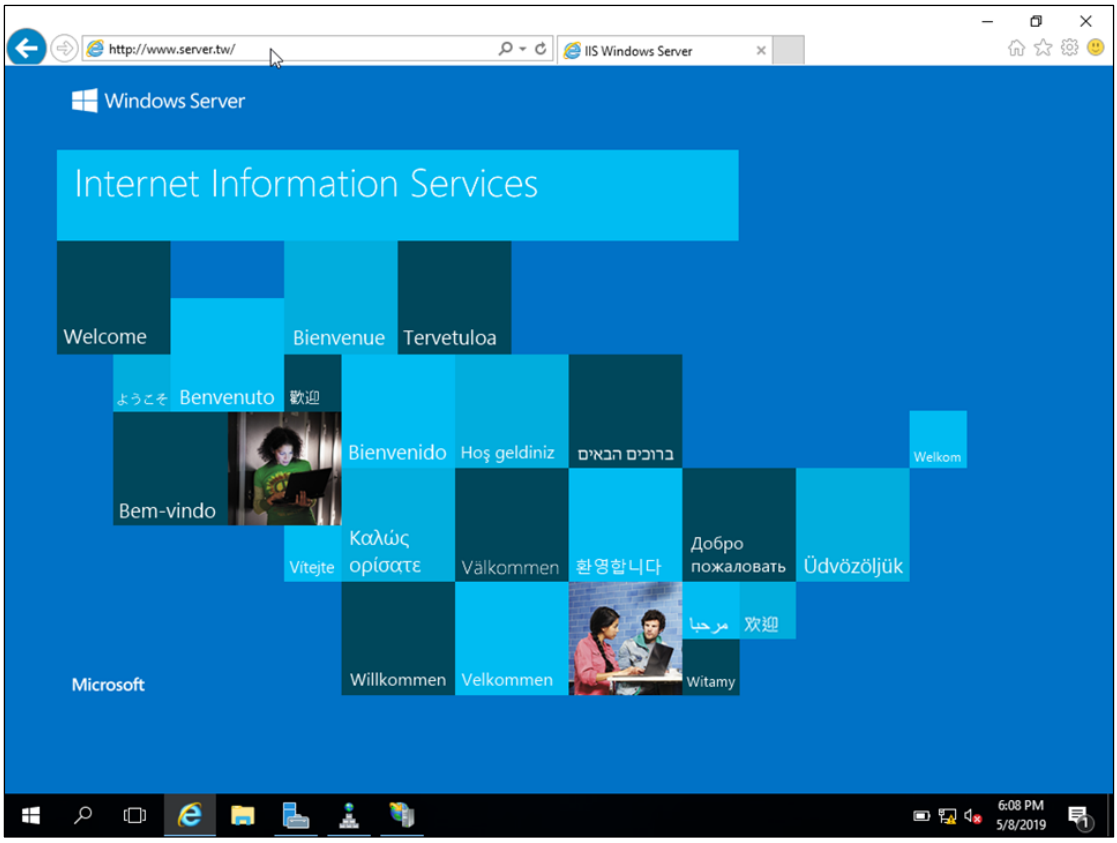

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[5], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
ns1.server.tw.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
www.server.tw.
6:06 PM
5/8/2019

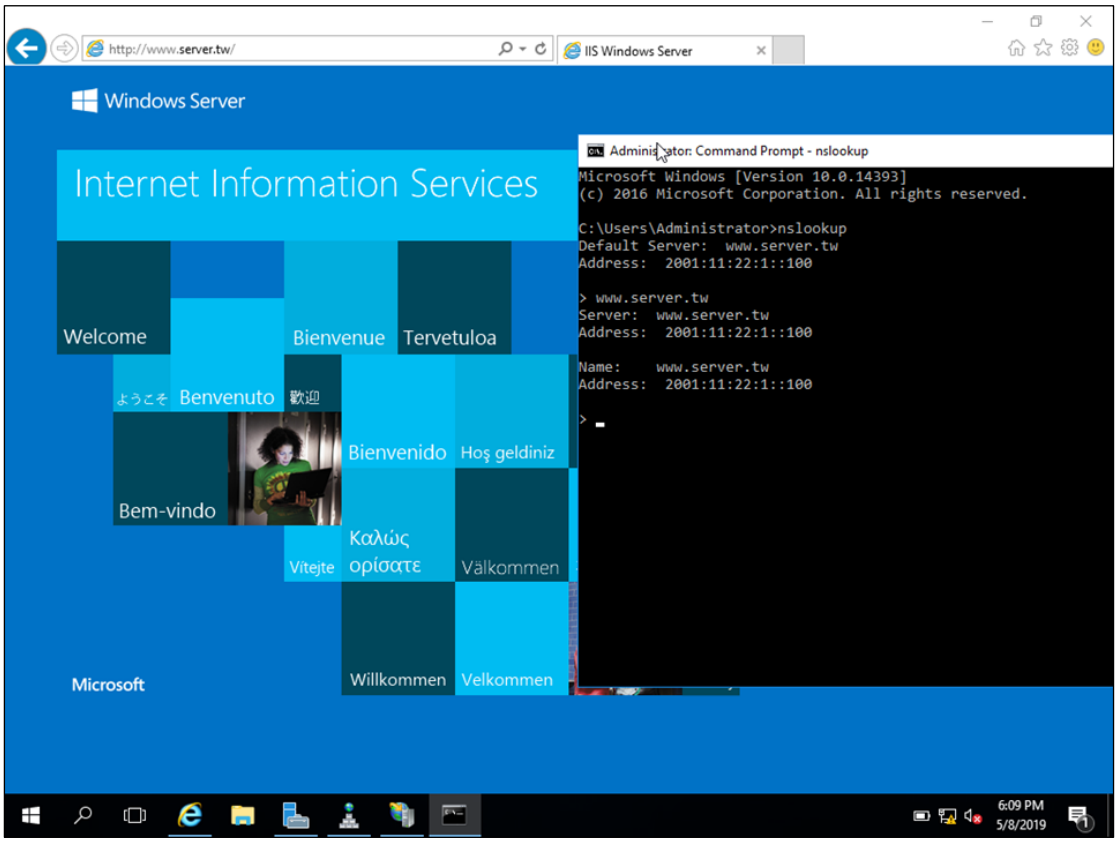

Server Manager
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: ns1.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
>
>
>
> 2001:11:22:1::100
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
6:05 PM
5/8/2019


點進網域新視界！
IPv6建置示範
IIS 系統設定

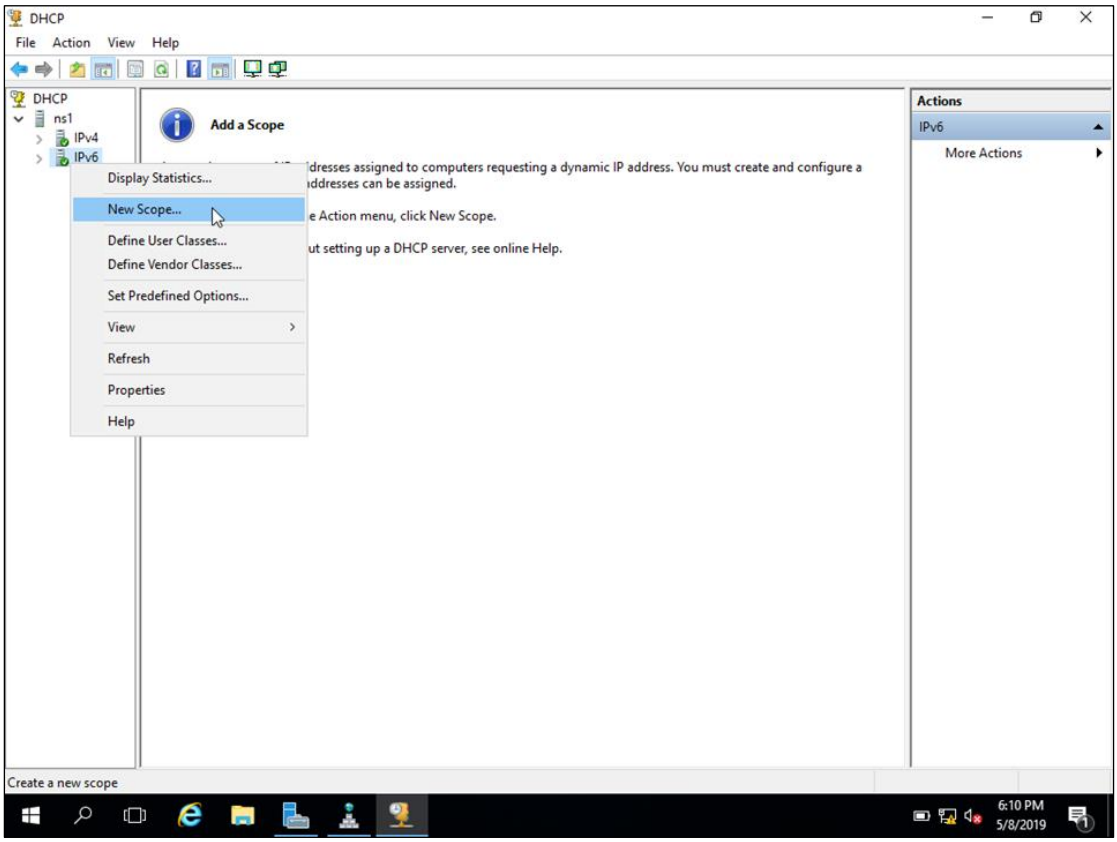

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud ser
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
DHCP 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
6:07 PM
5/8/2019

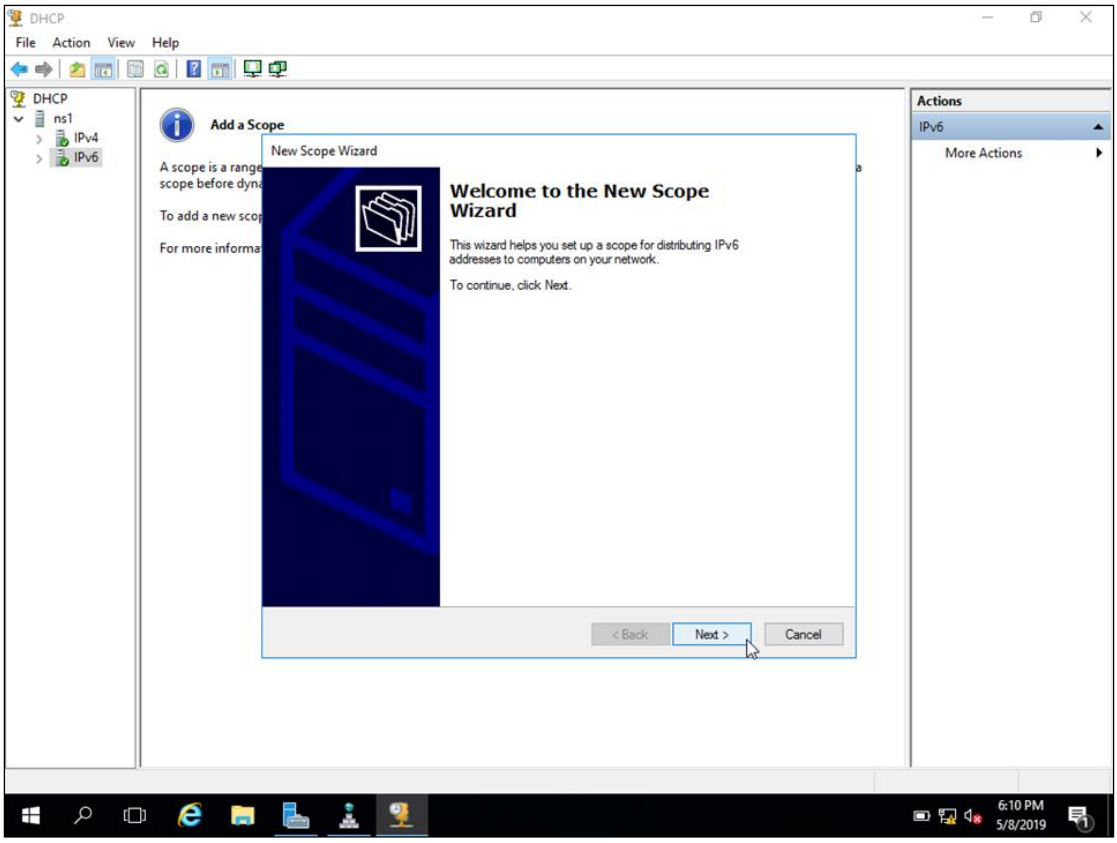

Internet Information Services (IIS) Manager
NS1 ‣ Sites ‣ Default Web Site ‣
File
View
Help
Connections
Start Page
NS1 (NS1\Administrator)
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
Help
Ready
6:07 PM
5/8/2019

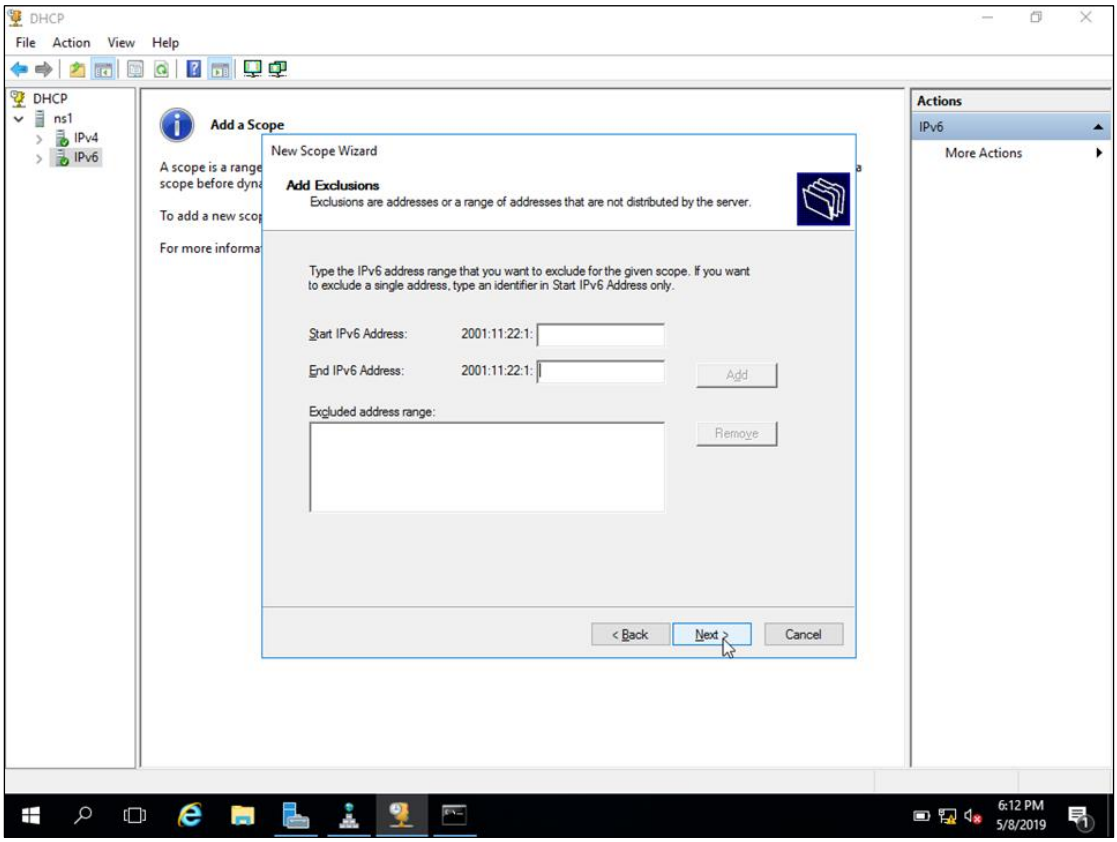

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bem-vindo
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Vítejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft
6:08 PM
5/8/2019

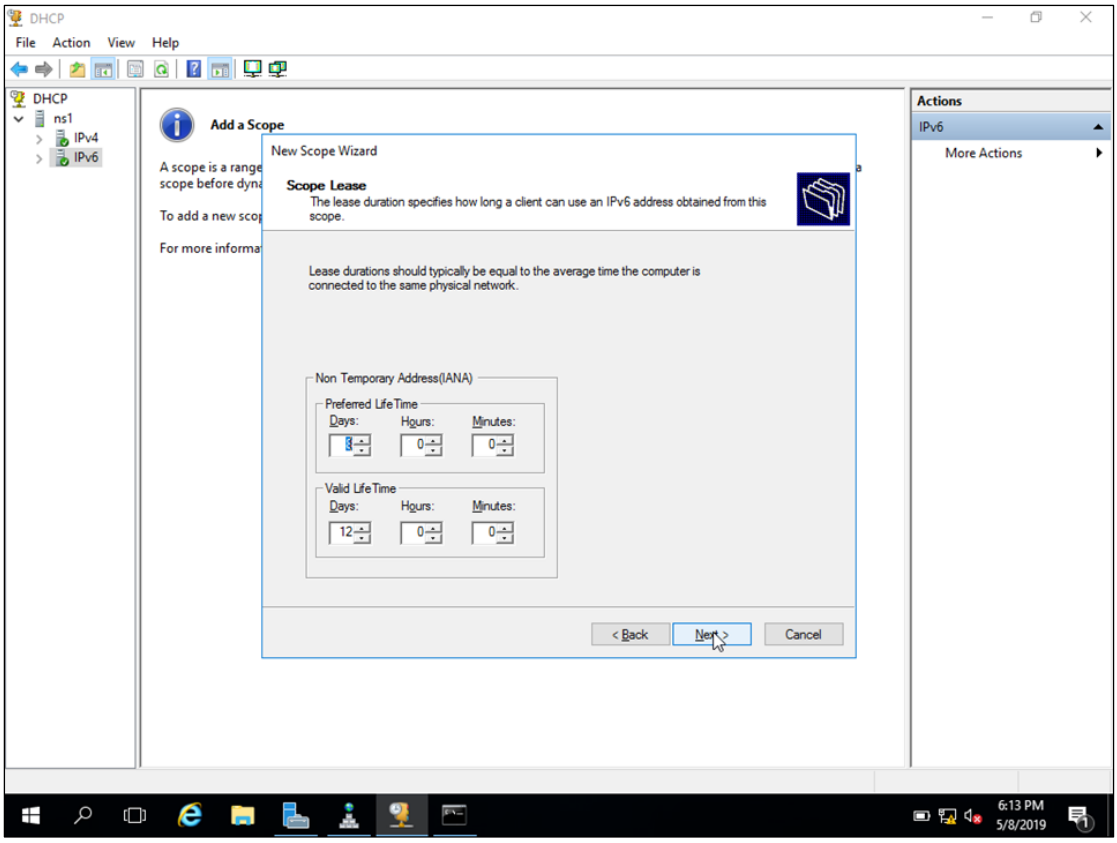

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: www.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: www.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bem-vindo
Bienvenido
Hoş geldiniz
Vítejte
Καλώς ορίσατε
Välkommen
Willkommen
Velkommen
Microsoft
6:09 PM
5/8/2019

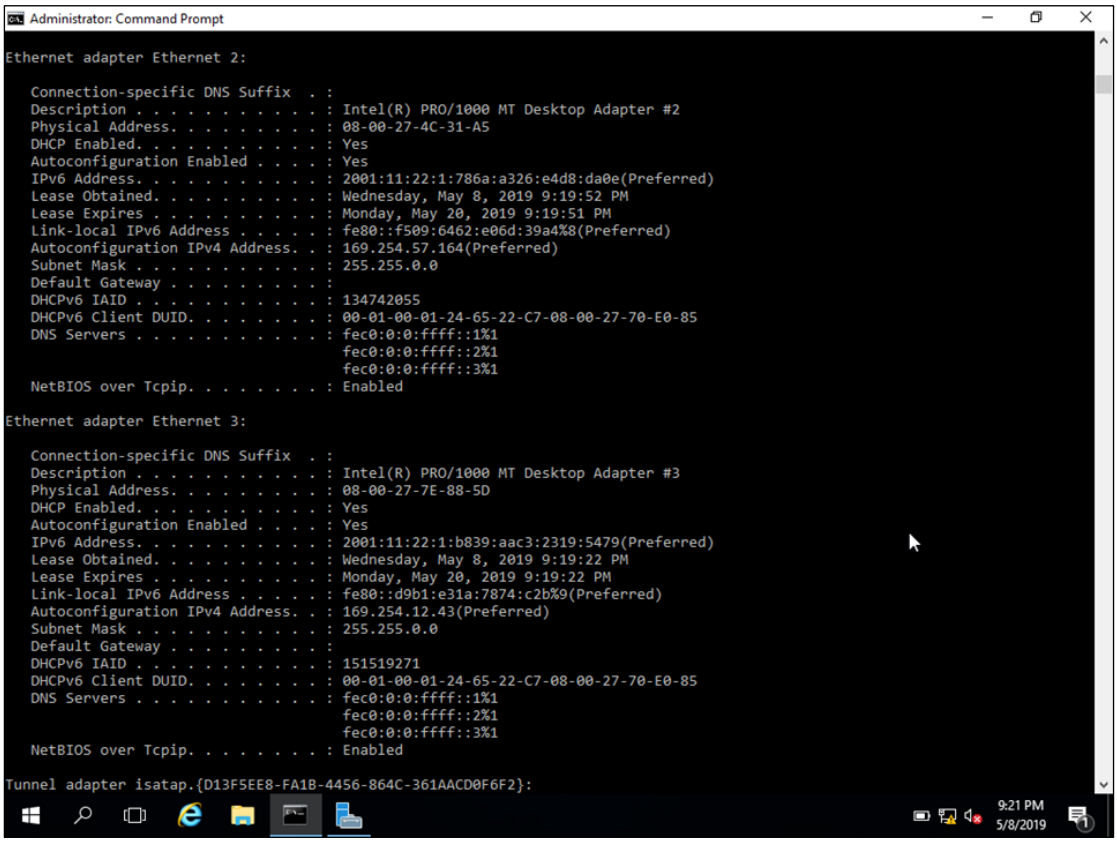

點進網域新視界！
IPv6建置示範
DHCP 系統設定


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
Display Statistics...
New Scope...
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
View
Refresh
Properties
Help
Actions
IPv6
More Actions
Create a new scope
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IPv6 addresses to computers on your network.
To continue, click Next.
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.
Start IPv6 Address: 2001:11:22:1:
End IPv6 Address: 2001:11:22:1:
Add
Excluded address range:
Remove
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:12 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Scope Lease
The lease duration specifies how long a client can use an IPv6 address obtained from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network.
Non Temporary Address(IANA)
Preferred Life Time
Days: Hours: Minutes:
8 0 0
Valid Life Time
Days: Hours: Minutes:
12 0 0
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:13 PM
5/8/2019


Administrator: Command Prompt
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Physical Address. . . . . : 08-00-27-4C-31-A5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:11:22:1:786a:a326:e4d8:da0e(Preferred)
Lease Obtained. . . . . : Wednesday, May 8, 2019 9:19:52 PM
Lease Expires . . . . . : Monday, May 20, 2019 9:19:51 PM
Link-local IPv6 Address . . . . . : fe80::f509:6462:e06d:39a4%8(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.57.164(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 134742055
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Ethernet 3:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #3
Physical Address. . . . . : 08-00-27-7E-88-5D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:11:22:1:b839:aac3:2319:5479(Preferred)
Lease Obtained. . . . . : Wednesday, May 8, 2019 9:19:22 PM
Lease Expires . . . . . : Monday, May 20, 2019 9:19:22 PM
Link-local IPv6 Address . . . . . : fe80::d9b1:e31a:7874:c2b%9(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.12.43(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 151519271
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Tunnel adapter isatap.{D13F5EE8-FA1B-4456-864C-361AACD0F6F2}:
9:21 PM
5/8/2019

資料庫IPv6調整示範

點進網域新視界！

在設定MySQL過程中需要設定

--bind-address= [IP/Hostname]

[IP/Hostname] 可以是

IPv4 address

IPv6 address

Hostname

在 my.cnf 設定檔中的[mysqld] 底下

設定 bind-address = ::

只要設定 :: 就可以接收 IPv4 or IPv6 的連接

179

點進網域新視界！

作業系統與網站升級流程步驟和檢查項目清單

網路服務升級 IPv6 檢測作法說明

https://is.gd/UCmheO

IPv6 網際網路通訊協定 升級推動方案

網路服務升級 IPv6 檢測作法說明

網際網路通訊協定升級推動辦公室檢測 DNS、Web、Email、以及 FTP 等各項外部網路服務是否升級至 IPv6 的檢測作法說明如下：

一、檢測 DNS 服務是否升級至 IPv6

(1). 檢測方式說明：

DNS 服務升級 IPv6 之檢測為透過純 IPv6 連線逐層檢查，從最上層的 root DNS 檢測起，再檢測 .tw DNS 以及 .com.tw/.gov.tw/.org.tw DNS 等，再到貴機關的 DNS 主機，一層一層的檢查，

a.檢測各層的 DNS 主機是否有支援 IPv6；

b.檢測各層的 Domain name 是否有設 AAAA 紀錄。

(2). 檢測作法：

逐層檢測時，若有發生檢測不通過的情形，可以在 Linux 環境下用下列 dig 指令的方式了解哪個部份有問題，指令如下：

dig -6 [填入欲檢查的 DNS] AAAA +trace

(例如：dig -6 www.gsnv6.tw AAAA +trace)

(3). 常見問題

181

線上檢測服務升級

https://www.gsnv6.tw/inventory/checkservicepub.cgi

線上檢測服務升級IPv6

檢測程式作法說明

若是檢測一般Web網站，前面請加 http:// ，例如 http://www.twnic.net.tw
若是檢測 https 網站，前面請加 https:// ，例如 https://www.gsnv6.tw
若是檢測 Email, DNS, FTP，請直接輸入主機名稱(domain name)，例如 dns2.twnic.net.tw
本網站 www.gsnv6.tw 的IPv6位址為：2001:c50:ffff:1::9016

系統分類	服務系統URL(例如：www.gsnv6.tw，請留意上面之說明文字)
Web ▼	

送出檢測

182

IPv4/IPv6雙軌環境下資訊安全規劃概述

點進網域新視界！

ICP IPv4/IPv6升級及網路安全防護差異

- IPv4以ARP表格尋找要傳遞的IP位址，IPv6則以ICMPv6將通訊資訊包在封包內
- IPv4對於Domain的定義放在A record內，IPv6則以AAAA record對應
- IPv4使用DHCP動態配置IP，IPv6 則以DHCPv6達成相同功能
- MTU(最大傳輸單位)在IPv4是576個位元組，IPv6則是1280個位元組

- IPv6 Ready Logo是由國際IPv6論壇組成的標章委員會設計及制定的規範
- IPv6 Ready Logo認證分成Phase-1 Logo、Phase-2 Logo及功能性Logo
- Phase-1 Logo 表明設備包括強制性的核心機制基本上能夠與其他設備進行通訊
- Phase-2 Logo表明設備全部符合IPv6基本協議相關RFC
- 擴展功能性Logo有包括DHCPv6、IPSEC、SIP Logo等

- 新創公司建議使用Amazon的AWS及Google的Google Cloud Platform及Microsoft的Azure等的大型且完備的雲端主機
- 或者使用Linode、Digital Ocean等雲端主機
- 若使用台灣的雲端主機，須先詢問是否有支援IPv6，有些台灣雲端業者不支援

- 網站伺服器建議使用Apache、Nginx或IIS，因為普及率高，支援IPv6
- 如果考慮多平台支援，以Apache跟Nginx為優先考量

- 網站伺服器建議使用Apache、Nginx或IIS，因為普及率高，支援IPv6
- 如果考慮多平台支援，以Apache跟Nginx為優先考量

- 針對IPv6的網路設備的採購，建議購買有IPv6 Ready Logo的設備。
- 雲端主機如Amazon AWS、Google Cloud Platform及Microsoft Azure都有提供完整的服務，且支援IPv6，適合新創公司使用。
- 網站伺服器依據公司未來發展需求而定，不論是使用Apache、Nginx或者Microsoft IIS，都可以支援IPv6 。
- 網站作業系統不論是使用Unix based如CentOS、Ubuntu或者Microsoft Windows，目前都已經有支援IPv6 。
- 硬體防火牆在市場上大品牌眾多，如果是使用於機房，建議優先考慮使用硬體式防火牆 。

- ICP安全策略的制定從內部到外部，建議可以先參考現有IPv4的安全策略，並製作IPv6的安全管理規範，之後再針對差異部分，進行修正。

ICP IPv4/IPv6升級雙雙協定網路安全防護檢查項目清單

- 機房設備盡量挑選具有IPv6 Ready Logo的設備或者使用已經完整實現IPv6的雲端主機服務商(例如Amazon AWS、Google Cloud Platform、Microsoft Azure)。
- 路由器須開啟IPv6。
- 防火牆須設定IPv6過濾規則(防火牆分為硬體防火牆跟軟體防火牆)。
- 網站伺服器(包括Apache、Nginx及Microsoft IIS等)須開啟IPv6 listening並設定好安全規則。
- 作業系統也須開啟IPv6設定。

ICP IPv4/IPv6升級雙雙協定網路安全防護檢查項目清單

- 機房設備盡量挑選具有IPv6 Ready Logo的設備或者使用已經完整實現IPv6的雲端主機服務商(例如Amazon AWS、Google Cloud Platform、Microsoft Azure) 。
- 路由器須開啟IPv6 。
- 防火牆須設定IPv6過濾規則(防火牆分為硬體防火牆跟軟體防火牆) 。
- 網站伺服器(包括Apache、Nginx及Microsoft IIS等)須開啟IPv6 listening並設定好安全規則。
- 作業系統也須開啟IPv6設定。

- 應利用公司現有的安全漏洞掃描工具對修改的網站進行安全漏洞掃描，確保無安全問題。
- 利用壓力測試工具，對修改後的網站近行壓力測試，確保在同時支援IPv4跟IPv6的情況下，網站可以運作正常。
- 確定現在使用的安全漏洞/程式碼掃描工具都支援IPv6。

- 對於所有進出的IPv6封包都需要進行過濾。
- 針對ICMPv6封包進行過濾，可慮哪些可以放行，哪些需要阻擋，可以參考RFC4890。
- IPv6 extension header要進行過濾，並只能開放有需要的。
- 盡量維持IPv4跟IPv6規則的同步。

- 要求你的合作廠商一起升級IPv6。
- 從外部測試網站，利用一些IPv6 驗證網站或者申請一個外部的主機，進行外部測試。
- DNS記得要設定IPv6的AAAA record 。
- 連帶的服務也記得一併升級IPv6。

ICP IPv4/IPv6升級輔導手冊

- MySQL：儲存IPV6的欄位長度需要為varchar(39) 如果是要存 varbinary 則為 varbinary(16)
- [mysqld]
- bind_address= *
- 如果要限定只能用Ipv6連線，可以設定成 bind_address = ::1
- 當設定之後，從console 連進MySQL時，需要先建立一個ipv6的帳號
- mysql> create user ‘ipv6user’@‘::1’ identified by ‘ipv6pass’;
- mysql> create user ‘remoteipv6user’@‘2001:db8:0:f101::2’ identified by ‘remoteipv6pass’;

- Apache的設定檔為 httpd.conf
- Listen 80
- Listen 443
- Listen [::]:80
- Listen [::]:443
-
- <VirtualHost *:80 [::]:80>
- ...
- </VirtualHost>

- <VirtualHost [2607:f:1:11::4]>
- </VirtualHost>

- nginx設定檔為 nginx.conf
- 如果是443 SSL要啟用 ipv6
- server {
- listen 80 default_server;
- listen [::]:80;
- listen 443 ssl http2;
- listen [::]:443 ssl http2;
- }

- 新版的作業系統Kernel都有支援IPv6，但有些預設關閉、有些預設開啟。
- 作業系統許多都會內建防火牆機制，防火牆也需要一併將IPv6 的規則設定後啟用，以免造成IPv6封包可以讓網卡接送跟傳送 ，但是在軟體防火牆那一層卻被過濾掉，造成無法連線。

- 範例：僅允許特定IPv6 位址可以連線
- ip6tables -I INPUT -p tcp -m tcp --dport <port> -s 2b00:x:x:x::/64 -j ACCEPT

- 範例：禁止特定IPv6 位址不能連線
- ip6tables -I INPUT -p tcp -m tcp --dport <port> -s 2b00:x:x:x::/64 -j DROP

常見網路安全管理機制簡介

- 封包過濾防火牆
- NetFlow 流量監測
- DPI 資安防禦設備

201

(一) 防火牆

防火牆以提供網路封包篩選過濾為主要功能，其做法是依據預設好的規 則，對流入或流出的 IP 封包是否放行進行管制，以決定是否允許或阻止網路連線存取的行為。

202

(一) 防火牆

封包過濾通常只檢查封包的表頭(Header)，不會檢查資料段的內容，可以 檢查的項目包括來源 IP 位址、目的 IP 位址、協定種類(TCP、UDP 等)、 TCP 或 UDP 的來源埠、TCP 或 UDP 的目的埠、以及 ICMP 的訊息代碼等。

203

(一) 防火牆

封包過濾型防火牆建置簡單、價格便宜、效率佳，但不易定義出有效又能 長期使用的規則，也無法進行應用層協定的防護。

目前相當熱門的次世代防火牆

Layer 7 Applications Firewall

204

(二) NetFlow 流量監測

Netflow (Network Flow)是一套網路流量監測方式

一個 Flow 代表一個來源 IP 位址和目的 IP 位址之間傳輸的單向流量

且所有封包具有相同傳輸層的來源及目的端口號

205

(二) NetFlow 流量監測

Netflow 以網路介面為單位呈現分析的結果

包含各服務流量的資訊、各 IP 位址的流量資訊，甚至各種傳輸協議之流量高低排序...等等

並可以列出疑似受病毒感染或被植入惡意程式的電腦所使用的 IP 列表

206

(二) NetFlow 流量監測

網管人員可以透過Netflow 快速有效的掌握所管轄網路的狀態，包含效能、壅塞程度等資訊。

第一可從網路層的角度分析，例如有些攻擊行為可能針對某個特定埠進行攻擊，或是出現不合理的 IP 位址。

第二則是從傳輸層角度分析，例如透過Netflow 資料揭連線(Session)數目最多的主機，或者不正常的封 包控制旗標(TCP Flag)。

207

(三) DPI 資安防禦系統

DPI 為深層封包檢測的簡稱

其做法為經由接收路由器介面端口複製的鏡像(Port Mirror)封包

經由封包的內容的特徵比對

進行第三層到第七層的資安風險分析

208

(三) DPI 資安防禦系統

DPI 資安防禦系統可以判斷封包所屬的服務類型例如是否屬於 YouTube 等常見的服務流量

也可以偵測出典型的殭屍病毒，例如網路聊天感染(Internet Relay Chat Bot, IRC Bot)等安全相關的病毒程式，並可以將相關資訊儲存於資料庫中，再藉由網頁介面呈現統計資料

209

(三) DPI 資安防禦系統

許多具有安全疑慮的封包特徵值並無法從表頭欄位進行判別，DPI 系統則可以深入觀察封包內容，並檢驗出可疑封包及流量。

對於難以掌握的殭屍網路，都必須藉由 DPI 系統才比較容易檢驗出可疑的感染封包。

210

(三) DPI 資安防禦系統

但由於深度封包檢測需要較複雜的比對和檢測，若以通透模式 (Transparent Mode) 接在既有網路骨幹時，若流量超過設備的負荷，可能會導致進出口壅塞，甚至有可能出現封包遺失 (Packet Loss) 的狀況。

故大多數 DPI 設備都是採取旁聽模式 (Sniffer Mode) 去監測鏡像 (Mirror) 的流量。

211

雙協定網路安全管理機制差異性

以下整理比較 IPv4/IPv6 雙協定網路可能面臨的安全性議題

- IPv4 網路常見攻擊行為
- IPv6 網路在安全機制的強化

212

IPv4 網路常見攻擊行為

IPv4 的設計主要考慮點對點傳輸模型，在網路安全的考量較少，因此導致 幾種下列常見的攻擊行為：

- 服務阻斷式攻擊(Denial of Service Attack, DoS)：此種攻擊為對服務提供者進行大量非法要求，使得目標系統未處理這些非法要求而癱瘓正常服務提供
- 惡意程式散播(Malicious code distribution)：病毒或蠕蟲會藉由 IPv4 小位址空間裝載惡意程式散播危及主機甚至遠端系統的安全性

213

- 分片攻擊(Fragmentation Attacks)：利用作業系統需大量重組 IPv4 封包的特性，傳送不完全且不連續的片段封包導致主機當機
- 埠口掃描攻擊(Port Scanning)：利用端口掃描技術找出潛在的漏洞，由於 IPv4 的位址空間很小，整個 ClassC 網路僅需四分鐘就可全部掃描
- ARP 欺騙及 ICMP 重導攻擊(ARP poisoning and ICMP redirect)：偽造的 ARP 回應通知網域中主機不正確的對應資訊可能導致封包傳送錯誤

214

IPv6 網路在安全機制的強化

大部分 IPv4 常見的攻擊已可藉由成熟的防禦機制過濾出可疑封包，或是經由一些網路技術而避免。

IPv6 則從網路的設計上，提供比 IPv4 更完整的網路安全機制，說明如下：

215

IPv6 網路在安全機制的強化

- 預設啟動 IP 安全性協定(Internet Protocol Security, IPSec)：雖然 IPv4 也支援 IPsec，但為選擇性使用，而在 IPv6 由 RFC4301 指定所有網路節點都必須使用 IPsec 。

- IPsec包含Authentication Header(AH) 和 Encapsulating Security Payload (ESP)，以及 Internet Key Exchange (IKE) 等技術。這些技術在 IPv6 都提供更好的設計，可以防止封包欺騙、偽造、修改、重播等攻擊。

216

IPv6 網路在安全機制的強化

- 使用鄰居探索(Neighbor Discovery, ND)進行位址自動設定：不同於 IPv4 於資料鏈結(Link-Layer)層以 ARP-RARP 找出主機位址，ND 於網路層(network-layer)操作減少欺騙主機的可能

- 更多的位址空間(Large address space)：不同於 IPv4 掃描一個 Class C 僅需四分鐘，由於 IPv6 一個子網是由 64bits 組成整個掃描則需耗時 584,942,417,35 年。

217

IPv4/IPv6 雙協定共存的安全議題

雖然 IPv6 增強了大部分的安全性，但也並非萬能藥，仍然有許多安全性的挑戰。

導入 IPv4/IPv6 雙協定後的安全性議題可以分成下列幾個主題探討，網路管理者可根據這些建議，對內部網域進行管控，觀察 IPv6 相關 flow，若有異常流量情形，例如要求不存在之服務則可設定規則過濾之。

218

IPv4/IPv6 雙協定共存的安全議題

- 雙堆疊相關安全性問題：例如不適當的防火牆攔截、不穩定的 DNS 區域記錄等，因此在網路建立前就須審慎規劃
- ICMPv6 安全性問題：IPv6 網路存在封包被攔截的可能，由於採用開放式路由廣播訊息(Router Advertisement, RA)，以協調網域中主機自動獲取位址，可能發生節點假扮為路由設備並發出錯誤的 RA 廣播訊息。

219

IPv4/IPv6 雙協定共存的安全議題

- 標頭操作相關議題：由延伸性標頭(Extension header)及 IPSec 的使用可以抵擋掉大部分攻擊種類，然而，由於 EH 須被整個網路堆疊進行處理，很長的延伸性表頭及大封包可能被利用來癱瘓某些特定節點(例如防火牆)，或是假扮為攻擊，因此，最好的方式是過濾掉不支援的服務流量

- Spoofing 議題：欺騙技術仍然可能發生在 IPv6 網路中，但由於 Neighbor Discovery，Spoofing 欺騙的位址範圍僅侷限在內部網域。

220

IPv4/IPv6 雙協定共存的安全議題

- Flooding 議題：IPv6 位址不使用廣播位址已大幅減少攻擊的可能性，但多點位址傳送的位址仍然是問題，最主要的防範方式仍為過濾不存在服務之流量。

- 移動性 Mobility：移動性為 IPv6 的新特色，該協定是一複雜方程式，利用兩種類別的位址—真實位址(real address)和移動位址(mobile address)，由於此種網路的特性加上暫時性的移動位址可能暴露而成為欺騙攻擊，這需要特別安全性量測，並且網路管理者須全面了解設定。

221

IPv4/IPv6雙軌環境之資訊安全軟體與硬體設定

點進網域新視界！

IPv6 網路安全防護的建議

網路安全防護是矛與盾的戰爭，越厲害的矛會驅使發明更厲害的盾。

由於IPv6 網路尚未成為主流，相關的網路攻擊事件也幾乎還未聽聞，所以先就建議 IPv4 網路安全防護的做法為基礎，配合 IPv6 在通訊協定設計上的差異，進行規劃設置即可，同時也需要注意 IPv6 網路安全相關的研究報告，參酌安全設備廠商的建議，隨時進行安全強化的工作

223

1. 防火牆

清查既有防火牆是否支援 IPv6，如尚未支援，應經由韌體升級或重新採 購，取得支援 IPv6 的能力。以韌體升級方式支援 IPv6 的防火牆，必須注 意檢查 CPU Loading 及記憶體的消耗狀況，確定不會造成效能不足。

防 火牆支援 IPv6 後可參考 IPv4 既有規則設定 IPv6 的過濾方式，再依據監 控蒐集的 IPv6 流量資訊進行觀察，逐步補足 IPv6 的防禦規則。

224

1. 防火牆

ICMPv6 在 IPv6 網路扮演很重要的角色

在 IPv4 網路裡大部分的 ICMP 都會被關掉

再選擇適當的項目開放。

225

1. 防火牆

- 必須開放的ICMP：Types 1, 2, 3, 4, 128, 129, 130, 131, 132, 143, 148, 149, 151, 152, 153, 133, 134, 135, 136, 141, 142
- 通常開放的ICMP：Types 3 - Code 1, Type 4 - Code 0
- 必須過濾丟棄的ICMP：Types 138,144,145,146,147
- 視需要制定是否過濾丟棄的ICMP：Types 137,139,140,5-99,102,126

226

NetFlow

升級路由器的 IOS 至支援 NetFlow version 9，以提供 IPv6 的流量統計資 料，Netflow 分析軟體(如 Netflow Analyzer)也要升級到支援 IPv6

建議以不同時間排程將 IPv6 與 IPv4 流量資訊的抓取與分析時間錯開，以降低設備負載度

1:1 的 NetFlow 是目前正夯的研究資料收集目標

227

(1) 依服務類別統計流量：

每天依據服務類別統計流量資訊，例如依據 Inbound、Outbound、SSH 連線、FTP 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計。

統計的項目包括連線流量、封包數目、封包大小等，並在位居排名前面(如前 20 名)的服務類別中，觀察送出該流量的 IP 位址、總流量數、總封包數、總封包大小。

228

個人 IPv6 流量資訊查詢：

每天依據使用者 IPv6 位址統計網路流量資訊

統計的項目包含上述提到的各種服務

並以圖表呈現各類別流量一週的使用資訊

229

DPI System

DPI 主要目的為觀察封包 Payload 並比對出可疑流量，IPv6 流量 Payload的比對方式與 IPv4 並無不同，目前持續累積足夠的 IPv6 可疑流量特徵(Signature)，建議可配合 Netflow 的統計，針對異常流量進行 Payload 的觀察，以蒐集建立異常流量的特徵值數據庫

230

異常位址追蹤與控管

IPv6 用戶端位址的自動核發機制主要為 SLAAC (包含 SLAAC RDNSS 及 SLAAC + Stateless DHCPv6) 以及 Stateful DHCPv6，建議優先選用 Stateful DHCPv6 的位址核發機制，可以如同 IPv4 DHCP 的管理方式，記錄 IPv6 位址的核發記錄，並控管位址的核發原則，例如依據 MAC 位址綁定 IPv6 位址，或依據 MAC 位址管制是否核發 IPv6 位址。

231

異常位址追蹤與控管

如果選用 SLAAC 機制，則只能依據 Prefix 追蹤到相關的區域網路，雖然藉由 EUI-64 運算法可從 IPv6 位址反算出 MAC 位址，但用戶端可設定不使用 EUI-64，MAC 位址也可以手動變造，並不能保證能找出特定 IPv6 位址的使用者

所以在 SLAAC 的機制下，要責成每個區域網路的連線單位自行負擔/64 網段的資安管理責任

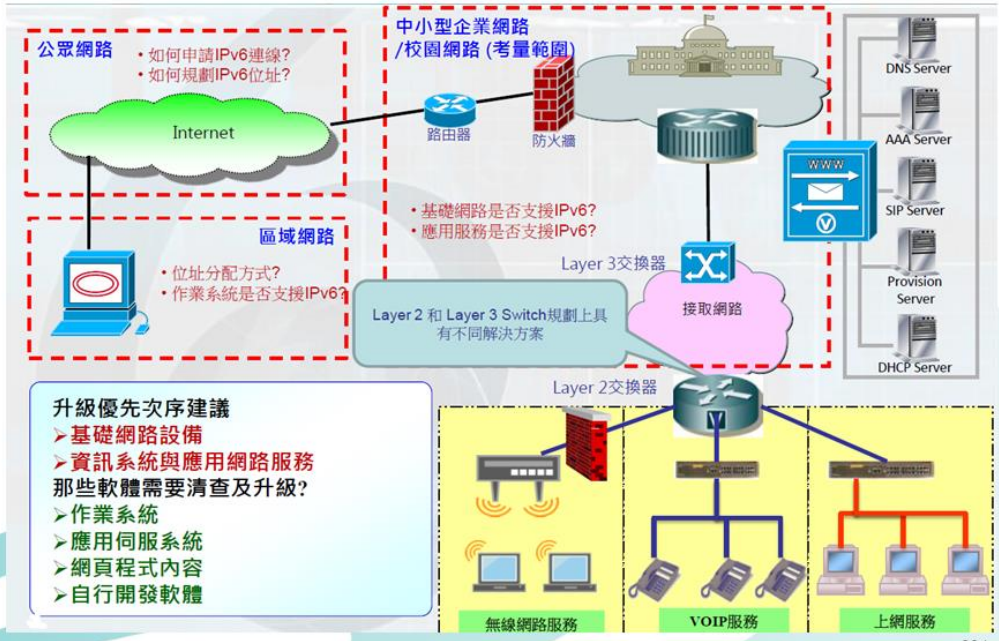
232

點進網域新視界！

IPv4/IPv6雙軌環境下資訊安全檢查項目清單(網路環境、作業系統、網站、資安設備)

233

IPv6網路升級考量



升級優先次序建議
- 基礎網路設備
- 資訊系統與應用網路服務

那些軟體需要清查及升級?
- 作業系統
- 應用伺服系統
- 網頁程式內容
- 自行開發軟體

234

升級作業考量 升級經費與人力評估

- 升級目標：
  - –IPv6升級非一蹴可幾
  - –降低導入成本為優先選擇
  - –達到採取無縫隙升級目標
- 評估重點項目：
  - –上級單位或上級主管願意提供多少預算進行升級？
  - –網路管理人員是否有足夠人力支援IPv6升級？
- 成立升級團隊
  - –網路管理人員是否有相關IPv6技術背景？
- 委外訓練：如：搭配購案採買新型網路系統…
- 自辦訓練：如：聘請講師…等

235

升級作業考量 網路架構升級評估

- 升級目標：
  - 以雙協定為升級終極導向
- 評估重點項目：
  - 外部接取網路調查：
- 網路服務供應商(ISP)是否提供IPv6接取方案？
- 上級單位是否提供IPv6接取方案？
  - 內部網路架構調查：
- 釐清現有IPv4網路拓樸圖
- 規劃未來雙堆疊(Dual Stack)網路拓樸圖

236

升級作業考量 網路架構升級評估

- 網路設備IP位址規劃以及如何配置？
- 基礎網路設備調查：
  - 內部傳輸設備：路由器、L3交換器、L2交換器…等是否支援雙協定？
  - 資安防護設備：IDS、IPS、防火牆…等是否支援雙協定？
  - 網路管理設備：流量監控設備及流量報表程式是否支援雙協定？
  - 加值服務設備：VPN Server、Network Storage …等是否支援雙協定？

237

升級作業考量 終端設備升級評估

- 升級目標：
  –從終端使用者之角度來思考

- 評估重點項目：
  - 使用者較常使用那些Internet & Intranet服務？
    EX：DNS, Web Services (eForm)、E-Mail Services…等
  - 清查終端資訊設備是否支援雙協定?
    使用者設備之作業系統支援現況，EX：Windows, Linux…
    資訊系統設備之應用程式，EX：DHCP, FTP, DNS…
  - –是否以採購方式進行IPv6升級方案？
  - 添購新型終端資訊設備以支援雙協定？
  - 添購新版作業系統授權碼以支援雙協定？

238

升級作業考量 維運人員與使用者心態

- 評估重點項目：
  - 網路維運人員心態：
    - 因已熟系IPv4運作與設定拒絕配合
    - 須花費額外時間重新了解新的技術
    - 須花費時間熟悉新設備及設定，如：IPv6配發機制、DNS設定
  - 使用者面對升級心態：
    - 因使用習慣排斥配合升級及修改設定
    - 因額外費用拒絕更換現有軟硬體
    - 因網路順暢度對升級的誤解
  - 宣導政策減緩對未知的恐懼：

239

升級作業考量 維運人員與使用者心態

- 評估重點項目：
  - 網路維運人員心態：
    - 因已熟系IPv4運作與設定拒絕配合
    - 須花費額外時間重新了解新的技術
    - 須花費時間熟悉新設備及設定，如：IPv6配發機制、DNS設定
  - 使用者面對升級心態：
    - 因使用習慣排斥配合升級及修改設定
    - 因額外費用拒絕更換現有軟硬體
    - 因網路順暢度對升級的誤解
  - 宣導政策減緩對未知的恐懼：
    - 教育訓練與講座
    - 提供簡易的升級設定降低技術門檻
    - 誘因式的導入，如：差別化服務..

240

調查升級網路架構

建議升級順序

1. 核心層(Core Layer)：
2. 分配層(Distribution layer)：
3. 接取層(Access Layer)：

241

基礎網路架構分類

核心層(Core Layer)

- 環境：骨幹網路 (Core Network, Backbone)
- 用途：負責運輸大量的網路訊務，並且達到快速與可靠的服務
- 設備：對外ISP連接之路由器，如：ATM Switch, MPLS Switch, Core Router…

242

基礎網路架構分類

分配層(Distribution layer)

- 環境：接取網路(Edge Network)
- 用途：負責做額外判斷網路訊務封包，提供Routing, Network Policy (如：Security, Filter, QoS…等)服務
- 設備：Layer 3 Switch, Firewall…

243

基礎網路架構分類

接取層(Access Layer)

- 環境：DMZ(外部WWW/DNS/E-mail 伺服器)，Server Farm (內部使用伺服器)，辦公室區域網路
- 功能：負責提供可靠的網路接取給終端設備或重要的Content和網路應用服務，提供Switching, Access Control (VLAN Tagging…)
- 設備：Layer 3 Switch(VLAN), Layer 2 Switch(VLAN), Wireless Router, PCs, Servers, Printers…

244

網路設備IPv6升級概念

設備汰換時，必須支援 Dual Stack IPv4/IPv6

- 處理Layer 3以上資訊相關的設備
  - 提供Routing技術，處理IP層封包的設備，如：路由器、第三層交換機(Layer 3 Switch)、防火牆、負載平衡器…等
- 處理Layer 2相關的設備
  - 提供Switching技術，第二層交換機，如：第二層交換機(Layer 2 Switch)
  - 確保可透通IPv6訊務 (包含Multicast與Unicast)

245

調查網路設備現況 (1)

- 網路傳輸設備
  - Switch Hub, Layer 2 Switch、Layer 3 Switch、Router…等
- 網路安全防護設備
  - 防火牆(Firewall, FW)、入侵偵測系統(IDS)、入侵防護系統(IPS) 、新一代防火牆(Network Generation Firewall, NGFW)…

246

調查網路設備現況 (1)

- 應用伺服器
  - DNS、Web、FTP、Proxy、Media、Database…
- 網路管理設備
  - SNMP Manager, Multi Router Traffic Grapher (MRTG)
- 終端設備
  - 個人電腦、筆記型電腦、平板電腦、行動電話…等

247

調查網路設備現況 (2)

清查網路設備IPv6支援程度

- 網路設備廠牌與供應商
- 網路設備廠軟體版本
- 網路設備授權年限
- 網路設備目前CPU乘載量

請注意，若是CPU 已接近滿載設備
建議重新添購新設備支援IPv6

248

調查網路設備現況 (3)

網路設備支援IPv6現況

- 原有網路設備已內建支援IPv6功能，網路管理員僅需執行基本IPv6指令，如：設定、啟動與測試...等步驟，即可升級支援IPv6。
- 原有網路設備未支援IPv6，透過官方所釋放的新版本韌體，進行官方標準更新動作，即可升級支援IPv6。
- 上述情況無法導入IPv6，則建議列入汰換清單，重新採購新型網路設備。
- 網路設備升級負責人

249

https://www.gsnv6.tw/download.html

IPv6內部網路完成升級報告書

IPv6內部網路升級作業規劃書

250

資料來源

- **TWNIC 財團法人台灣網路資訊中心**
- **行政院 NICI 小組網際網路通訊協定升級推動辦公室**

251


Thank You
252

二、 第二場教材


點進網域新視界！
ICP IPv4/IPv6
雙協定網路安全防護
技術人才培訓
教育訓練
曾家偉
20200515


點進網域新視界！
TWNIC
財團法人
台灣網路資訊中心
簡介

- 財團法人台灣網路資訊中心(TWNIC)是一個非營利性之財團法人機構，在交通部電信總局及中華民國電腦學會的共同捐助下，TWNIC於民國88年12月29日完成財團法人設立登記事宜，『財團法人台灣網路資訊中心』正式成立

- 主管機關乃為交通部，民國106年12月22日完成主管機關變更為國家通訊傳播委員會。捐助章程中規定TWNIC為我國國家級網路資訊中心(National Network Information Center)

3

服務宗旨如下：

- 非以營利為目的，以超然中立及互助共享網路資源之精神，提供註冊資訊、目錄與資料庫、推廣等服務。
- 促進、協調全國與國際網際網路(Internet)組織之間交流與合作，並爭取國際網路資源及國際合作之機會。
- 協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換。
- 協助或支援政府辦理各項事務，並推動網路資訊相關公益事務。

4

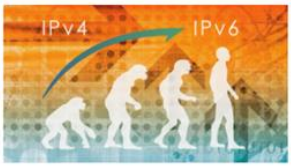
- TWNIC是目前國內唯一統籌網域名稱註冊及IP位址發放之超然中立之非營利性組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。

- 期盼更多人的參與及不斷檢討改進，為我國網際網路事業提供最佳服務，是TWNIC成立為財團法人之最大目的，希望我們團隊能進最大努力，各界也能不斷給予TWNIC更多的支持予鼓勵，使我國網際網路事業能更健全、更快速的發展。

5

域名服務

.tw/台灣10大類型網域名稱，註冊與管理服務。



IP/ASN申請

提供IP位址與AS Number申請，分配與管理服務。

Blog

掌握網路最新發展，政策，技術，趨勢與觀點。

研討會

參與TWNIC年度研討會，認識網路發展趨勢。

教育訓練

參與TWNIC系列教育訓練課程，認識最新網路應用課程。

社會責任

推動符合TWNIC服務宗旨之公益活動，協助推展全國各界網路應用之普及，以建立在地服務的品牌精神。

6


第32屆TWNIC IP
政策資源管理會議
「第32屆TWNIC IP政策資源管理會議」歡迎您踴躍報名參加！
2019-04-30 | 活動訊息
.tw To the World
泰文.tw 邁向域名國際化
泛用型網域名稱新增泰文IDN註冊公告事項
2019-05-17 | 中心公告
韓文.tw
邁向域名國際化
泛用型網域名稱新增韓文IDN註冊公告事項
2019-05-17 | 中心公告
2019 網路治理研習營
「2019 網路治理研習營」開放報名!
2019-05-08 | 活動訊息
「網路社群與數位合作」專家座談會
2019-05-06 | 活動訊息
ICANN APAC-TWNIC
ICANN與TWNIC共同在台北舉辦網路論壇
2019-04-18 | 活動訊息
7


IP/DNS 論壇
IP / DNS 論壇
@IPv6up.tw
首頁
貼文
關於
已說讚
追蹤中
分享
傳送訊息
IP / DNS 論壇
域名之友
@twnicNEWS
首頁
貼文
影片
讚
追蹤
分享
傳送訊息
Marco TeaLand
竹籃裡的山茶園
8

點進網域新視界！

IPv4/IPv6雙軌運作概念介紹

What is IP？

文件資料 → 信封、地址 → 郵政系統

網路資料 → IP 168.95.1.1 2001:CA0:68:A:1:3:3:1:1 → 網際網路

網路位址

IP類似門牌上的地址，能夠明確標示網路裝置的位址資訊

	IPv4	IPv6
發展年份	1981	1999
位址數量	2^{32}（約42億）	2^{128}（地球上每一粒沙都可以得到一個IP）
位址配置	設定缺乏彈性	支援自動配置(隨插即用)
NAT (位址轉換)	需將私有Private IP轉換成公眾Public IP	沒有位址短缺問題，無須位址轉換

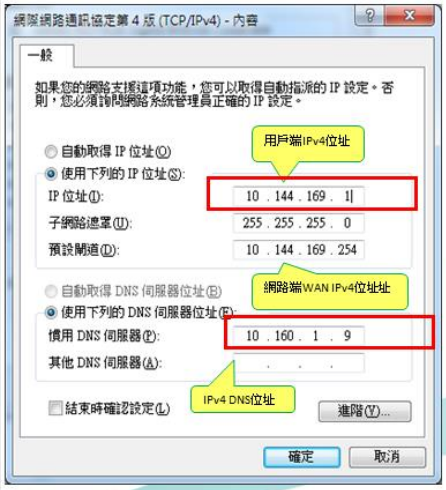
IPv4 Internet — IPv4 NAT — IPv4 — 1

IPv6 Internet — IPv6

IPv4 位址枯竭

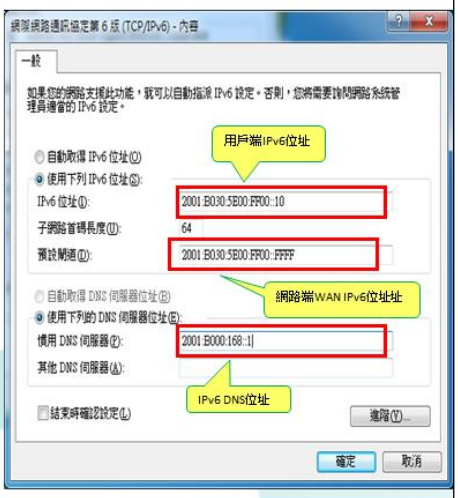
10

用戶主機連接網路的必要條件



用戶連網的條件

- IP位址
- Default GW
- DNS



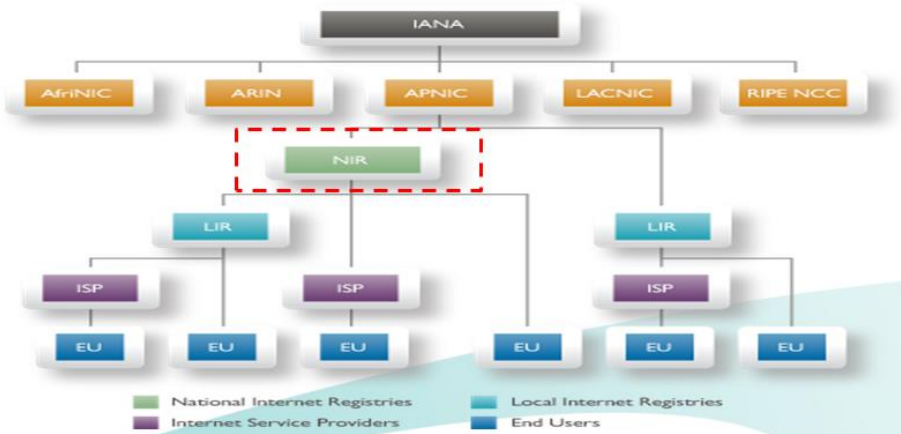



IP位址分配的組織

以紐約的IANA為中心（現委由ICANN管理）
其下再依區域分成五個區域註冊中心(Regional Internet Registries)

歐洲地區：RIPE NCC
　　Réseaux IP Européens Network Coordination Centre
北美地區：ARIN
　　American Registry for Internet Numbers
亞太地區：APNIC
　　Asia Pacific Network Information Centre
拉丁美洲：LACNIC
　　Latin American and Caribbean Internet Addresses Registry
非洲: AfriNIC
　　Africa Network Information Centre

IP位址指派機構



以亞太地區來說，RIR 可透過 NIR (National Internet Registry) 將資源發放給LIR (Local Internet Registry，一般皆為ISP) ，LIR 再將資源指定分發給其客戶。如此階層式的組織不但使得資源分配及管理更有效率，也可避免資源過度集中，避免不公平的資源分配

13

主要國家IPv4位址配發狀況

資料來源：*https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation*

Rank	Country or entity	IP addresses[3]	%	Population (mostly 2012)[4]	IP addresses per 1000
	World	4,294,967,296	100.0	7,021,836,029	611.66
1	United States	1,541,605,760	35.9	313,847,465	4,911.96
	Bogons	875,310,464	20.4		
2	China	330,321,408	7.7	1,343,239,923	245.91
3	Japan	202,183,168	4.7	127,368,088	1,587.39
4	United Kingdom	123,500,144	2.9	63,047,162	1,958.85
5	Germany	118,132,104	2.8	81,305,856	1,452.93
6	Korea, South	112,239,104	2.6	48,860,500	2,297.13
7	France	95,078,032	2.2	65,630,692	1,448.68
8	Canada	79,989,760	1.9	34,300,083	2,332.06
9	Italy	50,999,712	1.2	61,261,254	832.50
10	Brazil	48,572,160	1.1	205,716,890	236.11
11	Australia	47,573,248	1.1	22,015,576	2,160.89
12	Netherlands	46,379,784	1.1	16,730,632	2,772.15
13	Russia	42,762,784	1.0	138,082,178	309.69
14	Taiwan	35,383,040	0.8	23,113,901	1,530.81
15	India	34,685,952	0.8	1,205,073,612	28.78
16	Sweden	30,373,544	0.7	9,103,788	3,336.36
17	Spain	28,421,760	0.7	47,042,984	604.17
18	Mexico	25,862,912	0.6	114,975,406	224.94
19	Switzerland	20,872,696	0.5	7,655,628	2,726.45
20	South Africa	20,386,560	0.5	48,810,427	417.67

- 美國雖擁有接近全球半數之已配發IPv4位址數量，但也是目前推動IPv6最積極的國家
  - 其所分配到的IPv4位址空間並非全數分配到終端用戶
  - 每人平均分配到的IPv4位址仍不足以滿足用戶基本連網需求（例如手機、平板、 電腦以及相關穿戴式裝置）
- 中、印、俄和巴西人口眾多，但IP數/人小於1

IPv4 位址的分配類別

類 別	網 路 位 址	主機位址	最 多 主 機 數 量	可 分 配 的 組 織 數
A	8位元	24位元	16,777, 214	128
B	16位元	16位元	65,534	16,384
C	24位元	8位元	254	2,097,152

IPv4技術本身的缺陷

- 數目限制：
  - IPv4的網路位址只有32位元
  - 採用Class的方式劃分區域較缺乏彈性
- 效能問題：
  - 新興應用所需要的「QoS」服務，在IPv4上面實做極為困難。
  - CIDR的出現導致網路管理上的困難。
- 安全問題：
  - IPv4無法在基本的網路層提供安全的加密通訊
- 組態設定：
  - DHCP伺服器安裝設定不易，而且維持運作要花不少人力物力
  - 全自動化的組態設定

IPv4不只無法支應快速成長的為址需求，它的缺點是無法支援網路安全及國際漫遊的能力，還有IPv4需要利用網路位址翻譯器(Network Address Translator；NAT)，對經營者而言，它就增加了成本及管理上的負擔

16

NAT設備運作限制

- 無法雙向點對點連結
  - NAT環境只允許終端設備主動單向對外存取，無法滿足未來M2M雙向通訊應用的需求
  - Ex. 定位協尋/犯罪偵查/安全監理不易，NAT設備後端之裝置不易識別身分
- Port限制
  - 一個IP位址的port數上限是65536可使用，當NAT進行虛擬/實體IP轉換必須考量port是否足夠
  - Ex. 連線品質與效率受影響，當連線數被佔滿時，可能瀏覽網頁常常出現無法顯示網頁的情形發生
- 網路管理變複雜
  - IP網路的透通性與擴充性受到NAT的限制，增加網路管理的複雜度
  - Ex. 但當該組織必須合併多個區域網路時，必須仔細的重新規劃IP分配，否則很容易產生IP重覆的情形

17

因應措施	開源(回收、移轉)	節流(使用NAT)	部署IPv6
優勢 (Strengths)	無技術門檻與實施費用	屬於成熟技術，可節省IP位址的使用	• 擁有大量的位址，可根本解決位址不足問題 • 提升路由效率，內建QoS及IPSec等功能
劣勢 (Weaknesses)	• 無確實可行的方法(回收或移轉均無好的實行經驗)，也不具強制性 • APNIC曾嘗試執行一端時間，但效果不彰	• NAT對一些應用的連線數有限制、每一個使用者需要的連線數快速增加，SP須不斷擴建方能滿足需求 • NAT 增加服務提供成本(e.g. 設備費用、位址轉換時間…)亦不利未來多媒體應用的大頻寬需求 • NAT技術將使得網路拓樸僵化無彈性，不利未來新網路技術，如SDN，的發展	• 若採取短時間內大量佈署方式，會造成設備更新成本大福增加 • SP網路與服務各級工作同仁對於IPv6技術的掌握度尚有許多成長空間
機會 (Opportunities)	• 有部分IPv4位址(約有50個/8未出現在BGP routing table中)	**面對IP位址不足的事實但網路與服務尚未準備所妥善時，短期可採行的緩衝因應措施**	**• 相關RFC超過400篇，技術齊備，終端/網路設備/O.S.均已支援** **• 唯一可長可久而能永續發展的解決方案**
威脅 (Threats)	• 合法擁有的IP位址要回收不容易，也不具強制性 • IPv6相關技術與設備發展已成熟	非長期解決方案，對於大量使用者與視訊訊務、SP須不斷擴建N設備，大幅增加成本與減損網路拓樸彈性	IPv6屬於重要網路基礎建設，但沒有亮眼的獲利模式，讓許多公司採觀望態度

18

IP網路發展未來趨勢

More users ✚ More devices ✚ More applications

- 上網的裝置日益增多
  - Smart Phone、PAD、穿戴式終端
- 需求更貼近生活之智慧服務
  - 用戶導向的服務
  - 行動上網、IoT、IoE 、Cloud

19

Why IPv6 a must?

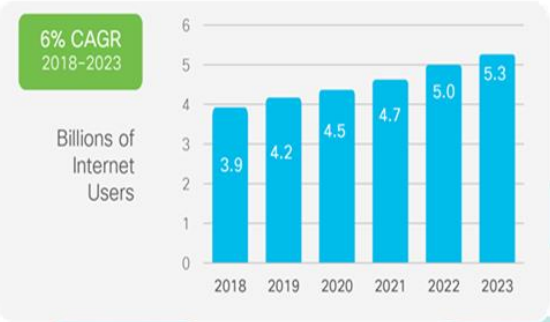
- IPv4位址已耗盡，IPv6是滿足網路永續發展的終極方案
  - 網際網路仍蓬勃發展，NAT做法凸顯IPv4位址不足與網路彈性不足的事實
  - 可確保既有與新興電信網路與應用服務永續發展而可長久的網路基礎
- 行動寬網及應用快速發展，IPv4位址供需嚴重失衡
  - 4G LTE與行動寬頻應用將帶動IP位址需求大幅成長
  - 終端設備支援能力IPv6 Ready，Apple iOS 9預設啟動IPv6
  - 全球IPv6 Enabled network的比例已接近40%
- 符合國際趨勢與政府發展政策，促進產業升級再造
  - 主要領導業者如Verizon、AT&T、DT 、Comcast均啟動全面導入IPv6的策略
  - 相關新興國家，如羅馬尼亞等，亦均積極導入IPv6 ，成長率快速上升
  - 行政院網際網路通訊協定升級推動方案，優先推動 IPv6 網路升級計畫

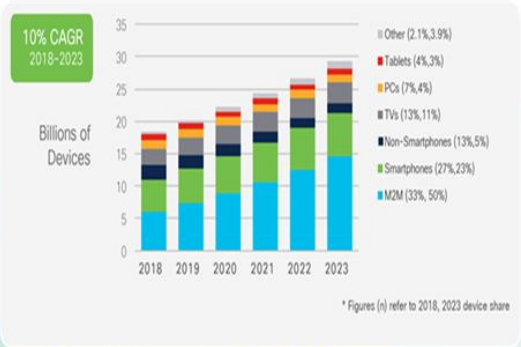
順勢導入 IPv6，以最低成本導入模式，維持既有服務並強化競爭優勢，掌握未來網路永續發展的契機

20

IPv6的必要性(1/2)

- IP是網路的門牌號碼，是網路通訊不可或缺的條件
  - IPv4數量為2^{32}約43億個，IPv6數量為2^{128}約為340澗的IP位址空間可讓世界上每一台連網裝置、都能得到IP位址
- IPv4位址已用罄，解決端對端通訊網路技術問題





IoT聯網裝置快速成長，引進IPv6是必然趨勢!

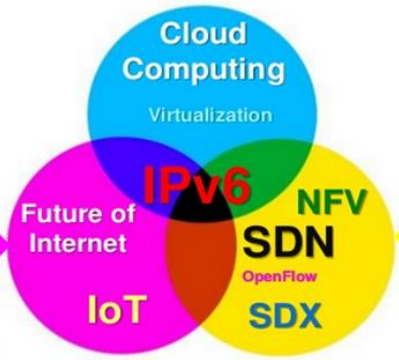
https://techblog.comsoc.org/2020/02/20/ciscos-annual-internet-report-2018-2023-forecasts-huge-growth-for-iot-and-m2m-tepid-growth-for-mobile/

21

IPv6的必要性(2/2)

- 更高的網路安全機制(IPSec)
- 強化雲端服務維運管理與佈署彈性

- 充裕的位址滿足無所不IoT連網需求
- Public IP又利於系統整合跨網互聯
- 提昇路由效能

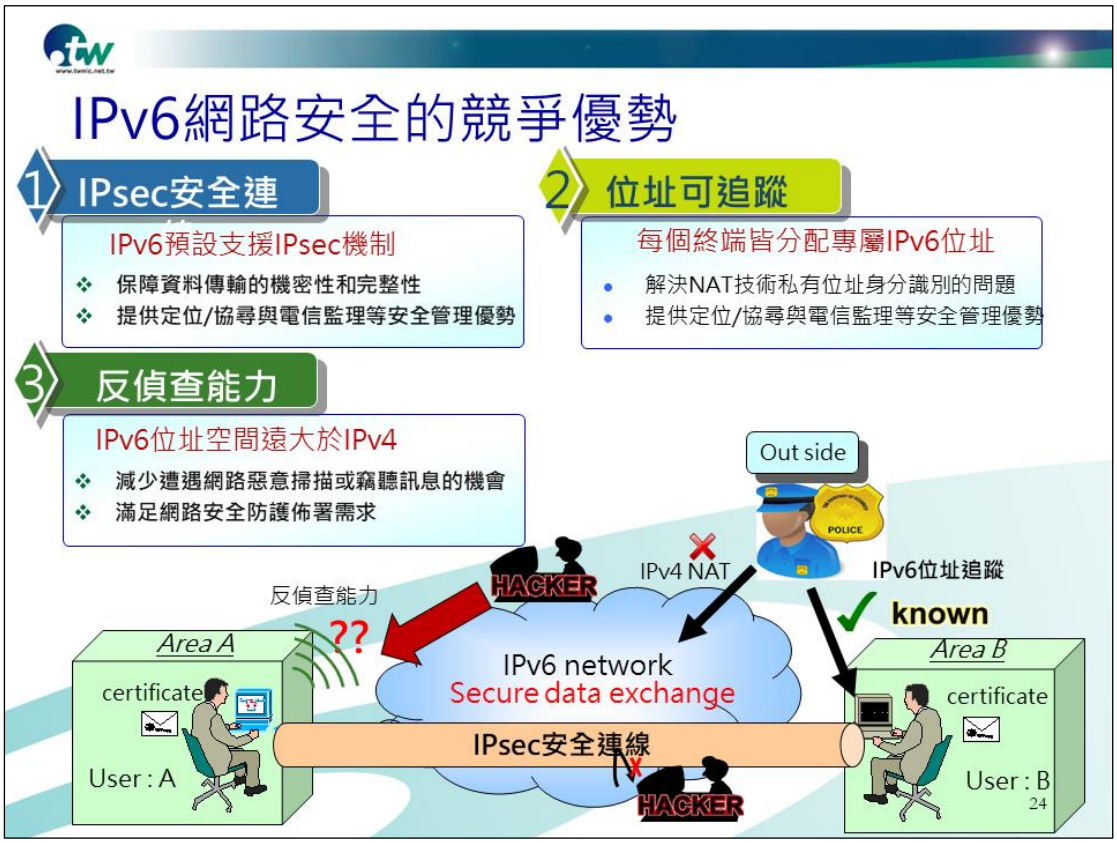


- 更優質服務品質管控機制
- 滿足網路服務終端裝置識別與通訊需求

引進IPv6符合網路虛擬化、可程式化技術演進及雲端化物聯網服務需求

22


IPv6具備之優勢
商業需求
•增加維運效率
•提高安全度
•支援移動性
•符合未來成長需求
•成本低廉
IPv6
五大特點
•需求導向
•任意接取
•位置無關
•快速靈活
•品質服務
高擴充性
沒有NAT
高移動性
高安全性
隨時隨地永遠連線
方便實現
IPv6的優點不止具備很多位址空間，最重要的是如何指派這麼多位址，符合客戶需求
23


IPv6網路安全的競爭優勢
1 IPsec安全連
IPv6預設支援IPsec機制
保障資料傳輸的機密性和完整性
提供定位/協尋與電信監理等安全管理優勢
2 位址可追蹤
每個終端皆分配專屬IPv6位址
解決NAT技術私有位址身分識別的問題
提供定位/協尋與電信監理等安全管理優勢
3 反偵查能力
IPv6位址空間遠大於IPv4
減少遭遇網路惡意掃描或竊聽訊息的機會
滿足網路安全防護佈署需求
Out side
POLICE
IPv4 NAT
IPv6位址追蹤
known
HACKER
反偵查能力
??
Area A
certificate
User : A
IPv6 network
Secure data exchange
IPsec安全連線
HACKER
Area B
certificate
User : B
24

IPv6對物聯網發展的優勢

- IPv6本身的優點
  - 統一的通訊方式
  - 開放標準
  - IPv6位址空間大(2^128)
  - 徹底解決IPv4位址枯竭
  - 自動定址
  - 隨插即用
  - 高擴充性
  - 路由效率較佳

- IPv6 IOT的特性與優勢
  - **訊息一致性：**物聯網與網際網路採用相同協定，可與網際網路接軌更為順暢
  - **跨平台溝通：**採用相同協定，使不同廠牌、不同公司開發之設備可溝通訊
  - **便於管理軟體(APP)開發：**針對標準開發彈性化管理軟體，簡化管理複雜度。
  - **適用於多種實體網路**(power line, 802.15.4,bluetooth,...)技術
  - 相關公開標準(IETF,4G LTE)與業界標準(ZigBee,Bluetooth)**均已採用IPv6**
  - 可**同時滿足**行動上網、雲端運算、萬物聯網之**大量位址需求**

IPv6、LTE、Cloud、Big Data
萬物聯網 (IoE)

25

IPv6可引領電信IT化與行動IoT業務創新

IPv6能滿足5G IoT大量裝端同時連網以及即時通訊的需求

位址空間

裝置識別

M2M通訊

隨差即用

- 提供異質網路共通傳輸介面
- 提供IoT裝置的識別與配置
- 避免NAT技術影響傳輸效能

M2M通訊

- 50~500B的裝置
- 1ms的延遲
- 10Gbit的傳輸率

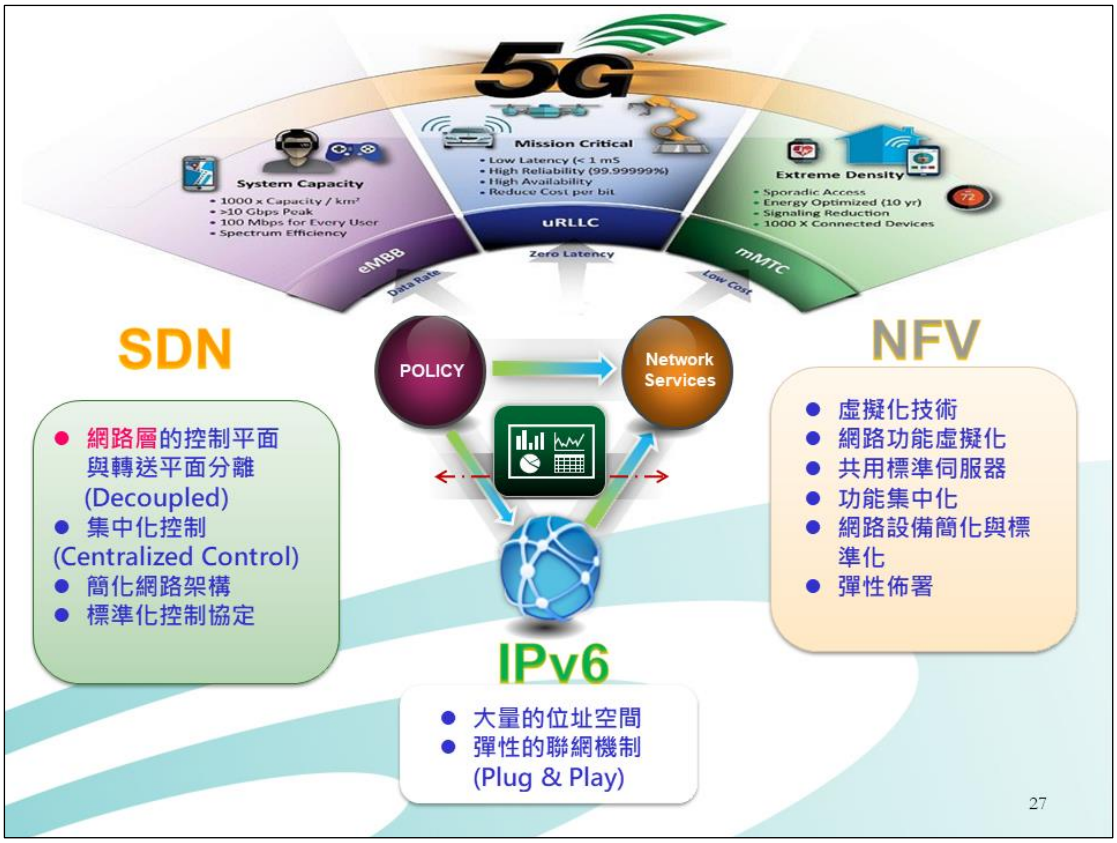
4G LTE　Wi-Fi

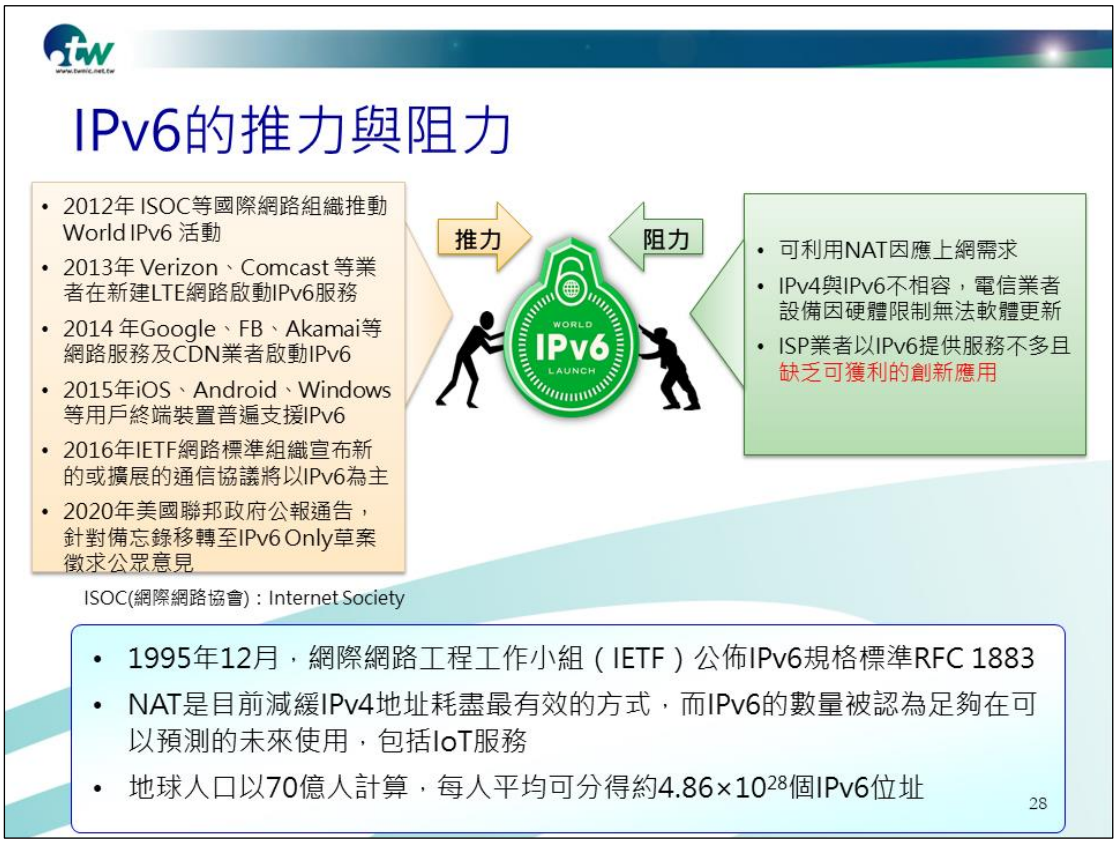
車聯網/自駕車

智慧城市

工業4.0 自動化控制

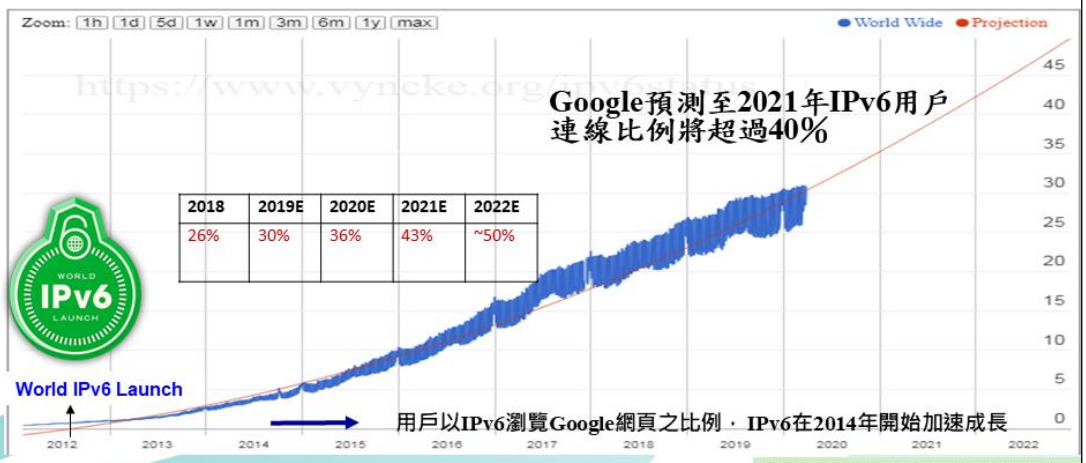
26


5G
System Capacity
• 1000 x Capacity / km²
• >10 Gbps Peak
• 100 Mbps for Every User
• Spectrum Efficiency
Mission Critical
• Low Latency (< 1 mS
• High Reliability (99.99999%)
• High Availability
• Reduce Cost per bit
Extreme Density
• Sporadic Access
• Energy Optimized (10 yr)
• Signaling Reduction
• 1000 X Connected Devices
eMBB
Data Rate
uRLLC
Zero Latency
mMTC
Low Cost
SDN
● 網路層的控制平面與轉送平面分離 (Decoupled)
● 集中化控制 (Centralized Control)
● 簡化網路架構
● 標準化控制協定
POLICY
Network Services
NFV
● 虛擬化技術
● 網路功能虛擬化
● 共用標準伺服器
● 功能集中化
● 網路設備簡化與標準化
● 彈性佈署
IPv6
● 大量的位址空間
● 彈性的聯網機制 (Plug & Play)
27


IPv6的推力與阻力
• 2012年 ISOC等國際網路組織推動World IPv6 活動
• 2013年 Verizon、Comcast 等業者在新建LTE網路啟動IPv6服務
• 2014 年Google、FB、Akamai等網路服務及CDN業者啟動IPv6
• 2015年iOS、Android、Windows等用戶終端裝置普遍支援IPv6
• 2016年IETF網路標準組織宣布新的或擴展的通信協議將以IPv6為主
• 2020年美國聯邦政府公報通告，針對備忘錄移轉至IPv6 Only草案徵求公眾意見
推力
阻力
WORLD IPv6 LAUNCH
• 可利用NAT因應上網需求
• IPv4與IPv6不相容，電信業者設備因硬體限制無法軟體更新
• ISP業者以IPv6提供服務不多且缺乏可獲利的創新應用
ISOC(網際網路協會)：Internet Society
• 1995年12月，網際網路工程工作小組（IETF）公佈IPv6規格標準RFC 1883
• NAT是目前減緩IPv4地址耗盡最有效的方式，而IPv6的數量被認為足夠在可以預測的未來使用，包括IoT服務
• 地球人口以70億人計算，每人平均可分得約4.86×10²⁸個IPv6位址
28

IPv6逐漸普及且訊務快速成長

- Google統計資訊顯示，現約30.9%的連網用戶使用IPv6
- 5G IoT大量終端以及M2M通訊的需求將加速IPv6成長



Source :https://www.vyncke.org/ipv6status/

29

IPv6發展現況

- 主要國家連線Google使用IPv6的比例
  - 比利時(57.08%) 名第一，德國(49.43%)排第二，希臘(47.66%)排第三

Google IPv6 Country Rank

Per-country ranking table based on data from Google IPv6 Statistics page.

#	Country	Adoption
1	Belgium	57.08%
2	Germany	49.43%
3	Greece	47.66%
4	Malaysia	47.2%
5	French Guiana	46.84%
6	Mayotte	44.31%
7	India	43.71%
8	Vietnam	43.56%
9	France	42.99%
10	Uruguay	42.62%
11	Switzerland	42.39%
12	United States	42.26%
13	Luxembourg	41.83%
14	Portugal	40.43%
15	Taiwan	38.3%

Source:https://www.aelius.com/njh/google-ipv6/

30

IPv6發展現況

- 依據 World IPv6 Launch Measurements的統計，全球各大電信營運商都在積極推動IPv6網路基礎設施改造
  - 印度Reliance JIO (87.76%)、美國T-Mobile USA (94.58%)、Verizon Wireless (85.62%)、Comcast (69.95%)、AT&T (61.31%)；法國Free (85.71%)；德國DT (70.43%)；日本KDDI (61.88%)

Show 10 entries Search:

Rank	Participating Network	ASN(s)	IPv6 deployment
1	Comcast	7015, 7016, 7725, 7922, 11025, 13367, 13385, 20214, 21508, 22258, 22909, 33287, 33489, 33490, 33491, 33650, 33651, 33652, 33653, 33654, 33655, 33656, 33657, 33659, 33660, 33661, 33662, 33664, 33665, 33666, 33667, 33668, 36732, 36733	73.98%
2	RELIANCE JIO INFOCOMM LTD	55836, 64049	87.76%
3	Charter Communications	7843, 10796, 11351, 11426, 11427, 12271, 20001, 20115, 33363	53.54%
4	Combined US Mobile Carriers	3651, 6167, 10507, 20057, 21928, 22394	85.36%
5	ATT	6389, 7018, 7132	61.31%
6	Deutsche Telekom AG	3320	70.43%
7	Claro Brasil	4230, 28573	58.83%
8	Orange Business Services	3215	63.84%
9	Cox Communications	22773	61.08%
10	British Sky Broadcasting	5607	87.97%

31

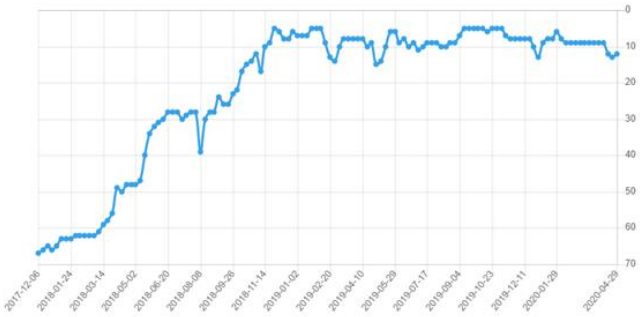
Source :https://www.worldipv6launch.org/measurements/

IPv6發展現況

台灣 IPv6

台灣全球排名：第12名

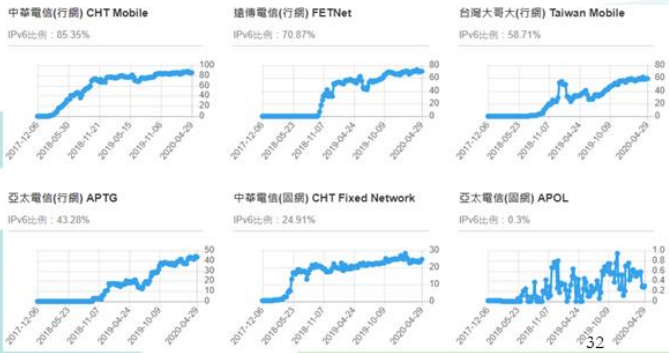
(IPv6比例: 42.43%)



台灣六大電信業者

① 4G LTE與VoLTE屬於新建網路，導入IPv6包袱較少

② 固網CPE設備支援IPv6程度不一，設備汰舊換新的過程複雜且費時



32

Source :https://ipv6now.twnic.net.tw/ipv6/index.html

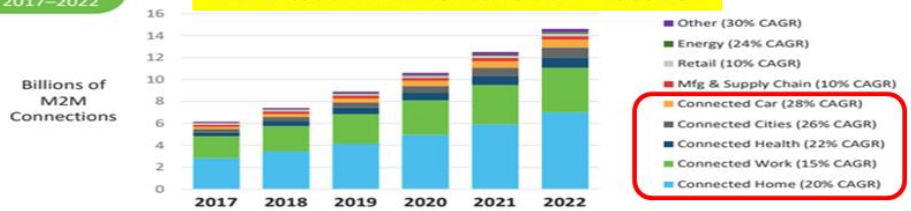
IPv6未來預測

Global M2M Connections / IoT Growth by Vertical

By 2022, connected home largest, connected car fastest growth

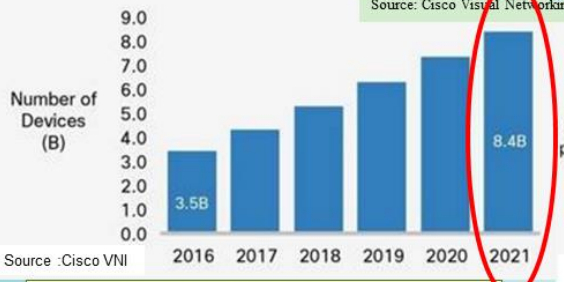
19% CAGR 2017–2022

IoT聯網裝置快速成長將帶動IPv6的需求



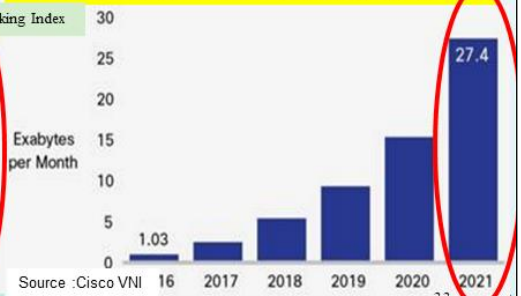
IPv6能滿足5G IoT大量終端同時連網以及M2M通訊的需求

Source: Cisco Visual Networking Index



Source :Cisco VNI

Global IPv6 -Capable Mobile Devices



Source :Cisco VNI

IPv6 Mobile Data Traffic Forecast 2016–2021

33

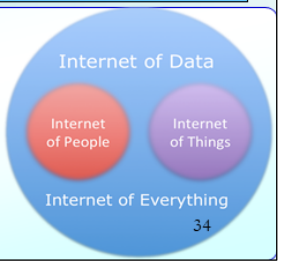
導入IPv6的差異

現在	未來
• IPv4對於ISP的發展限制 ▫ IP配置策略與位址需求 ▪ 固定制與非固定制IP配置模式 ▪ 4G+VoLTE每個終端至少需兩個IP ▫ 網路安全與路由效率 ▪ IPv4的安全管控機制不足 ▪ IPv4零散區塊影響路由傳輸效能 • NAT機制的發展瓶頸 ▫ 存在透通性與擴充性的問題 ▫ IP位址定位與終端識別複雜化 ▫ M2M的通訊應用發展受限 ▫ 持續採購NAT設備的投資成本	❖ 導入IPv6具備的技術優勢 ▪ 簡化表頭、封包設置優先序、改善路由效能 ▪ 預設IPsec網路安全機制 ▪ 突破NAT機制的發展瓶頸 ❖ 採取IPv6/IPv4 雙協定方式導入IPv6 ▪ 維持業者既有服務得以延續 ▪ 建立未來發展創新服務的基礎 ❖ 以IPv6作為新興應用通訊的基礎 ❖ 跨平台溝通：採用相同協定，使不同廠牌、不同公司開發之設備可溝通訊 ❖ 訊息一致性：物聯網與網際網路採用相同協定，可與網際網路接軌更為順暢

必要性

❖ 觀察IPv6國際發展趨勢，全球IPv6發展已逐步進入成長期；從啟動導入到真正提供商用網路服務，平均至少需3~4年時間！須及早因應！

❖ 無論IoT、SDN或雲端服務，IP位址皆為不可或缺的關鍵基礎，引進IPv6能確保維持既有服務與發展未來以IP為基礎的創新應用服務，掌握新一代網路創新研發商機



34

IPv6未來關鍵挑戰

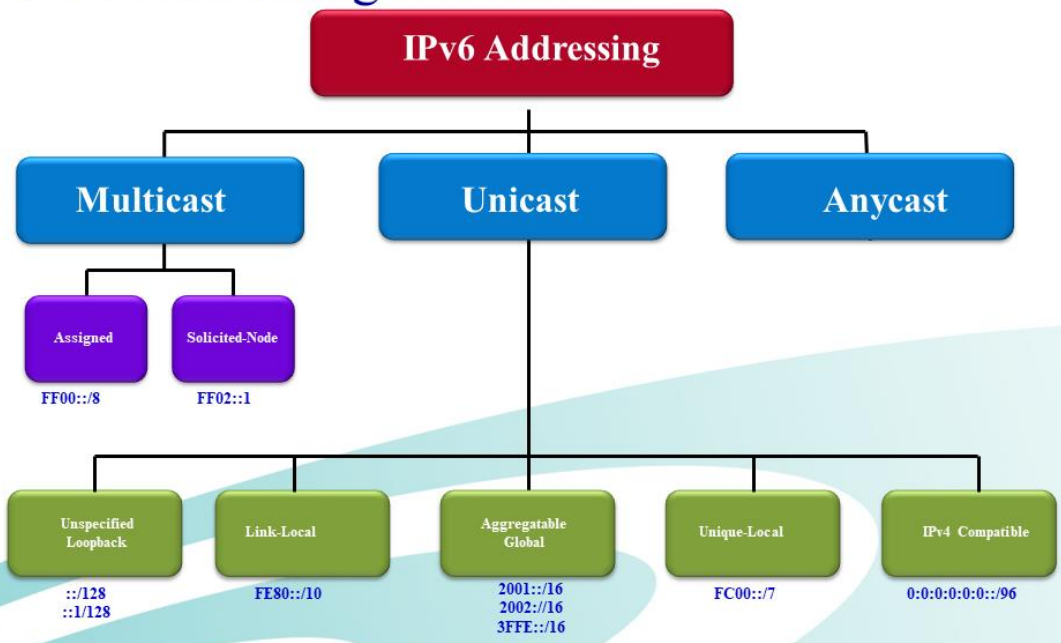
- IPv6網路連線品質仍須持續優化
  - IPv6涵蓋率不如IPv4可能影響服務品質與用戶體驗，因此IPv6網路連線與轉發路由等相關配置仍需要持續優化改善
  - IPv6可避免NAT的缺點，是未來網路通訊協定的主流
- CDN內容以及Cloud雲端平台發展緩慢，影響IPv6服務效率與品質
  - 企業推動IPv6易受限於第三方業者雲服務平台的IPv6能力不足，形成瓶頸
  - 須持續提升IPv6網路連線品質以及加強IPv6服務涵蓋範圍
- 網站和應用支援IPv6比例偏低，無法有效提升IPv6用戶規模和流量
  - 部分網站及應用的首頁已宣稱可支援IPv6/IPv4雙協定，但其支援IPv6的程度大多仍只侷限於IPv6首頁
  - IPv6的用戶規模和網路流量仍有相當大的成長空間
- 固定終端支援IPv6的情況不佳，影響IPv6端到端通訊部署
  - 固網CPE設備支援IPv6程度不一，且固網CPE設備汰舊換新的過程複雜且費時
- IPv6安全風險開始浮現，挑戰IPv6網路防護能力
  - IPv6攻擊案例逐漸增加，攻擊範圍也越來越廣泛
  - IPv6安全漏洞對系統 / 應用等各方面影響

35

點進網域新視界！

IPv6位址架構與格式

IPv6 Addressing Architecture



37

IPv6 位址的表示法（1/3）

- IPv6 位址長達128 bits，若是用2 進位表示， 一連串的1和0 保證讓人看了昏頭。若是也採用IPv4 的表示法，不但容易造成混淆，而且也還是很長。
- 最後大家終於達成共識，在表示IPv6 位址時，將它區分為8 段（Segment），每段由16 bits 組成，彼此以冒號（：）隔開，例如：

總共有8段

WXYZ: WXYZ: WXYZ: WXYZ: WXYZ: WXYZ: WXYZ: WXYZ

每段長度為16bits

- 其中的W 、X 、Y 和Z 都是代表16 進位數字, 也就是0 ~ F, 以下就是一些合法的IPv6 位址範例：

38

IPv6 位址的表示法（2/3）

- 2001：5E0D：309A：FFC6：24A0：0000：0ACD：729D
- ABCD：0000：0000：0000：0000：0000：0000：5A4D
- DABC：0020：0001：0008：0000：0000：0000：000D

- 但是這麼長的一串數字，甭說背起來，光是唸也很繞口。為了方便書寫， 對於開頭的0 可以簡化， 例如：0C12 簡化為C12、000A 簡化為A
- 如果W、X、Y、Z 都是0, 這整段16 bits 就可以省略不寫, 例如：

ABCD：0000：0000：0000：0000：0000：0000：5A4D簡寫為ABCD::5A4D
DABC：0020：0001：0008：0000：0000：0000：000D簡寫為DABC:20:1:8::D

- 上列的『::』（雙冒號）表示其中包含連續、數量不固定的0，也正因為如此, 如果出現兩個『::』， 就會讓人搞不清楚實際代表的IPv6 位址，例如：1234::5678::ABCD 可能是1234:0:0:5678:0:0:0:ABCD 或1234:0:0:0:0:5678:0:ABCD。因此在IPv6 規格中明訂，對於一個IPv6 位址, 這種雙冒號簡寫方式只能出現一次

39

IPv6 位址的表示法（3/3）

- 另一種常見的IPv6 位址表示法是『IPv6 位址/首碼長度』, 亦即在IPv6位址之後加上『/ 首碼長度』, 例如：

2001:0:0:B3::1234/64

IPv6位址 　　 **首碼長度**

- 首碼長度視位址的類型（Type）而定。IPv6 位址區分為Unicast、Multicast 和Anycast 3 種類型。

40

練習

- **2001 :0000 :0000 :CD30 :0000 :0000 :0000 :0000 / 64**
  - 2001 : :CD30 :0000 :0000 :0000 :0000 / 64
  - 2001 :0 :0 :CD30 :0 :0 :0 :0 / 64
  - 2001 :0 :0 :CD30 : : / 64
  - 2001 :0 :0 :CD30 : :0 / 64
  - **2001 : : CD30 : : /64**
  - **2001 :0 :0 :CD30 / 64**
  - **2001 :0 :0 :CD3 / 64**
  - **2001 : :CD30 / 64**
  - **2001 : :CD3 / 64**

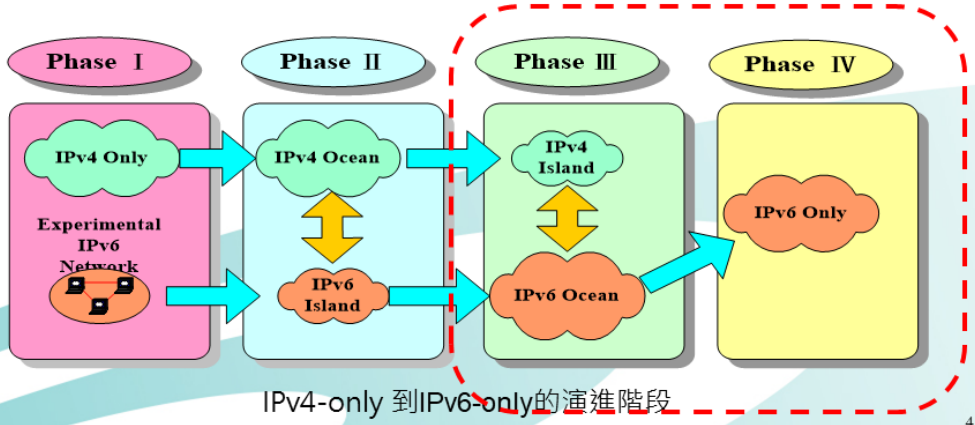
41

點進網域新視界！

IPv4/IPv6雙軌環境建置概述

IPv6網路演進部署

- 兼顧實務、保障品質、降低成本、網路演進是IPv6網路部署的四大基本原則
  - 不影響既有IPv4服務正常運作
  - 兼容既有設備，不強制用戶升級或更換設備
  - 網路基礎服務優先IPv6升級

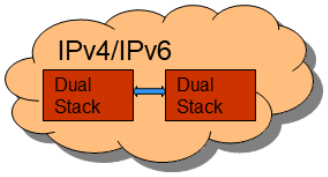


43

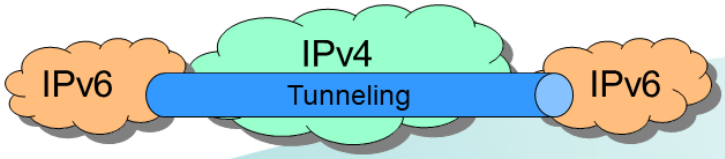
基礎IPv6轉移機制

Transition Mechanism (轉移機制)

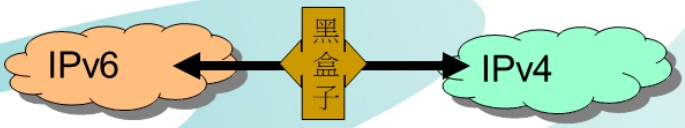
- **Dual Stack(雙協定化)**
  - 所有網路設備都具備IPv4和IPv6能力



- **Tunneling(穿隧技術)**
  - 網路邊緣或端點設備經由不相容網路連接之技術

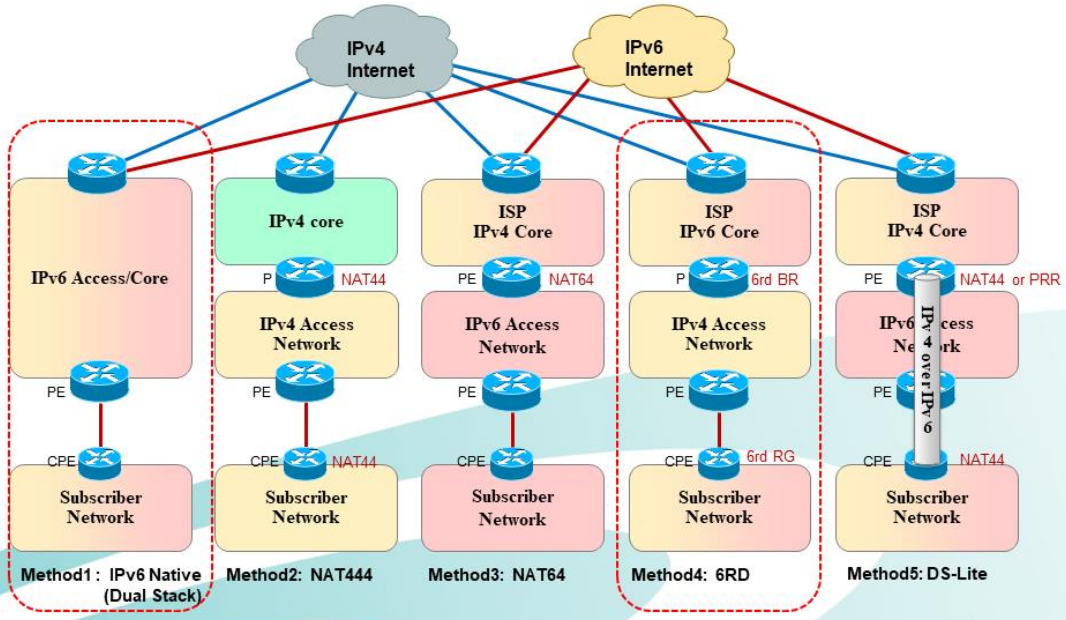


- **Translation(轉換機制)**
  - 具備只支援IPv6設備和只支援IPv4設備互相通信能力



44

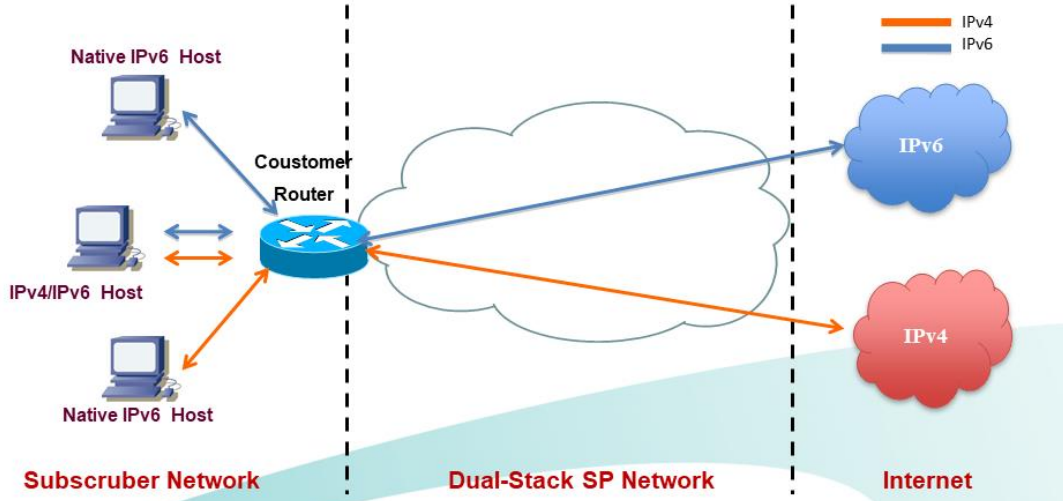
IPv4 and IPv6 共存機制



Source：www.cisco.com

45

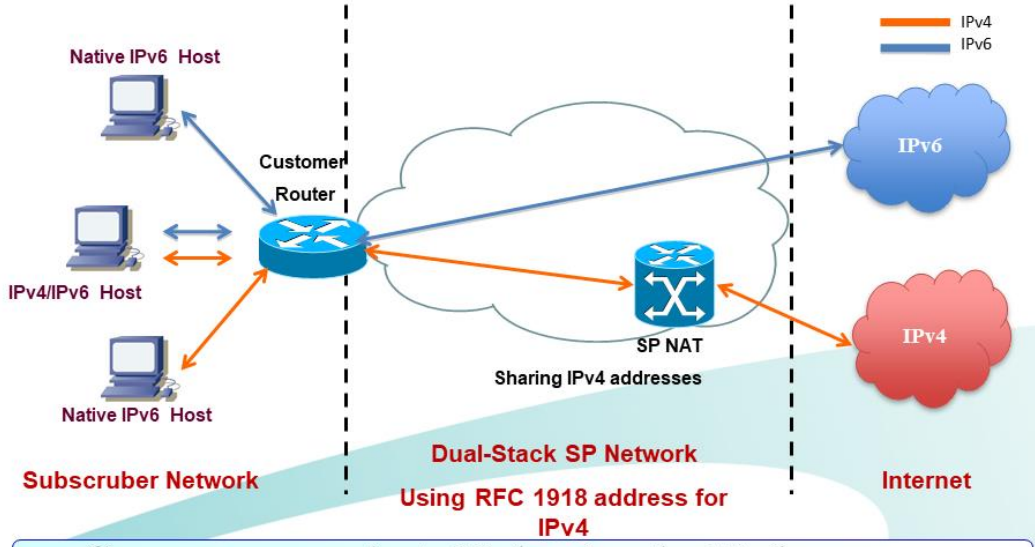
Dual Stack Network



- **The original transition scenario, but dependent on:**
  - **IPv6 being available all the way to the customer**
  - **Sufficient IPv4 address space for the customer**

46

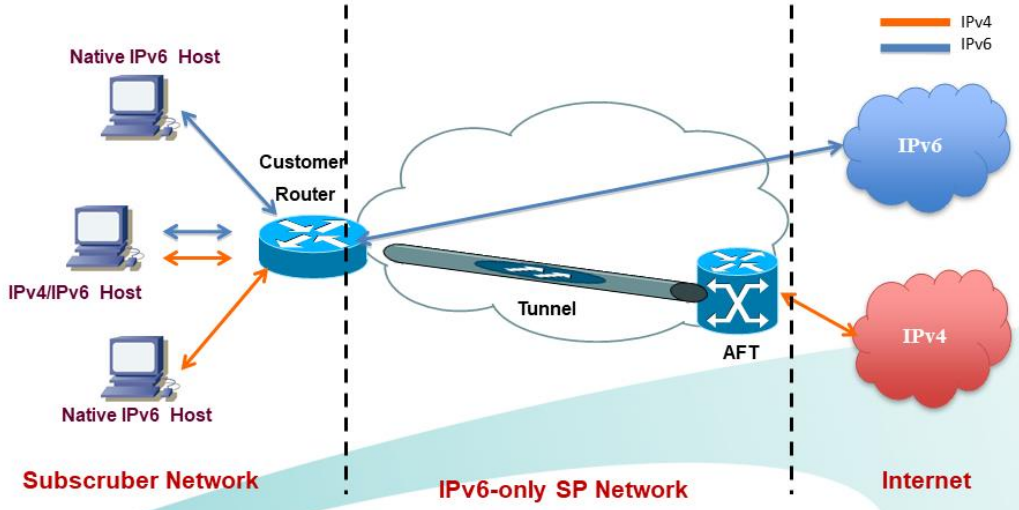
NAT444/SP NAT



- Consumer uses private IPv4 and native IPv6
- SP uses private IPv4 and native IPv6 for backbone
- Carrier-Grade NAT (RFC 6264)

47

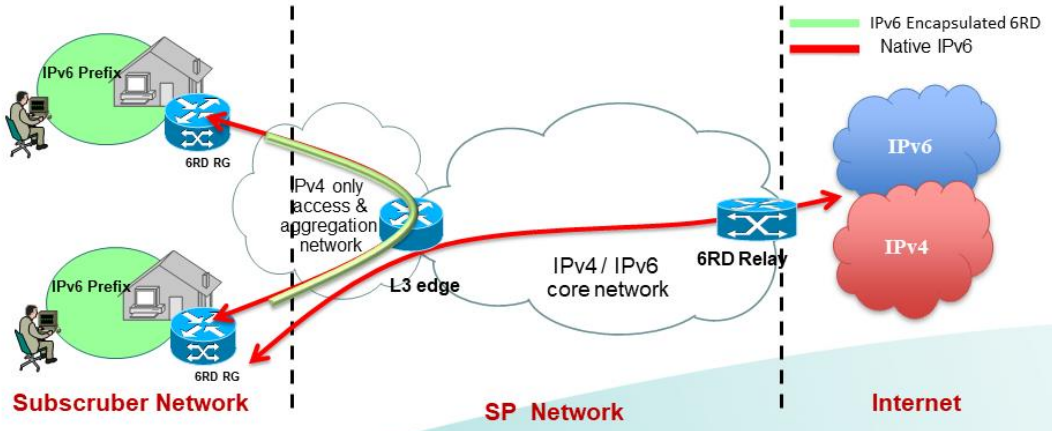
Dual Stack Lite



- SP has IPv6 only infrastructure
- For consumer, IPv4 tunnel to SP NAT, IPv6 native
- Carrier-Grade NAT (RFC 6264)

48

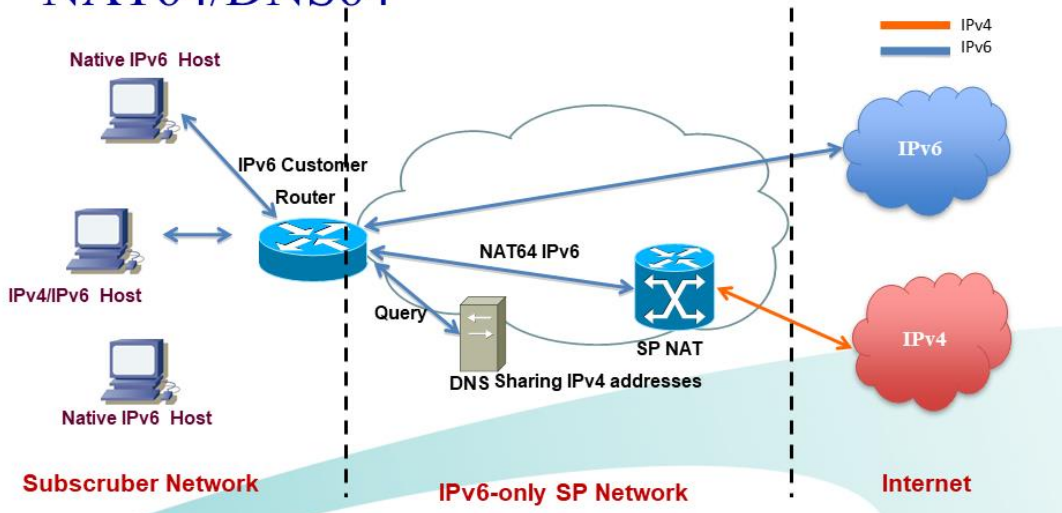
6RD



- IPv6 service in the home is essentially identical to native IPv6 service
- IPv6 Packets Follow IPv4 routing
- 6rd Border Relay traversed only when exiting or entering a 6rd Domain
- 6rd Border Relays are fully stateless, no limit on "number of subscribers" supported
- Border Relays may be placed in multiple locations, addressed via anycast.

49

NAT64/DNS64



- Consumer uses only IPv6 plus Protocol Translation to reach IPv4
- Service Provider uses only IPv6
- Carrier-Grade NAT (RFC 6264)
- Stateful NAT64 (RFC 6146)

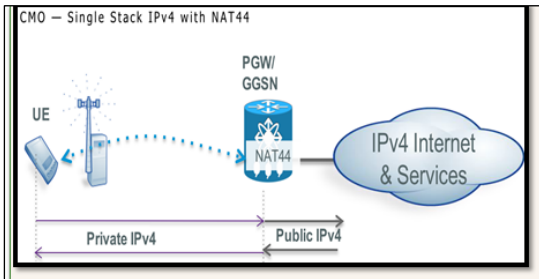
50

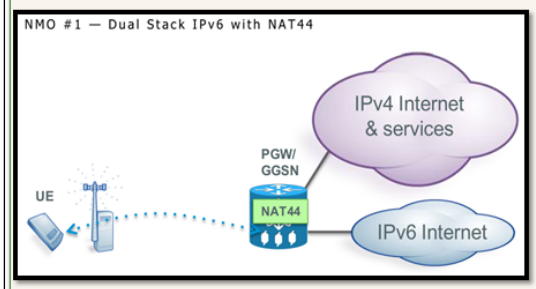
IPv4/IPv6網路共存技術發展現況

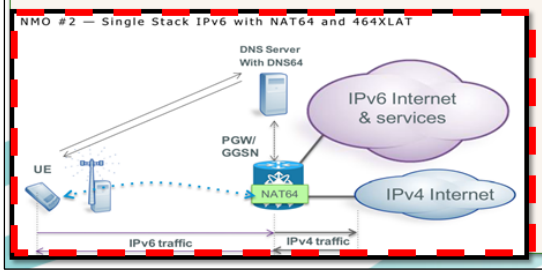
電信等級IPv4/IPv6網路共存供裝技術比較表					
	Dual Stack	NAT444	NAT64	6rd	DS-Lite
減少消耗IPv4位址	視業者IP配發策略而定	是	是	否(需結合其他技術)	是
未來擴充性	是	屬於搭配與過渡方案	屬於搭配與過渡方案	屬於搭配與過渡方案	屬於搭配與過渡方案
可與IPv6共存	是	是(需結合其他技術)	是	是	是
應用服務使用限制	無	部分應用限制	部分應用限制	無	部分應用限制
操作複雜度	高	高	高	中	高
除錯複雜度	高	高	高	中	高
需更換CPE	是	否	是	是	是
建議適用對象	既有業者	既有業者	新興業者	既有業者	新興業者
有實際進行建置或測試之ISP	大部分ISP (含Comcast、NTT)	NTT	China Mobile T-Mobile	FreeNet、Softbank、Comcast	Comcast

- 考量電信網路的既有IPv4需求以及未來應用服務的共存互通需求，多數ISP業者Dual-stack方案為主
- 新興業者因無法取得足夠的Public IPv4位址，因此可能採用IPv6 only + NAT64技術

51







Case1: single stack IPv4 with NAT44

- 純IPv4的狀況，不使用IPv6
- 使用NAT44技術作為減少IP位址損耗的主要方法
- 逐漸由Case 1演進至Case 2
- Eg.,中華電信、其他電信業者（包含Cable業者）

Case2: dual stack IPv6 with NAT44

- 維持IPv4佈署現狀，但用戶主機已啟動IPv4/IPv6 dualstack
- IPv4的部份可使用NAT44技術作為減少IP位址損耗的方法
- IPv6的部份直接連接連線
- Eg., 中華電信、其他電信業者（包含Cable業者）

Case3: single stack IPv6 with NAT64

- 未來Native IPv6用戶使用情境
- ISP只有IPv6用戶，需提供用戶連接既有IPv4服務
- 使用NAT64/DNS64技術作為服務IPv6用戶的主要機制
- Eg.,新興ISP/4G業者，新興企業

52

IPv4/IPv6雙軌網路環境建置

點進網域新視界！

第一部分

Unicast Address Structure

Global Routing Prefix	Subnet ID	interface ID
n bits	64-n bits	64 bits

2001:ca0:68:169::1234/64

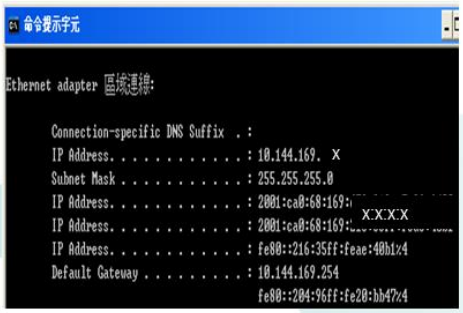
Network位址部份：

2001:ca0:68:169::1234

Interface位址部份:

非簡寫樣式:0:0:0:1234

簡寫樣式::1234



IPv6位址怎麼配置?

54

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)

55

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)

56

IPv6位址配置

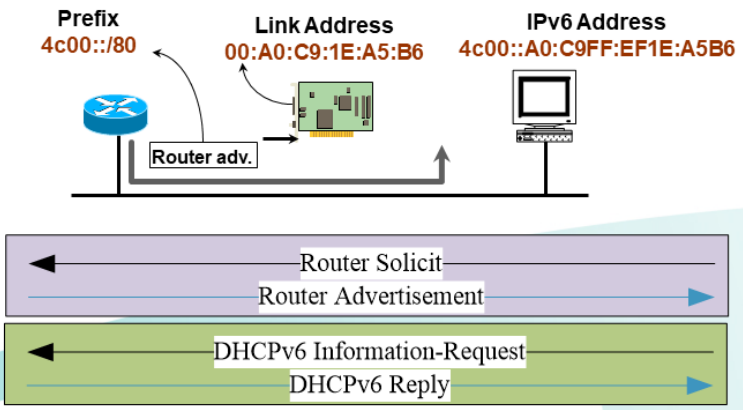
- 全狀態自動配置Stateful Auto-configuration(RFC3315 -> 8415)
  - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
  - 區域無法設置Router的網路環境
    ➔須要求RA標記Flag允許DHCP的使用
  - 運作於Server/Client模型
    ➔因安全或掌握IP等原因使用DHCP Server控管IP pool
- 無狀態自動配置Stateless Auto-configuration(RFC4862)
  - 使用者可自動取得IPv6位址，隨插隨用(Plug&Play)
    但仍須手動設定DNS位址
  - 管理者於網路設備僅需手動設定路由器RA訊息
- 全手動設定Static Configuration
  - 適合網域範圍較小之單位，管理者可一一掌握IPv6發放

57

用戶連網的條件與IPv6自動配置方法（1/2）

"Plug and play" feature

- **Stateless mode : via ICMP (no server required)**



用戶連網的條件

- IP位址
- Default GW
- DNS

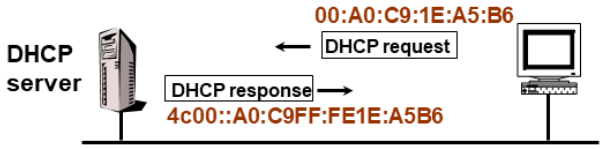
IP位址與Default基本上由網路設備路由通告配置
DNS位址基本上由stateless DHCPv6 方式配置

58

用戶連網的條件與IPv6自動配置方法（1/2）

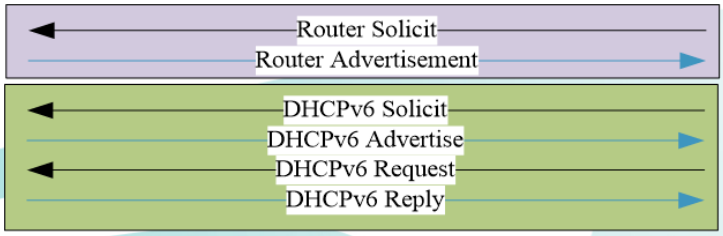
"Plug and play" feature

□Stateful mode：via DHCP



用戶連網的條件

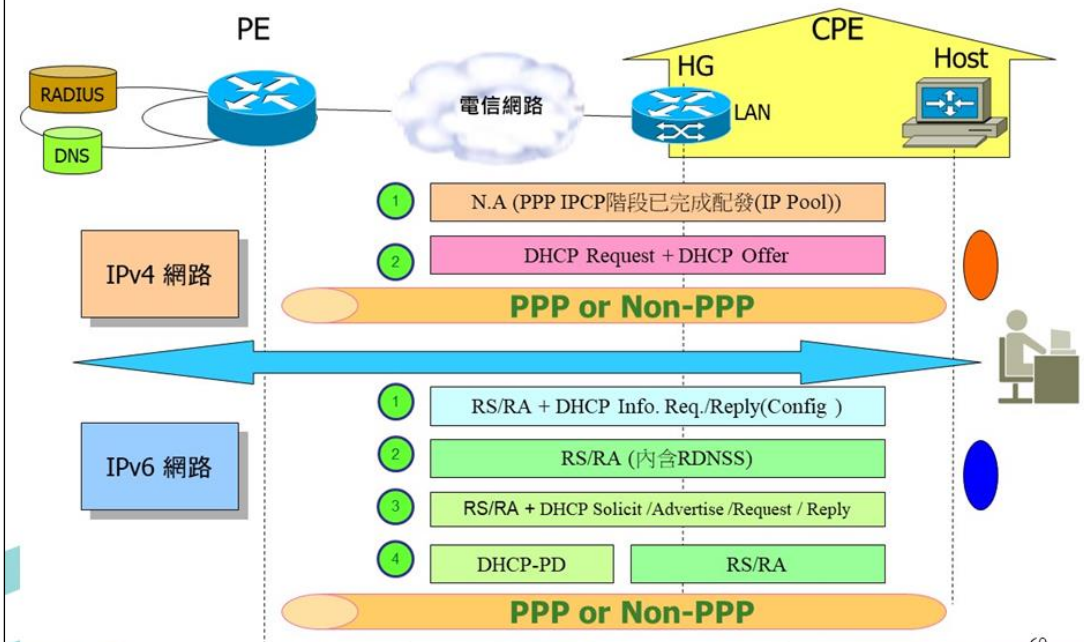
- IP位址
- Default GW
- DNS



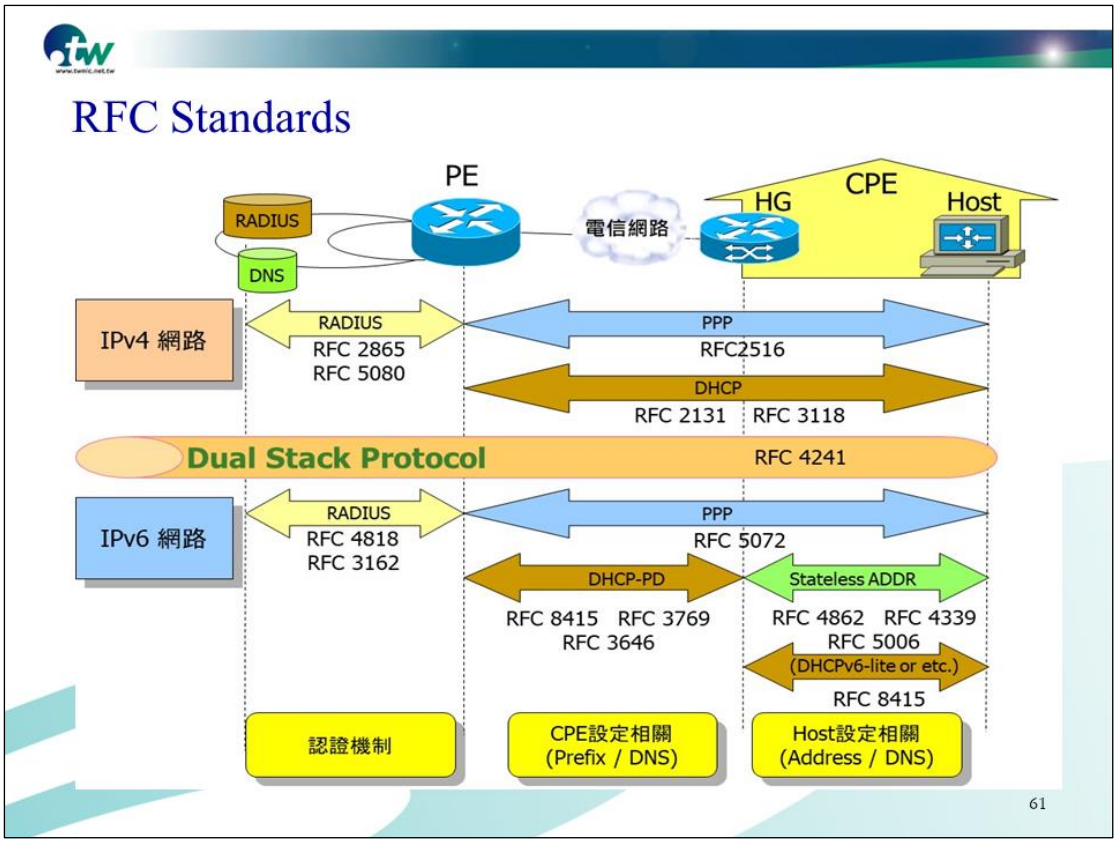
Default GW基本上由網路設備路由通告配置
IP位址與DNS位址基本上由stateful DHCPv6 方式配置

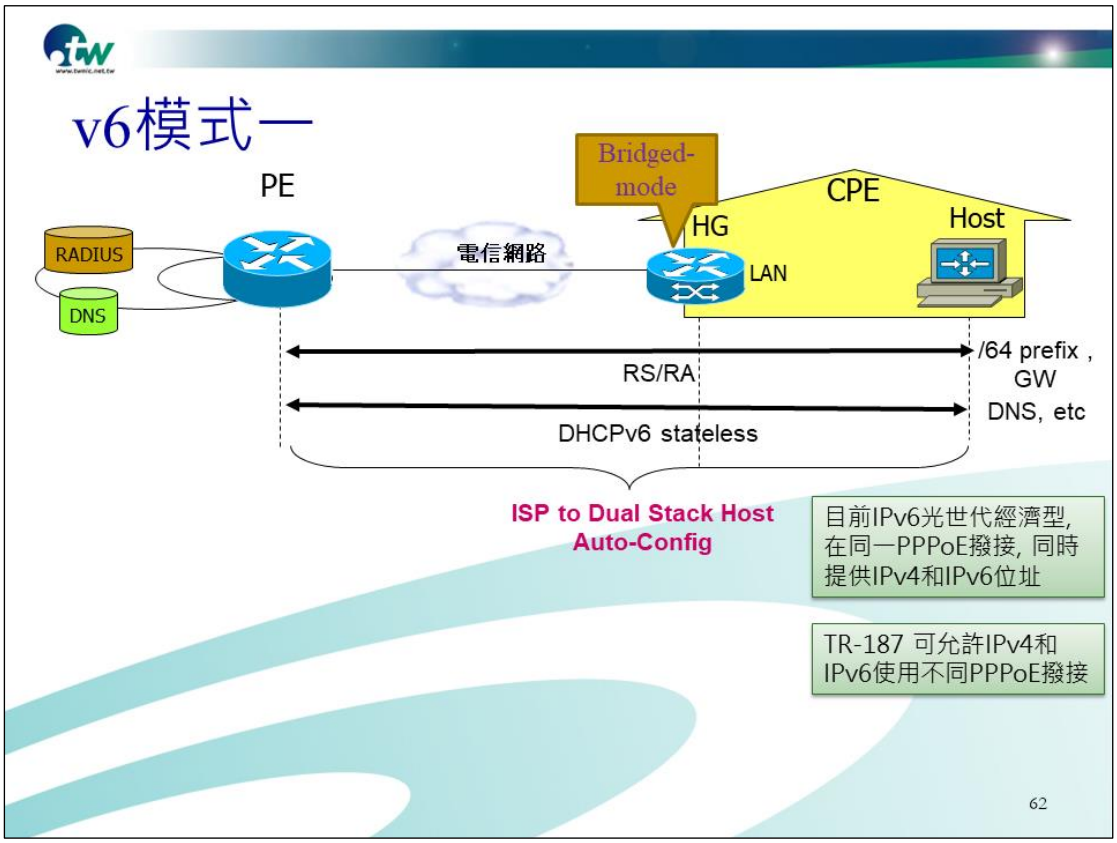
59

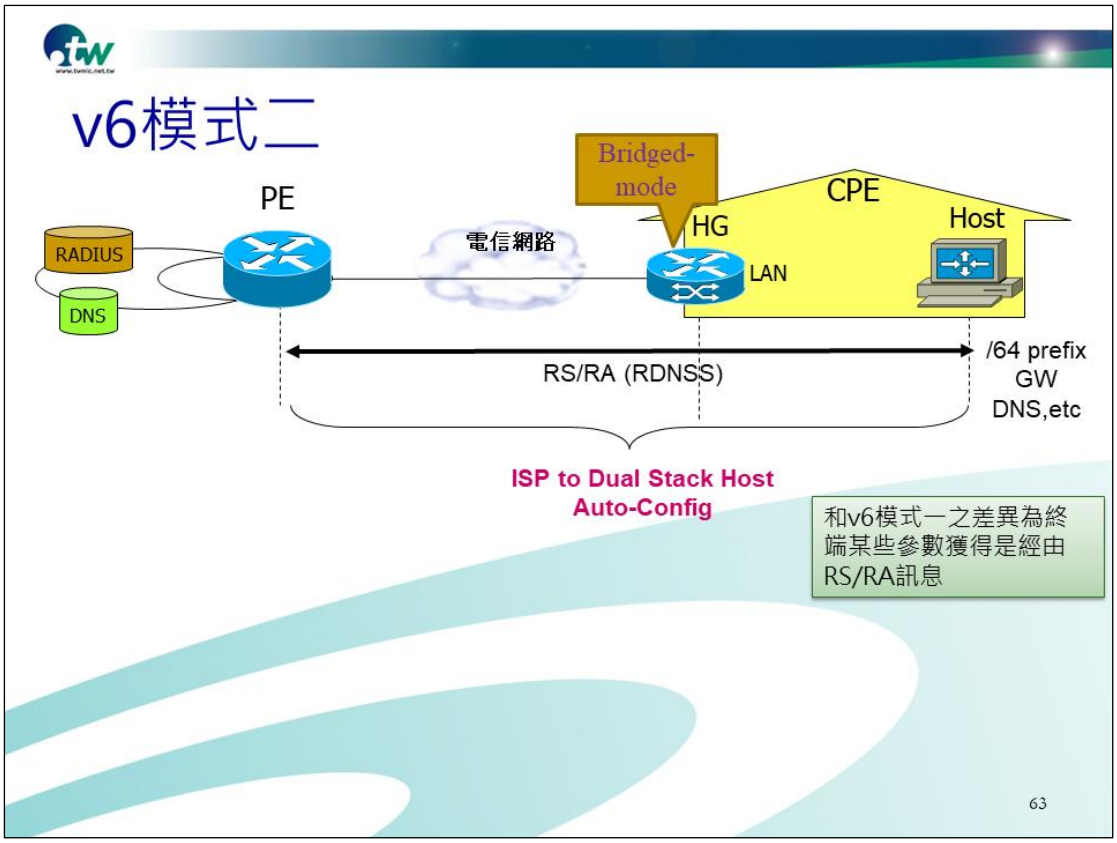
電信網路IPv4/IPv6位址配發模式

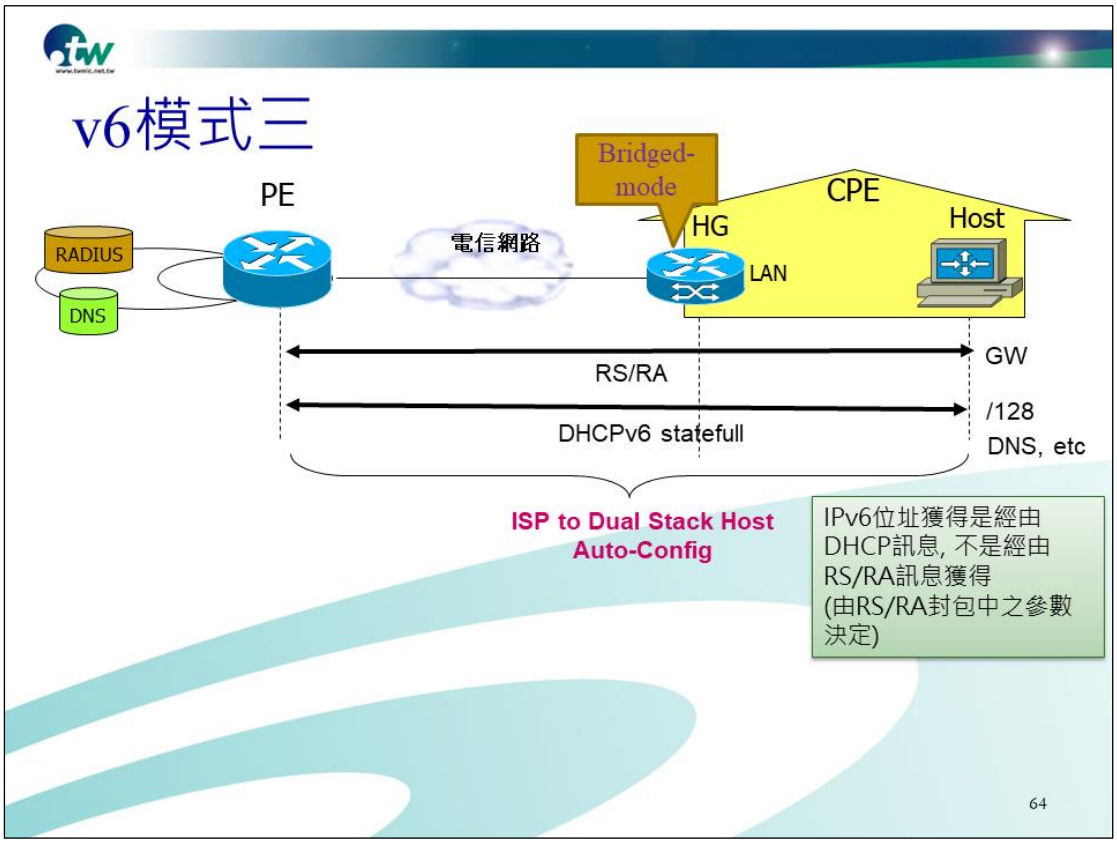


60

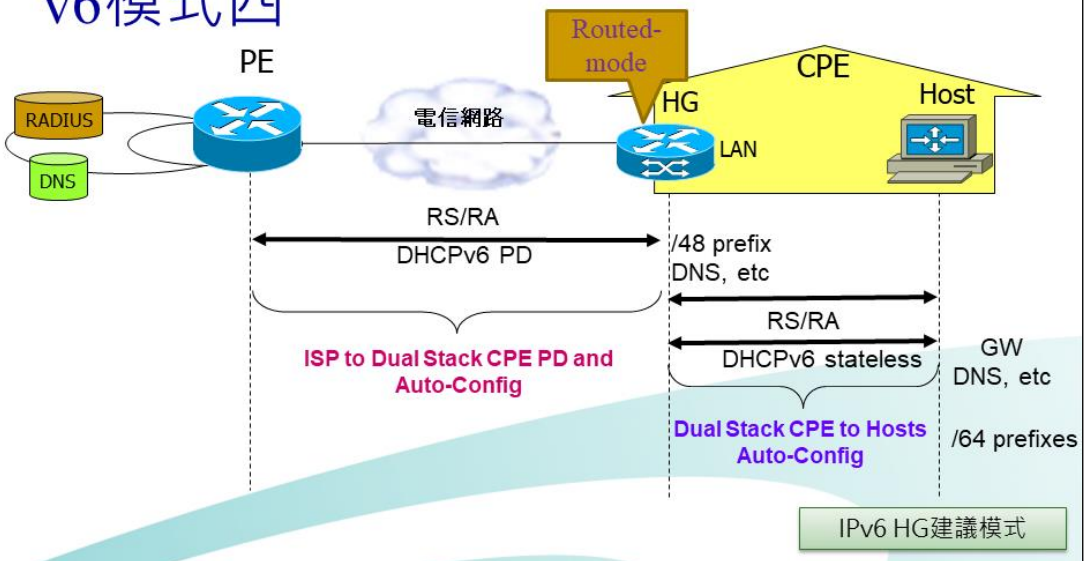

RFC Standards
PE
RADIUS
DNS
電信網路
HG
CPE
Host
IPv4 網路
RADIUS
RFC 2865
RFC 5080
PPP
RFC2516
DHCP
RFC 2131
RFC 3118
Dual Stack Protocol
RFC 4241
IPv6 網路
RADIUS
RFC 4818
RFC 3162
PPP
RFC 5072
DHCP-PD
Stateless ADDR
RFC 8415
RFC 3769
RFC 3646
RFC 4862
RFC 4339
RFC 5006
(DHCPv6-lite or etc.)
RFC 8415
認證機制
CPE設定相關
(Prefix / DNS)
Host設定相關
(Address / DNS)
61


v6模式一
PE
Bridged-mode
CPE
HG
Host
RADIUS
DNS
電信網路
LAN
/64 prefix ,
GW
DNS, etc
RS/RA
DHCPv6 stateless
ISP to Dual Stack Host
Auto-Config
目前IPv6光世代經濟型,
在同一PPPoE撥接, 同時
提供IPv4和IPv6位址
TR-187 可允許IPv4和
IPv6使用不同PPPoE撥接
62


v6模式二
Bridged-mode
PE
CPE
HG
Host
RADIUS
DNS
電信網路
LAN
RS/RA (RDNSS)
/64 prefix
GW
DNS,etc
ISP to Dual Stack Host Auto-Config
和v6模式一之差異為終端某些參數獲得是經由RS/RA訊息
63

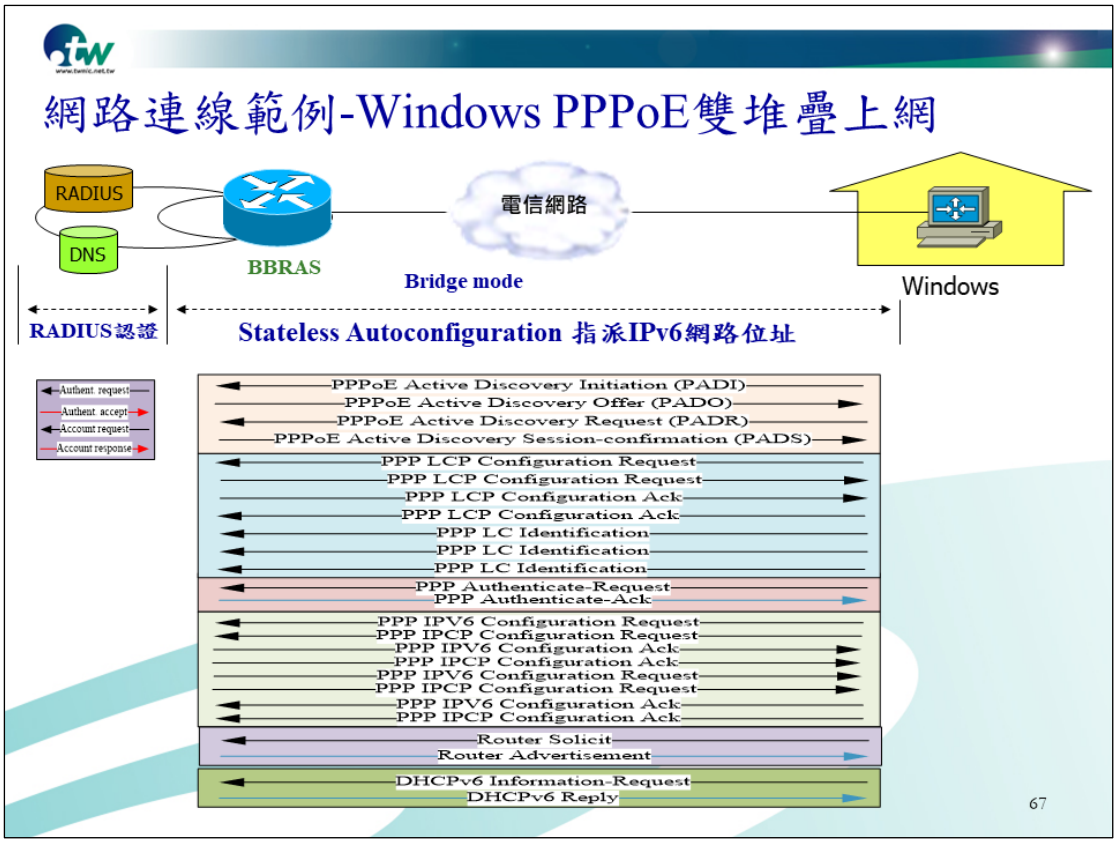

v6模式三
Bridged-mode
PE
CPE
HG
Host
RADIUS
DNS
電信網路
LAN
RS/RA
GW
DHCPv6 statefull
/128
DNS, etc
ISP to Dual Stack Host Auto-Config
IPv6位址獲得是經由DHCP訊息, 不是經由RS/RA訊息獲得(由RS/RA封包中之參數決定)
64

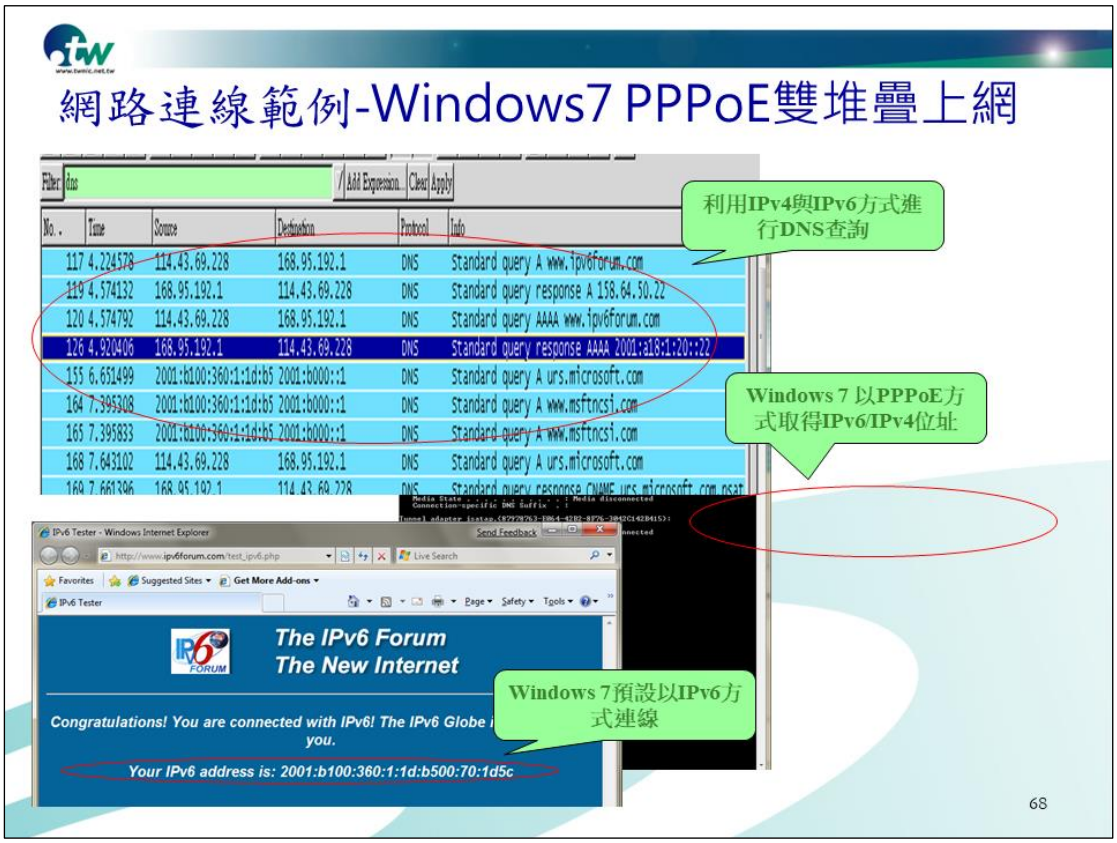
v6模式四



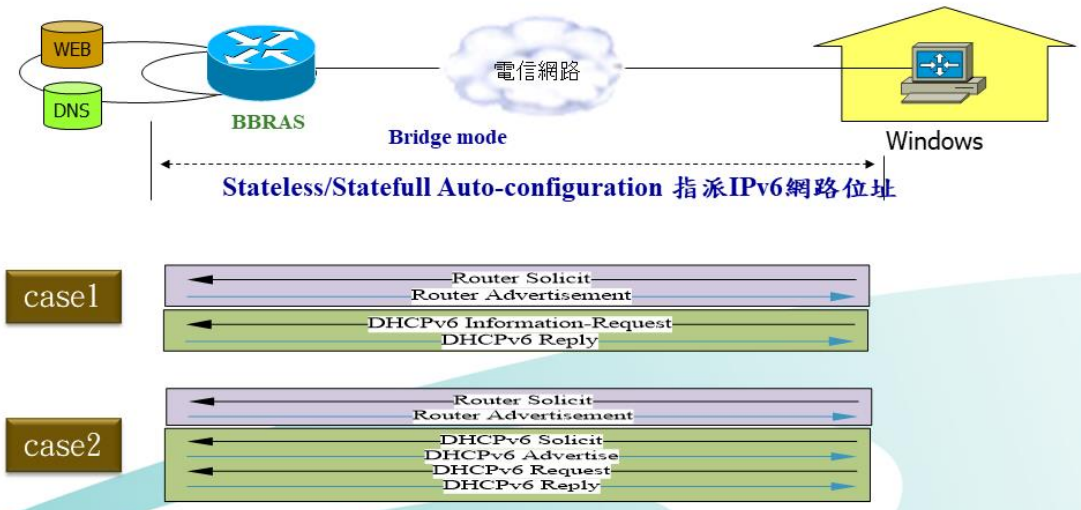
IPv4/IPv6雙堆疊網路位址配發方式

IPv4位址配發方式	PPPoE or Non-PPPoE（IP Pool or DHCPv4 server）			
IPv4DNS配發方式	IPCP 階段配發			
IPv6位址配發方式	PPPoE or Non-PPPoE			
位址與參數配發模式	RS/RA	RS/RA+ DHCP Info. req/Reply (2-way)	DHCPv6 Solicit/Adv./Req./Reply (4-way)	Routing Mode DHCP-PD For HG Solicit/Adv./Req./Reply
IPv6DNS配發方式	RDNSS	DHCP Info. req/Reply (2-way)	Solicit/Adv./Req./Reply (4-way)	由HG配發給HOST
RFC	RFC 5006	RFC 3315	RFC 3315	RFC 3633 RFC 4241
RAS 支援能力	不支援	支援	不支援	不支援
Win OS支援能力	待確認	支援	支援	支援
建議供裝模式	X	V	X	X

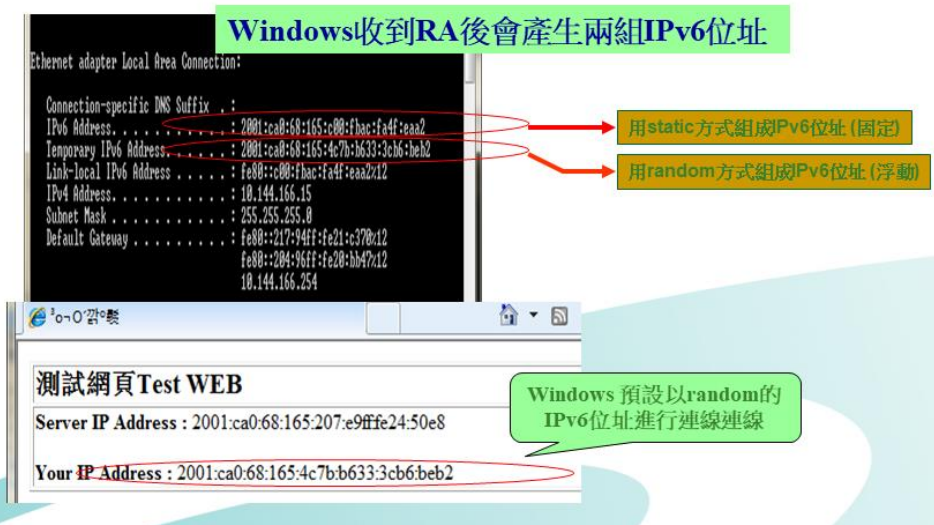

網路連線範例-Windows PPPoE雙堆疊上網
RADIUS
DNS
BBRAS
電信網路
Bridge mode
Windows
RADIUS認證
Stateless Autoconfiguration 指派IPv6網路位址
Authent. request
Authent. accept
Account request
Account response
PPPoE Active Discovery Initiation (PADI)
PPPoE Active Discovery Offer (PADO)
PPPoE Active Discovery Request (PADR)
PPPoE Active Discovery Session-confirmation (PADS)
PPP LCP Configuration Request
PPP LCP Configuration Request
PPP LCP Configuration Ack
PPP LCP Configuration Ack
PPP LC Identification
PPP LC Identification
PPP LC Identification
PPP Authenticate-Request
PPP Authenticate-Ack
PPP IPV6 Configuration Request
PPP IPCP Configuration Request
PPP IPV6 Configuration Ack
PPP IPCP Configuration Ack
PPP IPV6 Configuration Request
PPP IPCP Configuration Request
PPP IPV6 Configuration Ack
PPP IPCP Configuration Ack
Router Solicit
Router Advertisement
DHCPv6 Information-Request
DHCPv6 Reply
67


網路連線範例-Windows7 PPPoE雙堆疊上網
利用IPv4與IPv6方式進行DNS查詢
Windows 7 以PPPoE方式取得IPv6/IPv4位址
Windows 7預設以IPv6方式連線
The IPv6 Forum
The New Internet
Congratulations! You are connected with IPv6! The IPv6 Globe
you.
Your IPv6 address is: 2001:b100:360:1:1d:b500:70:1d5c
68

網路連線範例-Windows Non-PPPoE雙堆疊上網



網路連線範例-Windows Non-PPPoE雙堆疊上網



IPv4/IPv6雙軌網路環境建置

點進網域新視界！

第二部分

可支援IPv6功能的作業系統

Category	OS	版本需求	Notes
Desktop	Windows 7/8/10	支援(Enabled by default)	Includes a DHCPv6 client. Will use RFC3041 privacy addresses otherwise
	Windows 2008/2016	支援(Enabled by default)	support DNS and DHCP over IPv6
	Windows Vista	支援	Includes a DHCPv6 client. Will use RFC3041 privacy addresses otherwise
	FreeBSD	Ver. 4.0 以上	Based on the KAME project
	Linux	Ver. 2.4以上, Ver 2.6.15佳	Available by default on most distributions
	NetBSD	Ver. 1.5 以上	Based on the KAME project
	OpenBSD	Ver. 3.9 以上	Based on the KAME project
	Sun Solaris	Ver. 8 以上	Ver. 8 以上
	IBM AIX	AIX 5.2 以上, (WAS 6.0以上)	AIX 5.2 以上, (WAS 6.0以上)
	MAC OS X	Ver. 10.2 以上	No integrated DHCPv6 client nor MLDv2 support
Smartphone & Table	iOS	Ver. 9.0以上	Only available in automatic mode. If IPv6 is on the network it will auto-configure.
	Android	Ver. 6.0以上	
Embedded	VxWorks	PLATFORM CD 1.1	No integrated DHCPv6 client nor MLDv2 support

Source:http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems#cite_note-6
Source:http://www.sixxs.net/wiki/IPv6_Capable_Operating_Systems

72/65

可支援IPv6功能的應用程式

Application	IPv6 supported?
AbsoluteTelnet	Yes
Apache httpd	Yes
Apple Mail	Yes
BIND	Yes
BSD Telnet	Yes
CUPS	Yes
cURL	Yes
ffproxy	Yes
FileZilla	Yes
ftp.exe	Yes
Google Chrome	Yes
Hiawatha	Yes
IIS	Yes
Internet Explorer	Yes
Irssi	Yes
Java	Yes
Konqueror	Yes
lighttpd	Yes
Linux CIFS VFS	Yes
Linux NetKit ftp	Yes
Linux NetKit Telnet	Yes
Microsoft DNS	Yes

Application	IPv6 supported?
Microsoft Outlook	Yes
mIRC	No
Mozilla / SeaMonkey	Yes
Mozilla Firefox	Yes
Mozilla Thunderbird	Yes
Nmap	Yes
OpenLDAP	Yes
OpenSSH	Yes
OpenVPN	Planned
Opera	Yes
Outlook Express	No
Pidgin	Yes
Polipo	Yes
Privoxy	Yes
PuTTY	Yes
Quagga	Yes
rsync	Yes
Safari	Yes
Samba	Yes
Simple DNS Plus	Yes

Application	IPv6 supported?
SmartFTP	Yes
Squid cache	Yes
srelay	Yes
telnet.exe	Yes
TightVNC	Optional
tinc	Yes
Trillian	?
UDP Speed Test 3	Yes
VLC	Yes
Wget	Yes
Winamp	Yes
Windows File and print sharing	Yes
Windows Media Player	Yes
WWWOFFLE	Yes
XChat	Yes
xinetd	Yes
µTorrent	Yes

大部分應用程式已經具備支援IPv6能力

Source：http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support
https://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_common_applications

可支援IPv6功能的設備

編號	項目	規範建議
IPv6 主機 (Host) 必要規格		
1	核心項目	IPv6 Ready Logo Phase-2 Core for Host
IPv6 主機 (Host) 選項規格		
2	安全選項	IPv6 Ready Logo Phase-2 IPSec for End-Node
3	網管選項	IPv6 Ready Logo Phase-2 SNMP for Agent (以 SNMPv 2c 和 RFC 4293 IP MIB 為參考標準)
4	移動性選項	IPv6 Ready Logo Phase-2 Mobility for Mobile Node 或 Correspondent Node
5	DNS 選項	RFC 3596
6	DHCPv6 選項	IPv6 Ready Logo Phase-2 DHCPv6 for Client (支援 Client 模式，標準為 RFC 3315)
7	應用程式選項	SIP：IPv6 Ready Logo Phase-2 SIPv6 for User Agent Email、Web 及其他應用程式：必須同時支援 IPv4/IPv6 通訊協定

備註：選項項目請依據主機功能需求選列。

編號	項目	規範建議
IPv6 路由器 (Router) 必要規格		
1	基本項目	IPv6 Ready Logo Phase-2 Core for Router
IPv6 路由器 (Router) 選項規格		
2	安全選項	IPv6 Ready Logo Phase-2 IPSec for Secure Gateway
3	網管選項	IPv6 Ready Logo Phase-2 SNMP for Agent (以 SNMPv 2c 和 RFC 4293 IP MIB 為參考標準)
4	移動性選項	IPv6 Ready Logo Phase-2 Mobility for Home Agent
5	DNS 選項	RFC 3596
6	DHCPv6 選項	IPv6 Ready Logo Phase-2 DHCPv6 for Server (支援 Server 或 Relay Agent 模式，標準為 RFC 3315)
7	路由選項	根據路由器之容量及使用地點，決定適當通訊協定 SOHO Router：支援 RIPNG (RFC 2080) 大容量 Router：支援 OSPFv3 (RFC 5340)和 BGP-4+ (RFC 2545、RFC 4271)

備註：選項項目請依據主機功能需求選列。

可支援IPv6功能的設備清單請參閱
http://www.ipv6ready.org/

可支援IPv6功能的網站

- 網站需具備IPv6連線能力及註冊IPv6網域名稱

序號	類別	所屬單位	網站名稱(點選可直接網站)	IPv6位址	登錄時間	IPv6連線狀態
1	公司	各界貿易有限公司	http://delonghi.com.tw	2002:3cf8:903c::3cf8:903c	2010-06-23	正常運作
2	公司	JYKK JAPAN INC	http://snowscoot.com.tw	2001:b50:82:195:224:110	2010-06-23	正常運作
3	公司	鏡頭科技股份有限公司	http://www.ipv6.ringline.com.tw	2001:b021:28::1	2010-07-31	正常運作
4	公司	代美國購有限公司	http://dear.com.tw	2001:470:0:b4::4834:46aa	2010-06-23	正常運作
5	公司	天心商場	http://condom.com.tw	2001:470:0:e7::4a52:2869	2010-06-23	正常運作
6	公司	泓泰資訊企業有限公司	http://thenet.com.tw	2002:d203:4621::d203:4621	2010-06-23	正常運作
7	公司	五一零數位科技有限公司	http://510tech.com.tw	2002:3cfb:4750::3cfb:4750	2010-06-23	正常運作
8	公司	智微數位科技股份有限公司	http://373834.com.tw	2002:d314:6782::d314:6782	2010-06-23	正常運作
9	公司	Tommy Hilfiger Licensing LLC	http://hilfiger-denim.com.tw	2001:7b8:3:5::80:1	2010-06-23	正常運作
10	公司	Tommy Hilfiger Licensing LLC	http://hilfigerdenim.com.tw	2001:7b8:3:5::80:1	2010-06-23	正常運作
11	公司	康輔科技股份有限公司	http://ez-care.tw	2002:7b32:36a6::7b32:36a6	2010-06-23	正常運作
12	公司	Edo Popken Consulting	http://edopopken.tw	2001:b50:82:195:225:114	2010-06-23	正常運作
13	公司	Webassest	http://metevista.tw	2001:888:2000:29::206:85 2001:888:2000:29::206:86 2001:888:2000:29::206:87 2001:888:2000:29::206:88	2010-06-23	正常運作
14	公司	Webassest	http://metev-vista.tw	2001:888:2000:29::206:86 2001:888:2000:29::206:87 2001:888:2000:29::206:88	2010-06-23	正常運作
15	公司	Novso	http://novso.tw	2a00:14e8:102:4::4 2a00:14e8:102:4::5	2010-06-23	正常運作
16	公司	Webassest	http://zsover.tw	2001:888:2000:29::206:81 2001:888:2000:29::206:82 2001:888:2000:29::206:83 2001:888:2000:29::206:84	2010-06-23	正常運作
17	公司	BIT BV	http://tokina.tw	2001:7b8:3:5::80:1	2010-06-23	正常運作
18	公司	台灣網路資訊中心	http://www.twnic.net.tw	2001:c50:ffff:1::228	2010-06-23	正常運作

Status[?]	ID	Organization Name	URL	Region/ Country	Tags	Approved Time
IPv6 Enabled	W1-ES-00000001	Consulintel	www.ipv6tf.org	ES	IT Site	2009-05-02 22:41:02
IPv6 Enabled	W1-US-00000002	Hurricane Electric	he.net	US	Enterprise Site	2009-05-02 22:24:58
IPv6 Enabled	W1-US-00000003	Best4Men.com LLC	ipv6.best4men.com	US	Others	2009-05-02 15:31:28
IPv6 Enabled	W1-US-00000004	Hurricane Electric	tunnelbroker.net	US	Enterprise Site	2009-06-09 21:21:18
IPv6 Enabled	W1-US-00000005	Broque	www.deus-exmachina.net	US	Personal Site	2009-05-02 21:03:10
IPv6 Enabled	W1-CA-00000006	NixxNET/CNS	6.nixx.ca	CA	Personal Site	2009-05-02 20:35:35
IPv6 Enabled	W1-US-00000007	Kim	tykimus.com	US	Personal Site	2009-05-02 21:02:35
IPv6 Enabled	W1-US-00000008	IPv6 Ready Logo	www.ipv6ready.org	US	Not-for-profit Cooperative Site	2009-05-04 15:11:42
SERVICE-IN	W1-DE-00000009	Personal Site	wiki.paepstin.info	DE	Personal Site	2009-05-05 07:36:28
IPv6 Enabled	W1-CA-00000010	Viagenie	www.viagenie.ca	CA	Enterprise Site	2009-06-09 21:21:28
IPv6 Enabled	W1-CN-00000011	BII Group	www.ipv6.net.cn	CN	IT Site	2009-05-07 12:45:27
IPv6 Enabled	W1-FI-00000012	Axu TM Oy	www.axu.tm	FI	IT Site	2009-05-08 [illegible]
IPv6 Enabled	W1-FI-00000013	TREX Tampere Region Exchange Oy	www.trex.fi	FI	IT Site	

可支援IPv6功能的網站清單請參閱

http://v6directory.twnic.net.tw/

http://www.ipv6forum.com/ipv6_enabled/approval_list.php

網路設備支援IPv6

- 網路設備如路由器, 交換器等主要廠牌均已支援IPv6
- 在進行各項測試作業之前，應先確認網路設備是否已啟動IPv6的功能，如何確定待測設備已啟動IPv6功能，主要可透過底下三種方式來確認：
  - 可洽設備廠商或代理商協助確認設備功能或型號；
  - 檢視設備本身的網路介面是否有fe80::開頭的IPv6位址格式；
  - 可確認設備是否通過IPv6 Ready logo設備認證

76

防火牆升級IPv6

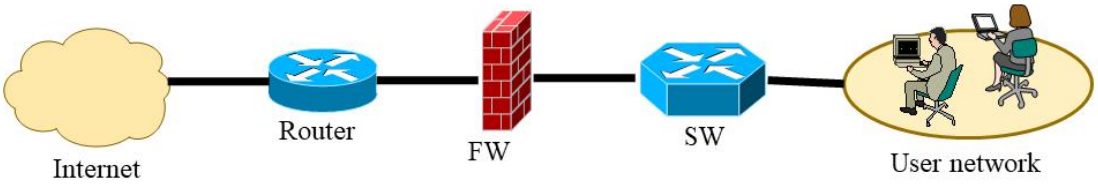
- 網際網路的盛行，越來越多的攻擊技術也不斷的產生，如何有效的阻隔外在的威脅，「防火牆」扮演關鍵角色
- 在功能上，防火牆可有效地監控內部網路和網際網路之間的任何活動，提供基本的內部網路安全防護
- 通過監測、限制、更改要通過防火牆的「封包」或「訊務」，屏蔽內部需要受保護的網路資訊、結構和運行狀況，防止資訊洩露，以此來保護網路的安全

IPv6防火牆特徵

- **No need to NAT**
- **Network scanning virtually not possible (/64)**
- **Deny DNS zone transfer**
- **Weaknesses of the packet filtering cannot be make hidden by NAT**
- **Support for IPv6 header chaining**
- **Support for IPv4/IPv6 transition and coexistence**
- **Not breaking IPv4 security**

77

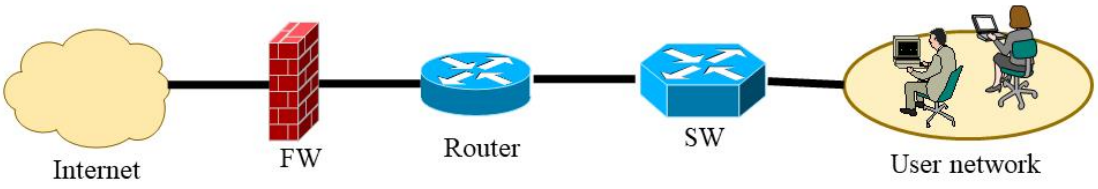
IPv6防火牆部署方法(1)



- Internet ↔ Router ↔ Firewall ↔ Net architecture
- Requirements:
  - Firewall must support/recognise ND/NA filtering
  - Firewall must support RS/RA if SLAAC is used
  - Firewall must support MLD messages if multicast is required

78

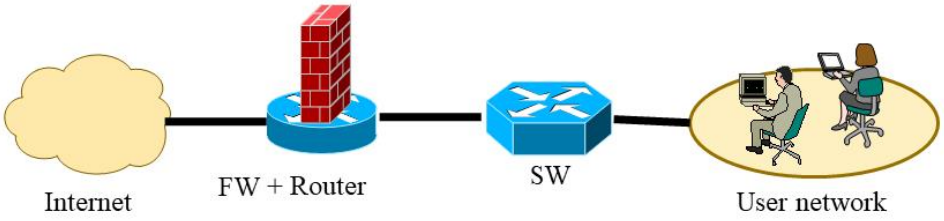
IPv6防火牆部署方法(2)



- Internet ↔ Firewall ↔ Router ↔ Net architecture
- Requirements:
  - Firewall must support ND/NA
  - Firewall should support filtering dynamic routing protocol
  - Firewall should have large variety of interface types

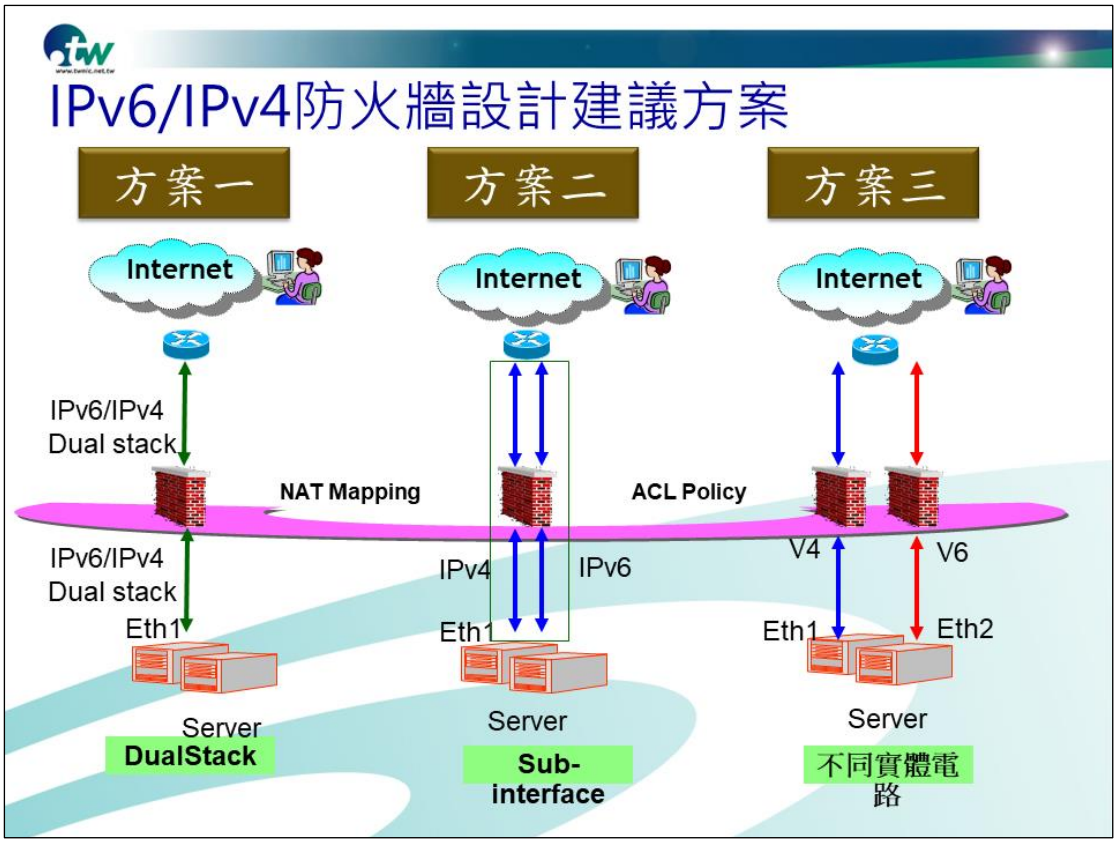
79

IPv6防火牆部署方法(3)



- Internet ↔ Firewall/Router(edge device) ↔ Net architecture
- Requirements
  - Can be powerful - one point for routing and security policy – very common in SOHO (DSL/cable) routers
  - Must support what usually router AND firewall do

80


IPv6/IPv4防火牆設計建議方案
方案一
方案二
方案三
Internet
Internet
Internet
IPv6/IPv4
Dual stack
NAT Mapping
ACL Policy
IPv6/IPv4
Dual stack
Eth1
IPv4
IPv6
Eth1
V4
V6
Eth1
Eth2
Server
DualStack
Server
Sub-
interface
Server
不同實體電路


點進網域新視界！
網路升級流程
步驟和檢查項目清單

IPv6網路升級考量

- 一個單位的網路使用者如何連至外頭的Internet？
  - 透過內部控管的有線或無線網路
    - IP配發機制、PC、L2/L3網路、DNS、Proxy、FW
  - 內部網路的IP可能為Private IPv4 or Global IPv6 or Unique local address
- 企業網路的使用者會access哪些Intranet服務？
  - Web services (eForm)、mail server
    - IP配發機制、PC、L2/L3網路、DNS、Servers

從終端用戶角度思考

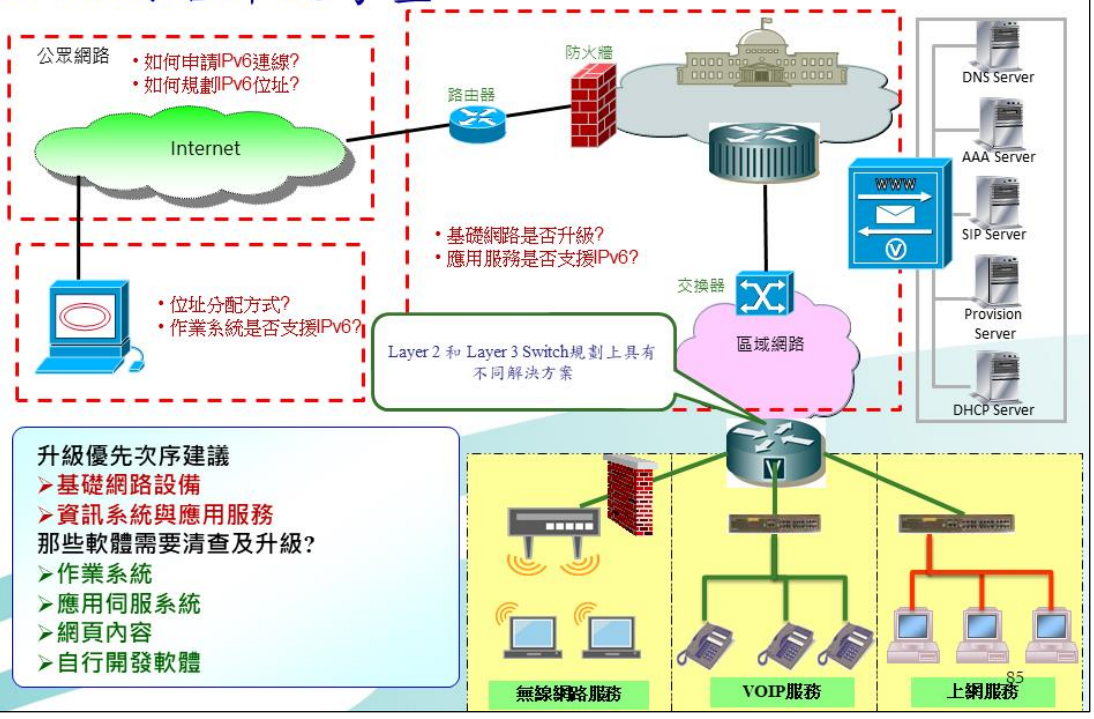
83

問題從哪裡發生

- 多數的網路異常，都是來自終端用戶反應，尤其是網路異動後。(如 IPv6 轉換)
  - 例：PC, IP phone, printer, POS 交換機，WiFi GW，資訊與應用系統等…
- 共通的問題
  - “不通”，“無法連線”，“檔案無法正常傳遞”，“應用程式無法回應”，“網路好慢”

84

IPv6網路升級考量



升級優先次序建議
- 基礎網路設備
- 資訊系統與應用服務

那些軟體需要清查及升級?
- 作業系統
- 應用伺服系統
- 網頁內容
- 自行開發軟體

85

升級作業環境評估
升級移轉評估-基礎

- **進行移轉時的評估重點**
  - 網路服務供應商(ISP)是否有提供雙協定服務?
  - 網路設備(路由器、交換器)是否支援雙協定?
  - 內部網路架構狀況為何?
  - 網路管理設備(流量監控及報表)是否支援雙協定?
  - 資安防護設備(IPS、IDS、防火牆等)是否支援雙協定?
  - 加值服務設備(VPN Server、Storage)是否支援雙協定?
  - 終端使用者的資訊設備是否支援雙協定?

86

升級作業環境評估
升級移轉評估 – 網路維運人員

- **網路維運人員**
  - 是否須更換或升級現有網通設備以支援雙協定?
  - 是否須採購支援雙協定的無線基地台及認證閘道器?
  - 是否須採購支援雙協定的資安防護及監控設備?
  - 是否須升級現有的網路應用加值設備?
  - 是否須升級現有的網路應用加值設備?
    - 電子郵件(E-Mail)服務設備
    - 虛擬私人網路(VPN) 服務設備
    - 負載平衡(Loading Balance)設備

87

升級作業環境評估
升級移轉評估 – 終端使用者部分

- **終端使用者**
  - 是否須採購或升級終端資訊設備以支援雙協定?
  - 是否須購買雙協定的作業系統的授權?
  - 是否須升級現有的應用程式軟體以支援雙協定?
  - 使用者移轉時須花費時間了解基礎知識
  - 使用者移轉時須花費時間熟悉新設備及設定
  - 使用者可能拒絕配合移轉、更換現有硬體及修改設定

88

升級作業環境評估

- 單位願意提供多少預算進行移轉?
- 使用者願意付出多少配合度進行移轉?
- 網路維運人員是否有足夠人力支援移轉?

89

IPv6部署重要事項

90

IPv6升級策略目標

- 降低導入成本
  - 網路設備升級至IPv6非一蹴可幾，礙於導入預算成本之限制，需針對現有網路設備規劃階段性的升級工作
- 規劃重要網路應用服務升級
  - 網路管理員可針對網路流量大或重要之網路應用服務，調查其服務之主要網路傳輸設備，並評估運作模式是否與IP層有關，以作為未來導入IPv6首要升級重點
- 規劃升級時程與順序
  - 有些重要的網路設備，流量雖不大，但是卻有立即性的升級需求，如IDC機房的服務，因IPv4位址已經用罄，且此類型服務大多直接提供對外服務，因此較有機會進行，則規劃上建議優先考量此設備

91

IPv6升級規劃作業建議

Phase I	Phase II		Phase III	
規劃	試用	驗證	推廣	上線
■ 作業流程規劃 ■ 網路架構設計 ■ IP位址申請 ■ IP位址分配與配置方式規劃 ■ 確認連線服務模式 ■ 網路設備盤點 ■ 應用服務盤點與導入規劃 ■ 研擬具體與行動方案	■ 系統導入流程確認 ■ 查測與管理系統流程確認	■ 網路與服務IPv6準備度現況分析 ■ 測試計畫與方法 ■ 安全與效能驗證 ■ 測試問題檢討與改善	■ 宣導推廣 ■ 小規模試用並確認IPv6商轉之可行性 ■ 加值服務規劃	■ 正式服務啟動 ■ 成效分析 ■ 客戶滿意度調查

教育訓練：開辦相關訓練課程，強化一般同仁對IPv6技術的熟悉度

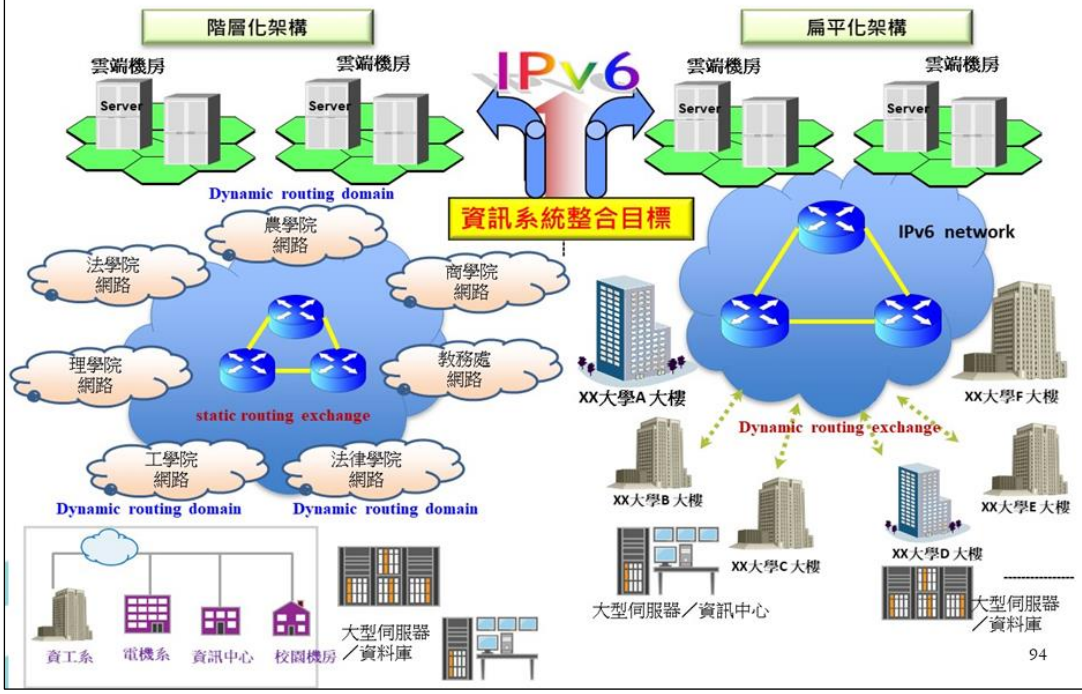
92

網路架構設計

- 瞭解管理網域的連接架構
  - 評估所管理的網域連接架構選擇合適的轉移技術
  - 瞭解各個單位與所管理的網路設備連接點以便設置新設定
- 瞭解管理網域 – 該如何切割 VLAN ?
  - 考量位址發配方式
  - 配合IPv6發放可同步檢討原先IPv4發放政策

93

架構討論



階層式與扁平化架構比較

- 網路管理架構在規劃選用時所需考慮的因素，通常包括網路規模、網路架構、部門組織架構、地理位置分佈等。
- 組織可以因應實際需要來選用不同的網路佈署架構

	階層式網路架構	扁平化網路架構
優點	◆分散網管控制權 ◆容易維護與更新 ◆資源利用率高	◆執行效率較高 ◆提高彈性
缺點	◆網路架構較複雜 ◆成本較高	◆路由表資訊較複雜 ◆容錯性較低 ◆網路管理較難掌握

95

IPv6位址申請與配置

- 依據管理網域大小決定申請數量
  - 由於IPv6設計使位址數量絕對足夠使用
  - 基本原則以單位網域大小根據Prefix長度進行申請
- 配合上層管理單位發放政策
  - 瞭解上層單位之Prefix配發政策
  - 申請最合適之網域大小
- 考量設定及發配的便利性
  - 考量使用者使用及管理者發配IP的情況
  - 如網段選擇最有利記憶之靜態設定
    ex. 配合樓層或單位編號之ID申請

96

位址規劃的策略

- 位址分配可以依據某種特定的邏輯來分割已經從RIR獲得的位址前綴。這些設計邏輯可以包含以下因素：

	地理邊界	組織機構邊界	業務類別邊界
說明	同一地區的所有子網分配相同的前綴	同一機構或同一類型機構的聯合體分配相同的前綴	為某些特定的業務預留地址前綴，，如：VoIP、內容分發服務、無線網路等等
優點	◆採用地理條件劃分網段，容易識別 ◆資源利用率高	◆採用階層式管理架構，容易管理 ◆容易維護與更新	◆採用應用類別區分網段，容易識別 ◆彈性較高

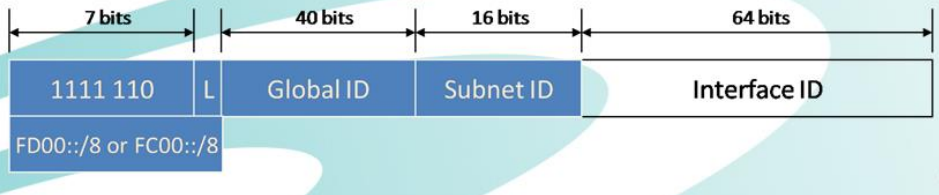
建議融合以上三種策略來劃分網路位址

組織機構邊界優先 → 地理邊界次之 → 業務類別邊界採用保留位址

97

Global Unicast與Unique-local address 位址考量

- **IPv6的位址規劃與IPv4的位址規劃類似，皆必須考慮aggregation的問題**
  - 網路架構的增長，必須保持路由聚集的需求
  - 採用Global Unicasting與Unique-local Address的考量
- **ULA會隨機選擇40位的Global ID，因此FC00::/7位址區塊內的ULA前綴必然是不聚集的。**
  - 在一個/48大小的ULA Global ID之下，仍然有16位的子網ID可供使用，適當分配ULA Global ID，盡量將邏輯上屬於同一對象的網路規劃到子網範疇以內，也是避免大網內部路由產生過多more-specifics的有效途徑。



98

Global Unicast與Unique-local address 比較

Global Unicasting address	Unique-local address
可在全球路由範圍內到達，與IPv4的Public位址相同，	類似IPv4的Pricate位址，無法與網際網路上的路由交換，僅能在私有網路中使用
Global unicasting address需統籌由全球網路管理機構進行分配與控管	Unique-local address不需要由全球網路管理機構進行分配與控管
Global unicasting address前三個bits是001，例如：3FFE:BOOO:123:456::1	FC00::/7是Unique-local address類型的前綴格式
在Multihoming的網路環境下，用戶可能要考慮兩個以上ISP所分配的位址空間	在網路ISP以及Global unicasting address變換時，ULA的位址編制不受影響，

99

位址規劃的策略

- 企業網路在部署時可考慮同時配置ULA與Global位址
  - 作業系統預設的位址選擇演算可以正確地選取來源和目的位址，即如果來源和目的主機都包含ULA位址時，則選擇ULA位址為優先(RFC 3484)
  - ULA與Global位址二者可採用一致的子網路編址方案
- 建議現階段一般企業網路位址劃先採用Global Unicasting address方式進行，並針對ULA發展狀況保持密切注意
- 如內網為NAT架構則可考慮NPT（RFC6296）

100

設備清查與盤點-
清查設備屬性

- **網路傳輸設備**
  - 如：Switch Hub, Layer 2 Switch、Layer 3 Switch、Router…
- **網路安全防護設備**
  - 如：防火牆(Firewall, FW)、入侵偵測系統(IDS)、入侵防護系統(IPS) 、 新一代防火牆(Network Generation Firewall, NGFW)…
- **終端設備**
  - 如：個人電腦、筆記型電腦、平板電腦、行動電話、…
- **應用伺服器**
  - 如：DNS、Web、FTP、Proxy、Media、Database…
- **網路管理設備**
  - 如：SNMP Manager, Multi Router Traffic Grapher (MRTG)

101

設備清查與盤點-
清查網路設備IPv6支援程度

- 清查網路設備IPv6支援程度
  - 網路設備廠牌與供應商
    - EX：CISCO 2811 (XXXX代理公司)
  - 網路設備廠軟體版本
    - EX：IOS 12.1(14)
  - 網路設備授權年限
  - 網路設備目前CPU乘載量
    - CPU已接近滿載設備，建議重新添購新設備支援IPv6
  - 網路設備支援IPv6現況
    - 情況1：原有網路設備已內建支援IPv6功能。
    - 情況2：需升級設備韌體，即可升級支援IPv6。
    - 情況3：上述情況無法導入IPv6，則建議列入汰換清單，重新採購新型網路設備。
  - 網路設備升級負責人

102

管理及除錯方式(1)

- **Fault management**
  - 部分使用者無法連接Internet時➔IPv4或VLAN設定問題
    - 請使用者檢查IPv4位址、遮罩及預設閘道是否設定正確
    - 採用DHCP Server提供使用者自動取得Private IP連接至路由器，反查該MAC位址找出所對應的Switch Port檢查設定
  - 部分使用者無法取得IPv6位址時➔作業系統設定問題
    - 完整製作IPv6各作業系統安裝流程(XP, Win 7, Linux Ubuntu, Linux CentOS…)
    - 將設定問題及解決方式集錦成FAQ提供參考

103

管理及除錯方式(2)

- **Configuration management**
  - 將網路規畫包含IPv4、IPv6 Prefix及VLAN ID表格化
  - 熟悉Router及Switch等網路設備設定指令(網管人員訓練)
  - 將問題除錯訂定標準流程(Standard Operating Procedure)
- **Accounting , Performance and Security Management**
  - 目前應用層管理方面仍使用路由器設備所輸出的NetFlow資訊進行統計、管理與監控
  - 注意設備是否支援NetFlow V9 / sFlow等的輸出
  - 整理Flow輸出檔成為網路管理介面之程式撰寫(Optional)
  - 整合管理介面呈現流量報表資訊以便監控

104

IPv6升級作業—事前準備

- IPv4/IPv6雙協定技術選擇及測試
  - 由於Tunneling及Translating技術門檻較高，且額外購置網路設備成本不足
  - 非網路背景之使用者仍然習慣以IPv4進行連線
  - 選擇以Dual Stack實行IPv4/IPv6雙協定網路
- 申請IPv6位址(TWNIC或HiNet或區網中心)
  - 確定連線公眾IPv6網路方式
  - /64分配給終端用戶
  - /56分配給家庭用戶
  - /48分配給企業用戶

105

IPv6升級作業—事前準備

- 規劃位址發放及使用
  - 由於IPv6數量足夠使每一單位獨立擁有一段/64之IPv6位址
  - 使用者方便考量及設備支援下，採取無狀態自動取得(Stateless Auto-configuration)
  - 單一VLAN可使用符合EUI-64格式的自動取得位址
- VLAN切割與重新劃分
  - 配合IPv6升級作業重整VLAN並重新規劃IPv4位址
  - 劃分每單位擁有獨立VLAN
    - 優點：各實驗室間IP網段獨立使用，各單位間流量隔離，且能夠使每一單位以無狀態自動取得方式使用一組/64之IPv6位址
    - 缺點：須一一設定Switch連接連線單位的Port對應VLAN，造成網管人員於轉移時工程負擔

106

IPv6升級作業-DNS IPv6配置

網域名稱伺服器（DNS）

- 正向位址解析
  - 支援A資源記錄(IPv4); AAAA資源記錄(IPv6)
  - 同時回應A與AAAA記錄的DNS請求
- 反向位址解析
  - 支援PTR記錄
- AAAA DNS請求的傳送(Transport) : IPv4/IPv6

	IPv4	IPv6
Hostname to IP address	A record : www.abc.com A 192.168.1.30	AAAA record : www.abc.com AAAA 2001:B030:6:8::2
IP address to Hostname	PTR record : 30.1.168.192.in-addr.apra. PTR www.abc.com	PTR record : 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.0.6.0.3.0.b.1.0.0.2.ipv6.apra PTR www.abc.com

107

IPv6升級作業-如何規畫IPv6位址

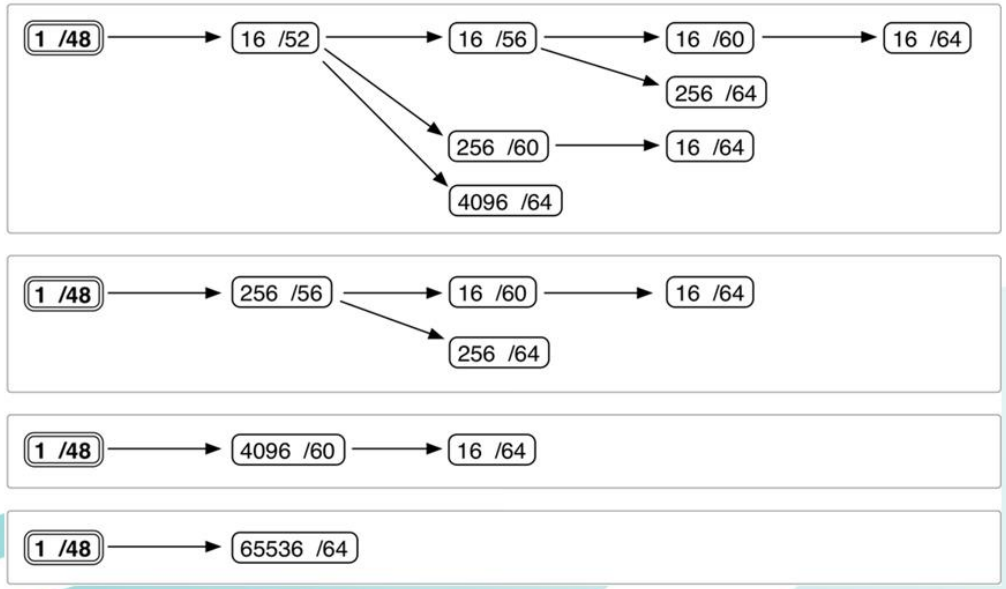
- IPv6網路以 /64網段為一個區域網路(Subnet)的最小位址分配單位
- /64位址網段可提供2的64次方IPv6位址供設備使用
- 子網段切割可考慮地理邊界、組織架構或業務類別來劃分

32 bits	24 bits	8 bits	64 bits
TLA/S-TLA	保留位元	子網段	Interface ID
← TWNIC →	← 保留控管 →		← 申請單位控管 →

子網段：用來區分不同的subnet，一個 /56 (子網段) 可細分256個 /64 subnet

108

IPv6 Subnetting



https://www.oreilly.com/library/view/ipv6-address-planning/9781491908211/ch04.html

109

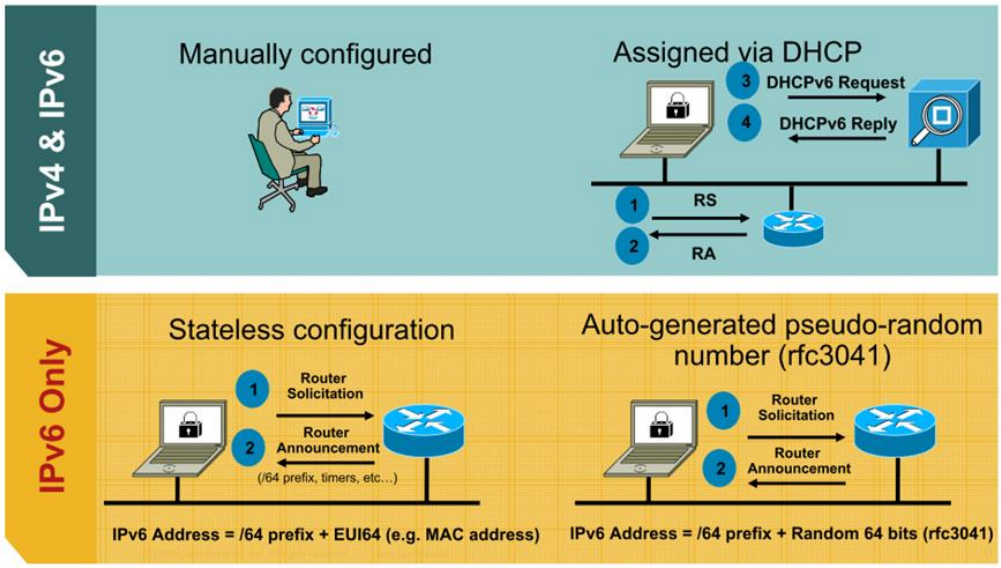
XXX大學網路 IPv6位址空間規劃建議範例

以地理位址劃分單位為範例

單位	分配網段	一個/56可配發的/64 樓層總數
教務處大樓	3FFE:BOOO:0000:0000::/56(配一個/56保留一個/56)	256
學務處大樓	3FFE:BOOO:0000:0200::/56 (配一個/56保留一個/56)	256
工學院大樓	3FFE:BOOO:0000:0400::/56 (配一個/56保留一個/56)	256
商學院大樓	3FFE:BOOO:0000:0600::/56 (配一個/56保留一個/56)	256
A棟大樓	3FFE:BOOO:0000:0800::/56	256
B棟大樓	3FFE:BOOO:0000:0900::/56(同上)	256
C棟大樓	3FFE:BOOO:0000:0a00::/56(同上)	256
D棟大樓	3FFE:BOOO:0000:0b00::/56(同上)	256
E棟大樓	3FFE:BOOO:0000:0c00::/56(同上)	256
以下依此類推	同上採循序分配原則配發	

110

IPv6升級作業- IPv6主機位址配發方式



Source: CISCO

IPv6升級作業-網路升級檢測

網路除錯通常使用 ping6 與 tracert6

如要進行此類測試，應事先檢查網路上相關設備是否已開放此類封包訊息傳送，如路由器、防火牆、伺服器、終端電腦等

如無法排除封包阻擋的問題，可以改用應用服務層協定(如port 80)進行測試

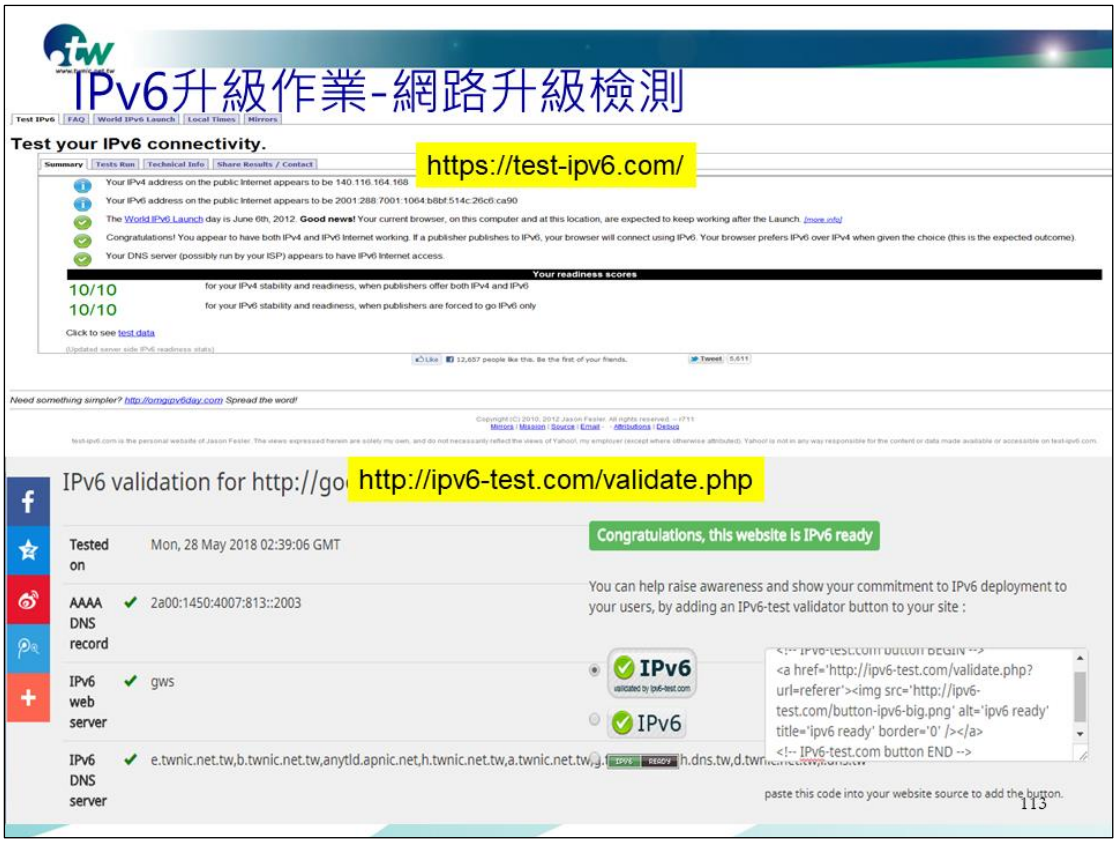
以下提供檢測IPv6能力的測試網站：

https://ipv6-test.com/validate.php

https://test-ipv6.com/

https://www.gsnv6.tw/inventory/checkservicepub.cgi

IPv6升級作業-網路升級檢測



113

小結

- 整體導入策略以盡量不影響使用者行為及不影響既有服務及供裝為目標
- 導入IPv6原則以『先網路，後服務』、『公眾網路優先，封閉網路次之』以及『由小而大，由點逐步擴展至面』
  - 相關網路應該利用設備汰換，順勢引進IPv6，以不大幅增加額外導入資本支出成本為目標
  - 新建之服務必須提供IPv6能力，以因應未來可能的需求

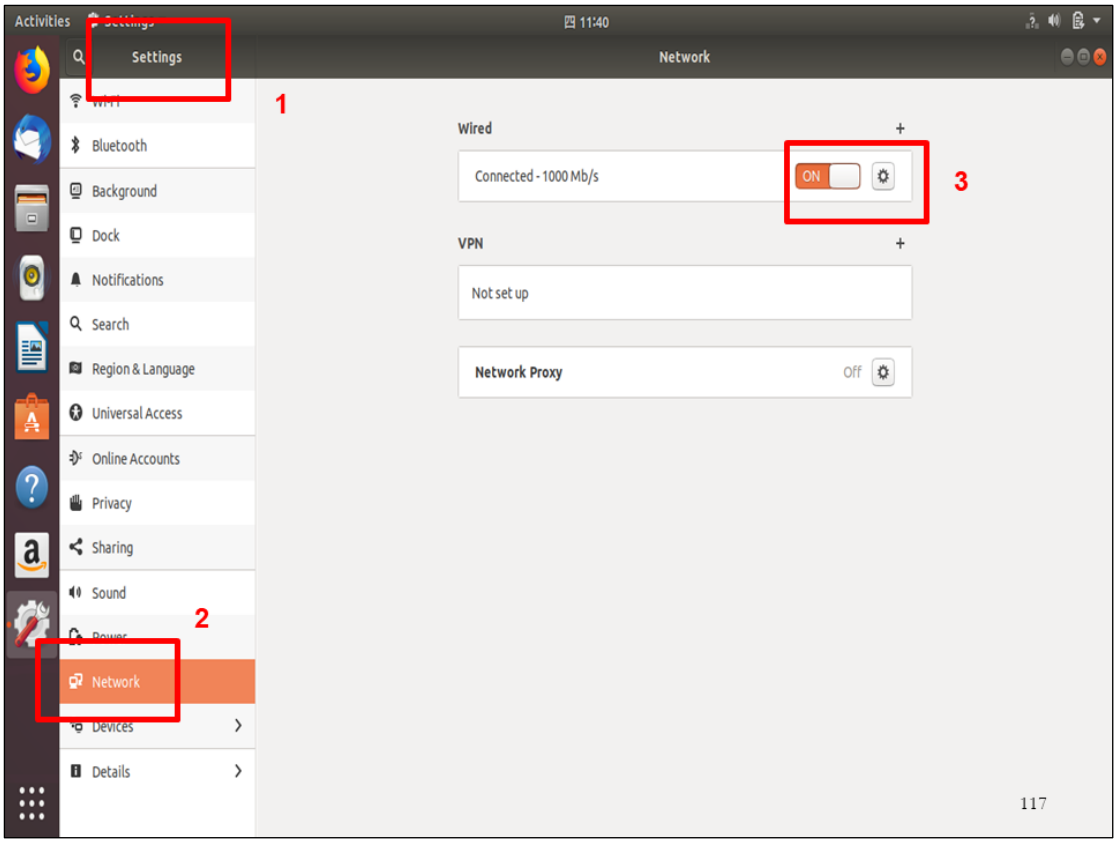
114

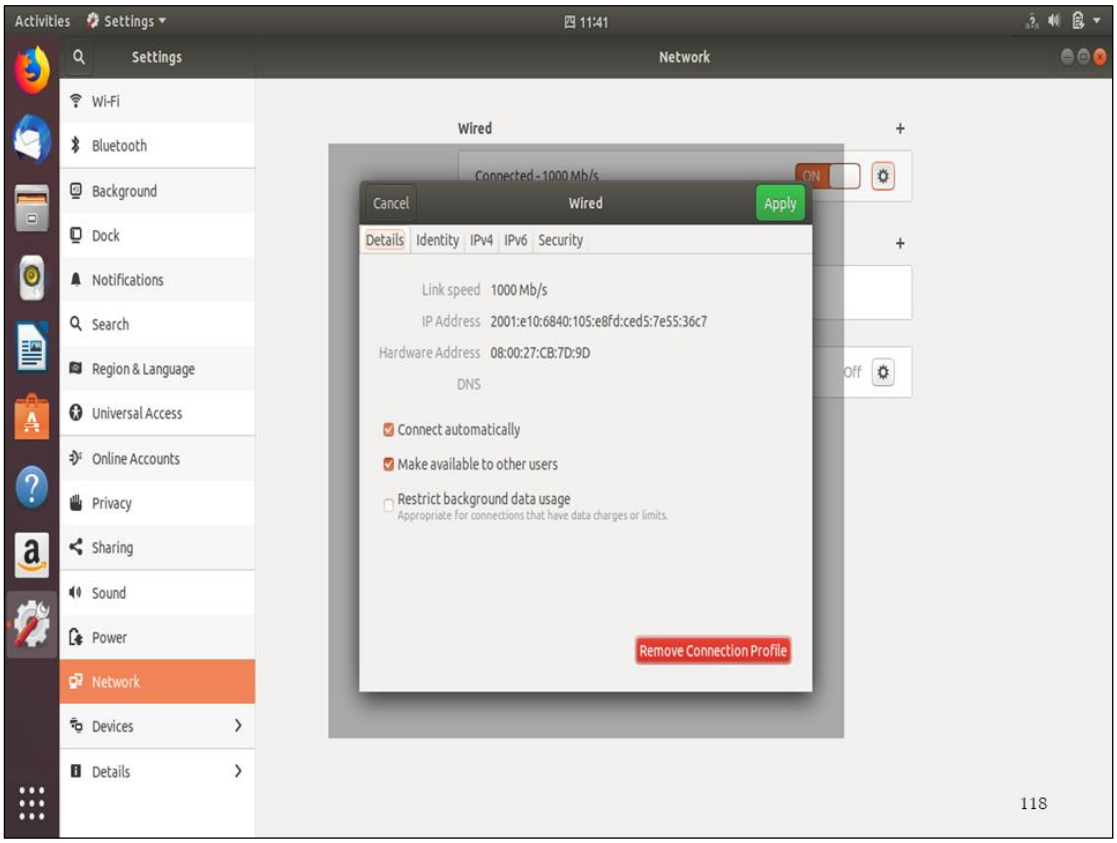
點進網域新視界！

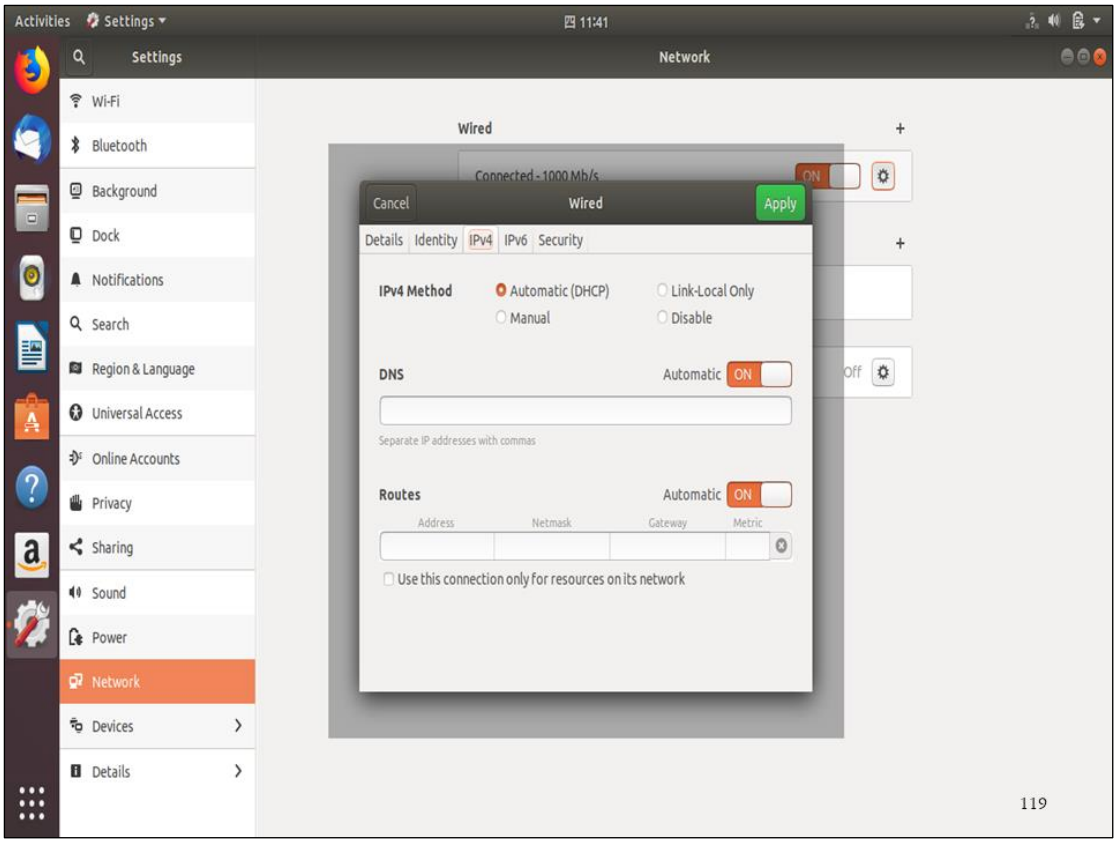
作業系統與網站升級建置範例

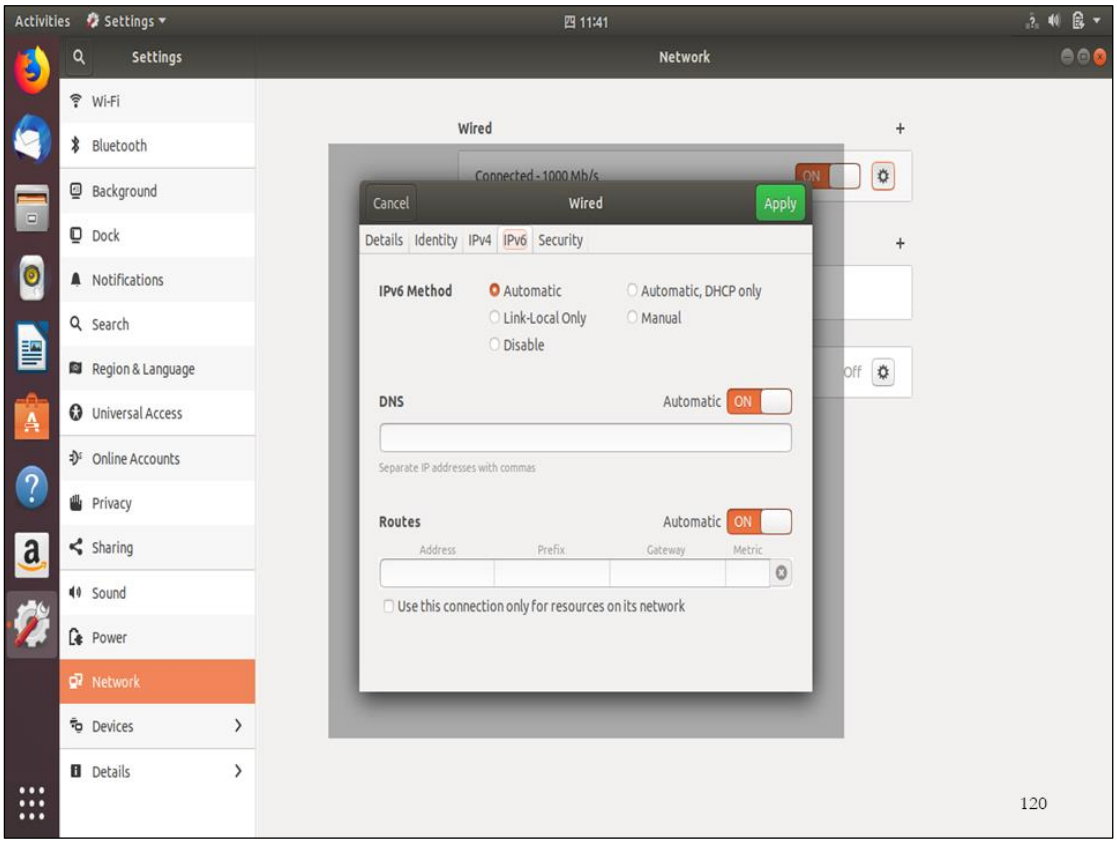
點進網域新視界！

IPv6建置 Ubuntu 作業系統


Activities
11:40
Settings
Network
1
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
2
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
3
VPN
Not set up
Network Proxy
Off
117

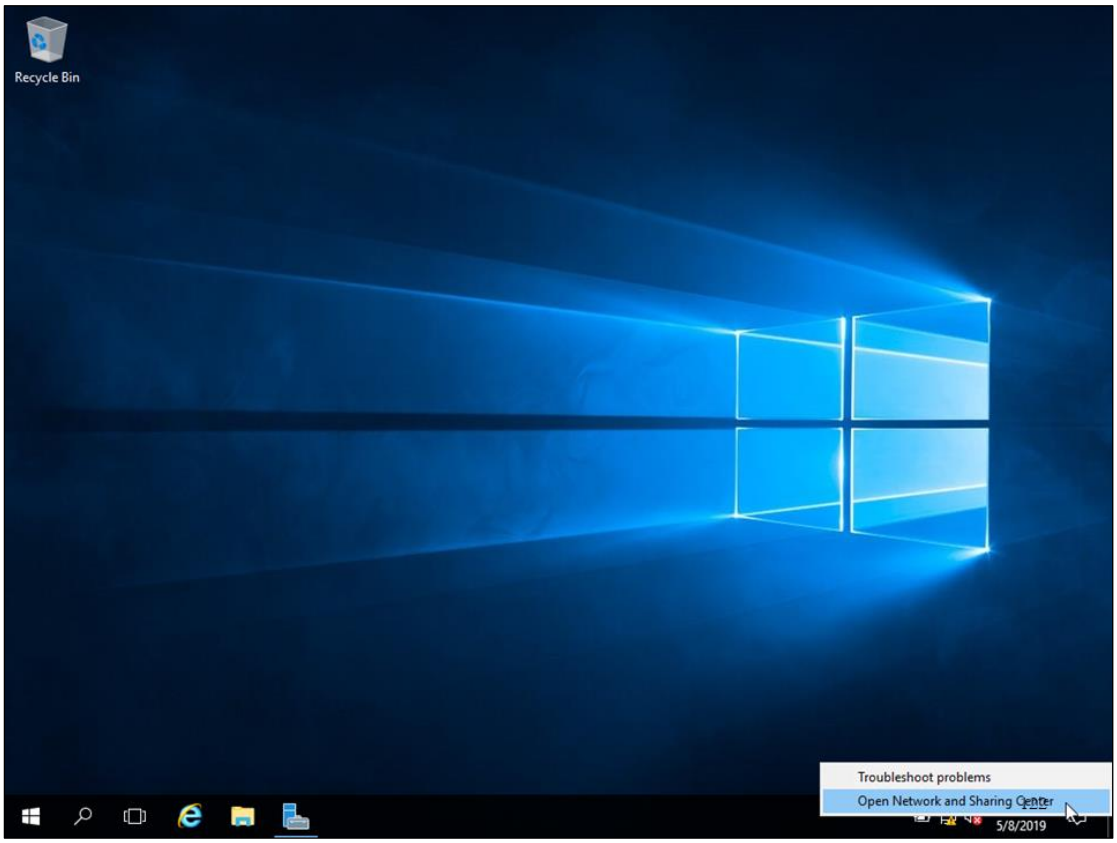

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile
Off
118

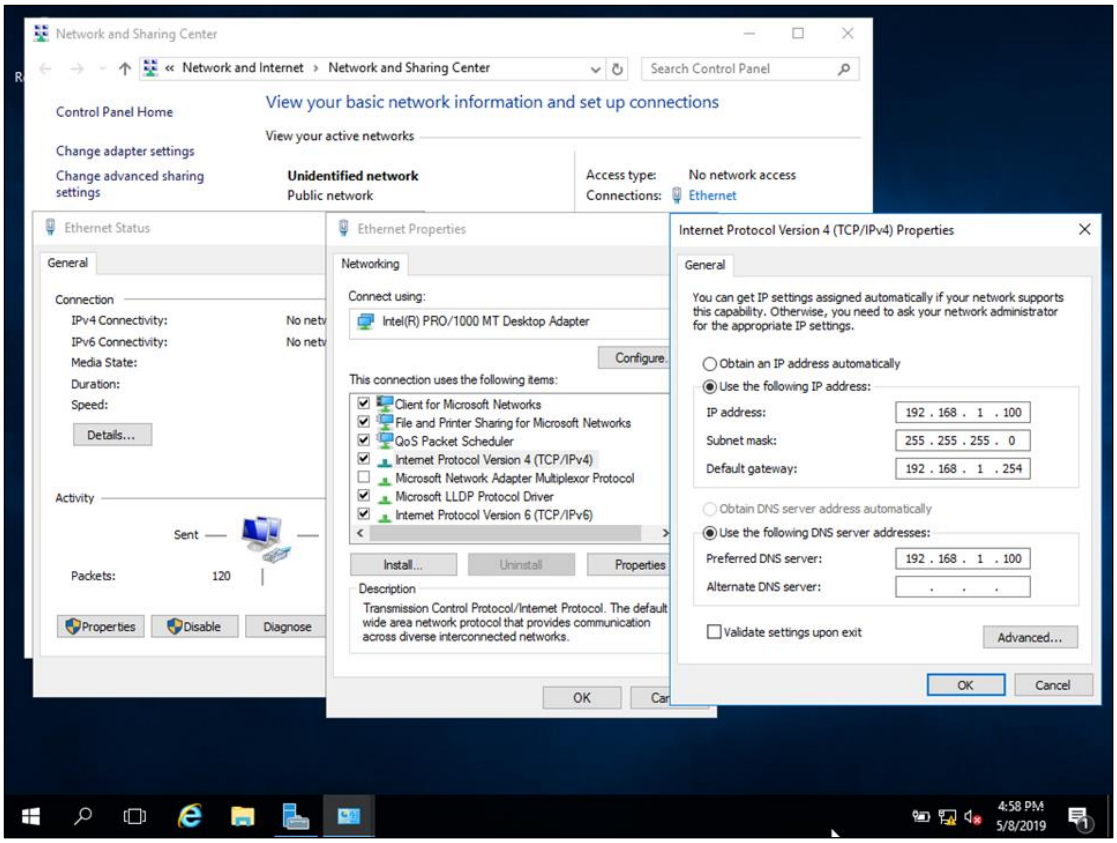

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Method
Automatic (DHCP)
Link-Local Only
Manual
Disable
DNS
Automatic
ON
Separate IP addresses with commas
Routes
Automatic
ON
Address
Netmask
Gateway
Metric
Use this connection only for resources on its network
119

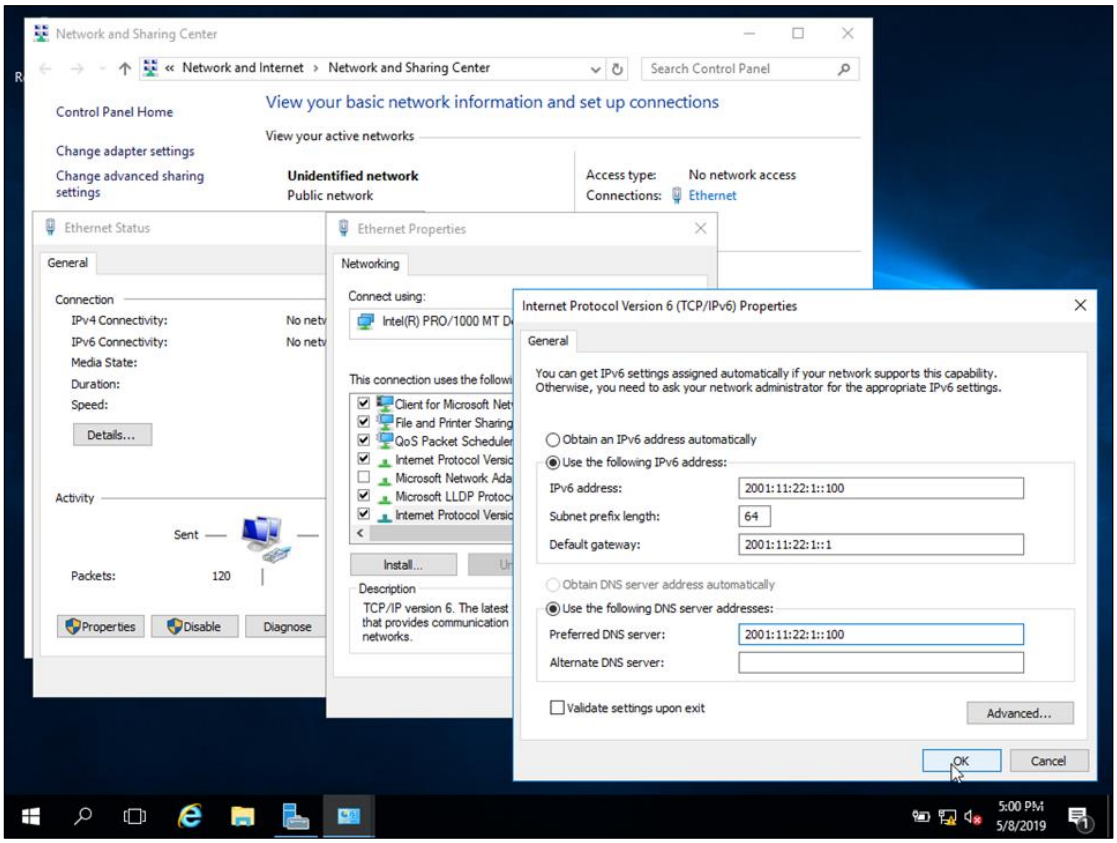

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv6 Method
Automatic
Automatic, DHCP only
Link-Local Only
Manual
Disable
DNS
Automatic
ON
Separate IP addresses with commas
Routes
Automatic
ON
Address
Prefix
Gateway
Metric
Use this connection only for resources on its network
120

點進網域新視界！

IPv6建置
Windows server 2016
作業系統

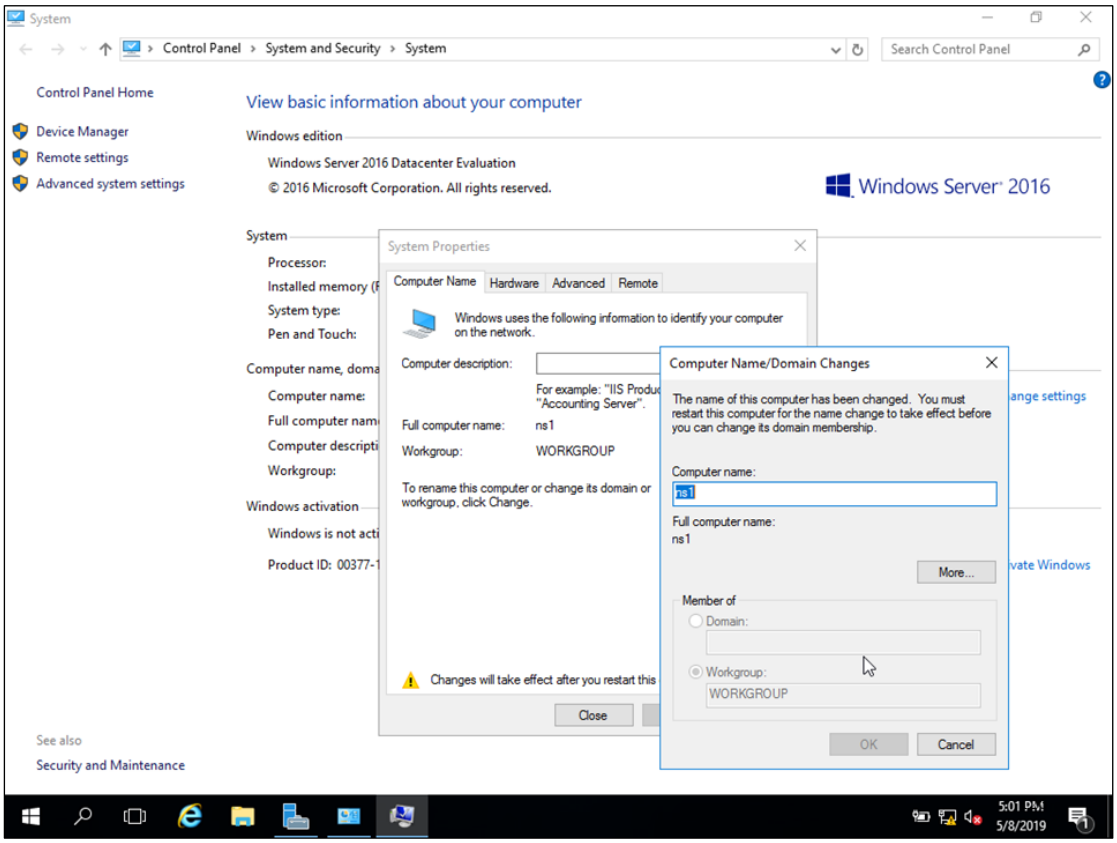


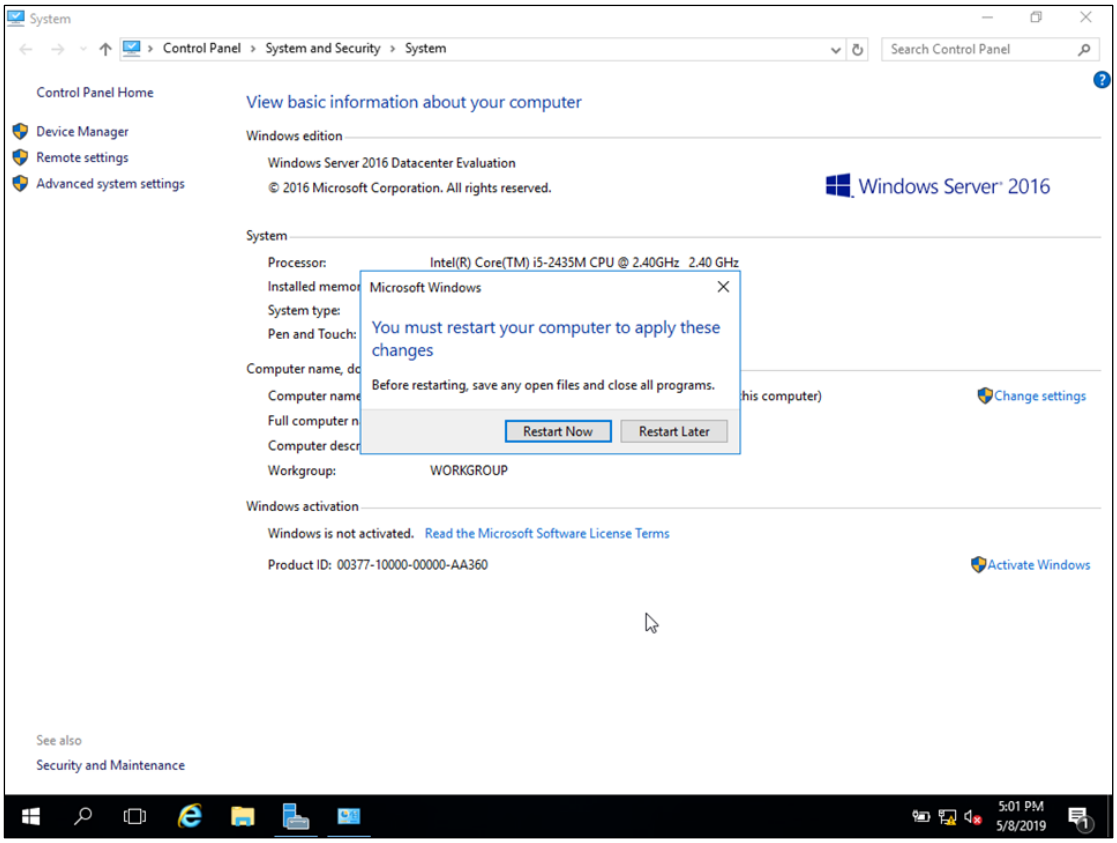

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
View your basic network information and set up connections
Control Panel Home
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
4:58 PM
5/8/2019

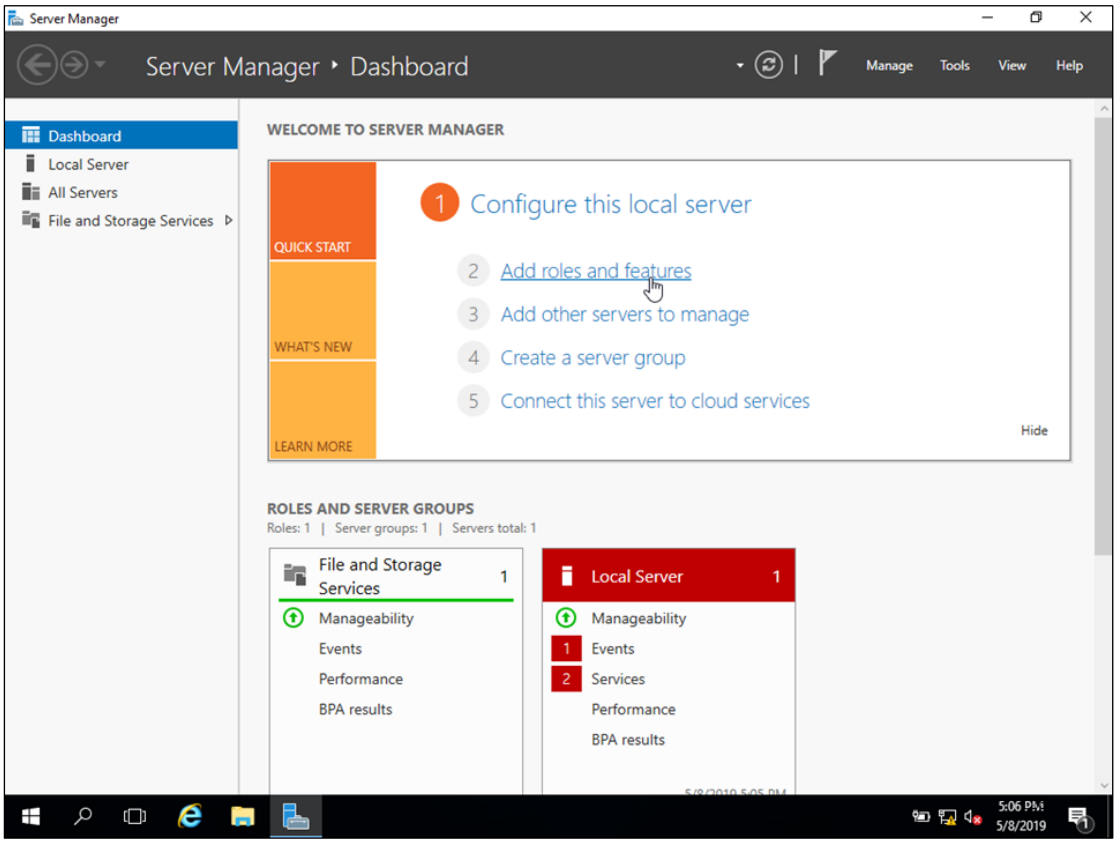

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
View your basic network information and set up connections
Control Panel Home
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT D
This connection uses the followi
Client for Microsoft Net
File and Printer Sharing
QoS Packet Scheduler
Internet Protocol Versio
Microsoft Network Ada
Microsoft LLDP Protoc
Internet Protocol Versio
Install...
Description
TCP/IP version 6. The latest that provides communication networks.
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: 2001:11:22:1::100
Subnet prefix length: 64
Default gateway: 2001:11:22:1::1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 2001:11:22:1::100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
5:00 PM
5/8/2019

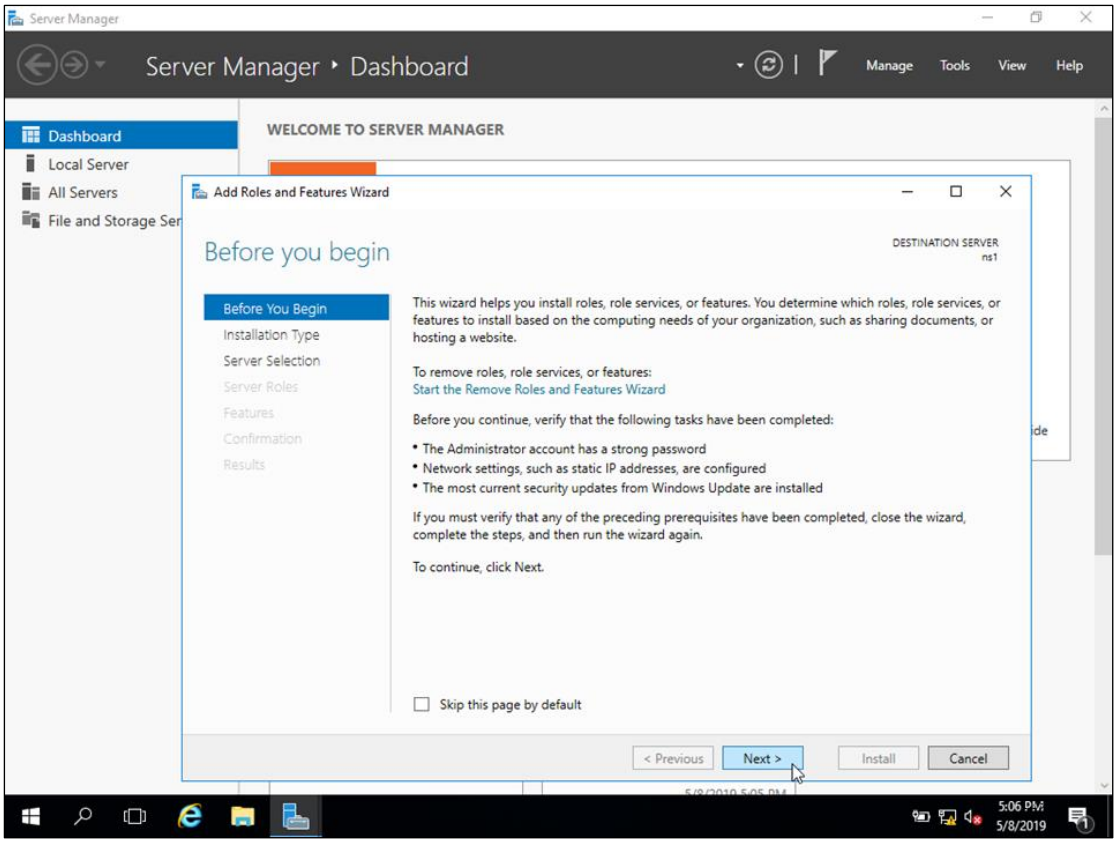
點進網域新視界！

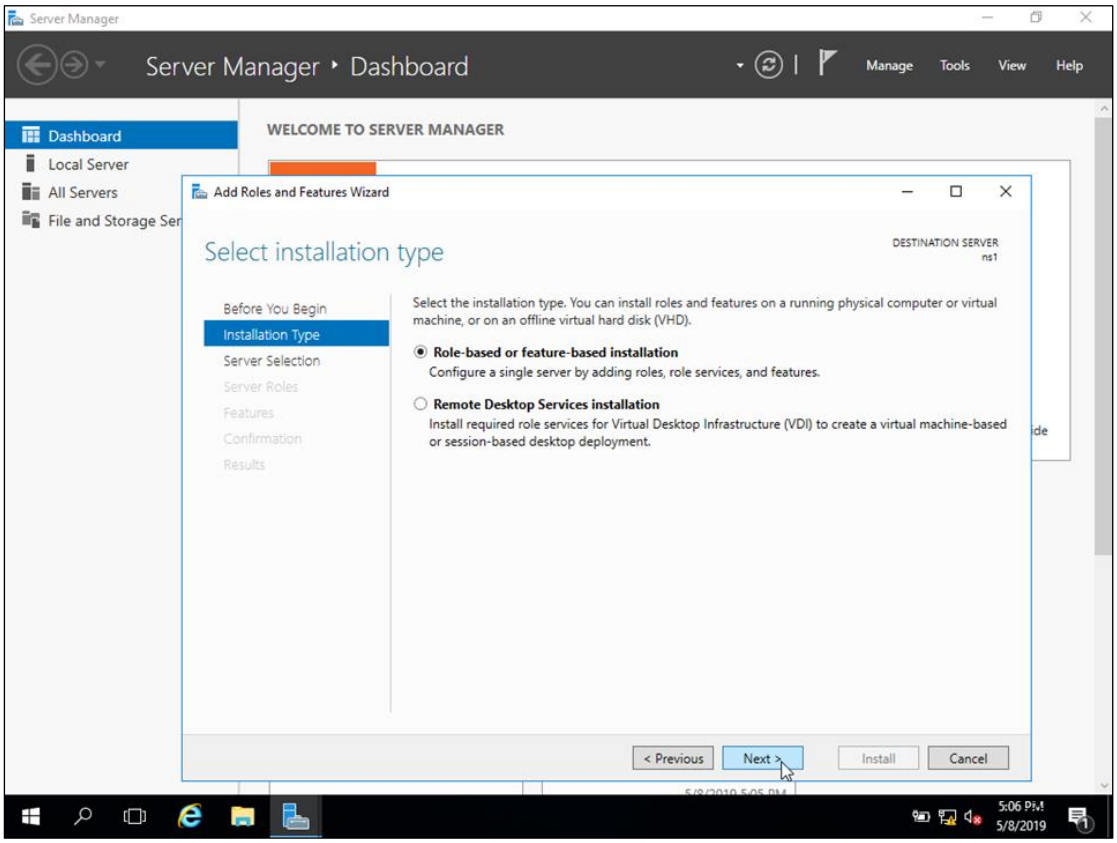
IPv6建置
DNS Server

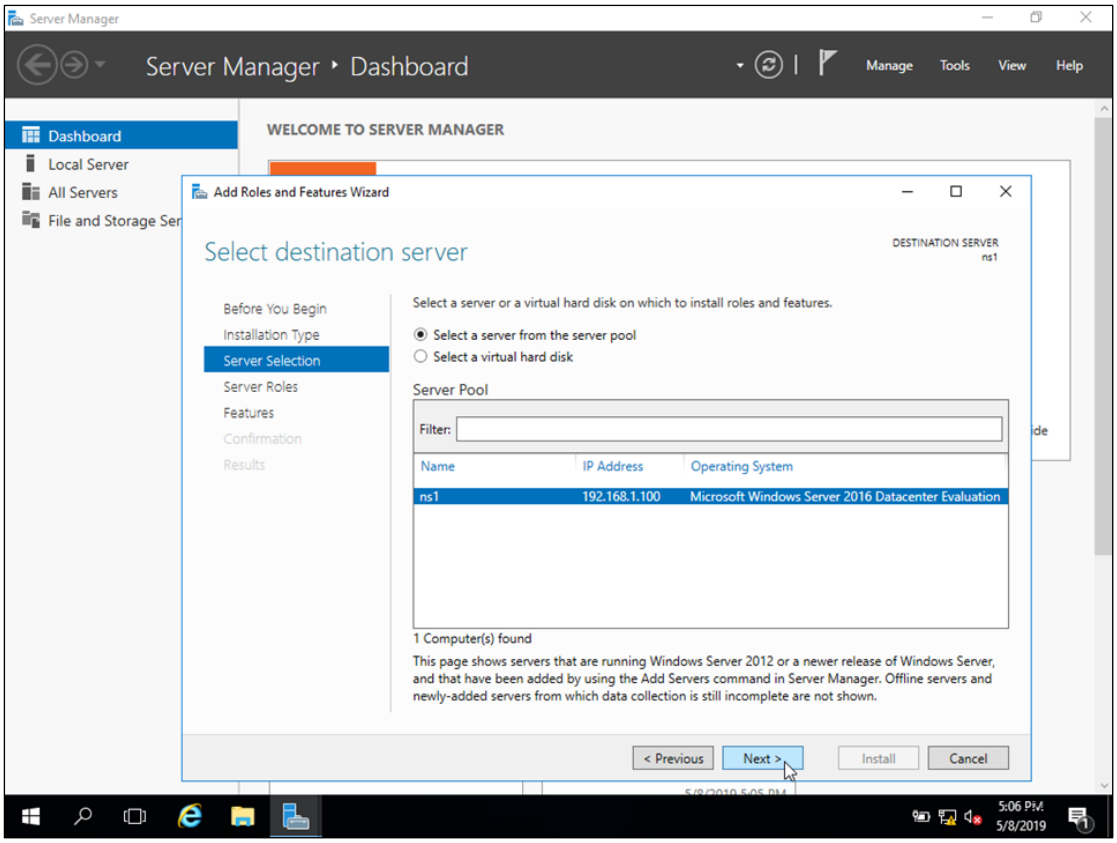


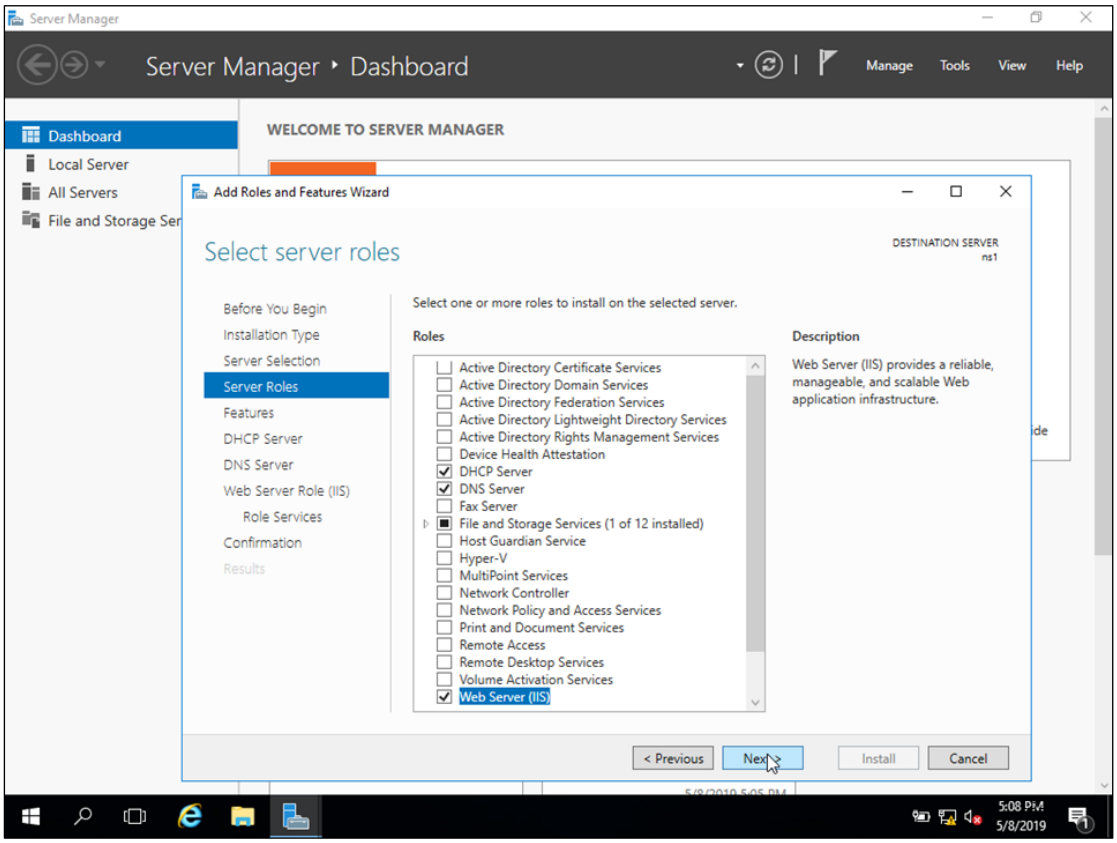

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor: Intel(R) Core(TM) i5-2435M CPU @ 2.40GHz 2.40 GHz
Microsoft Windows
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
Restart Now
Restart Later
Change settings
Workgroup: WORKGROUP
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-10000-00000-AA360
Activate Windows
See also
Security and Maintenance
5:01 PM
5/8/2019

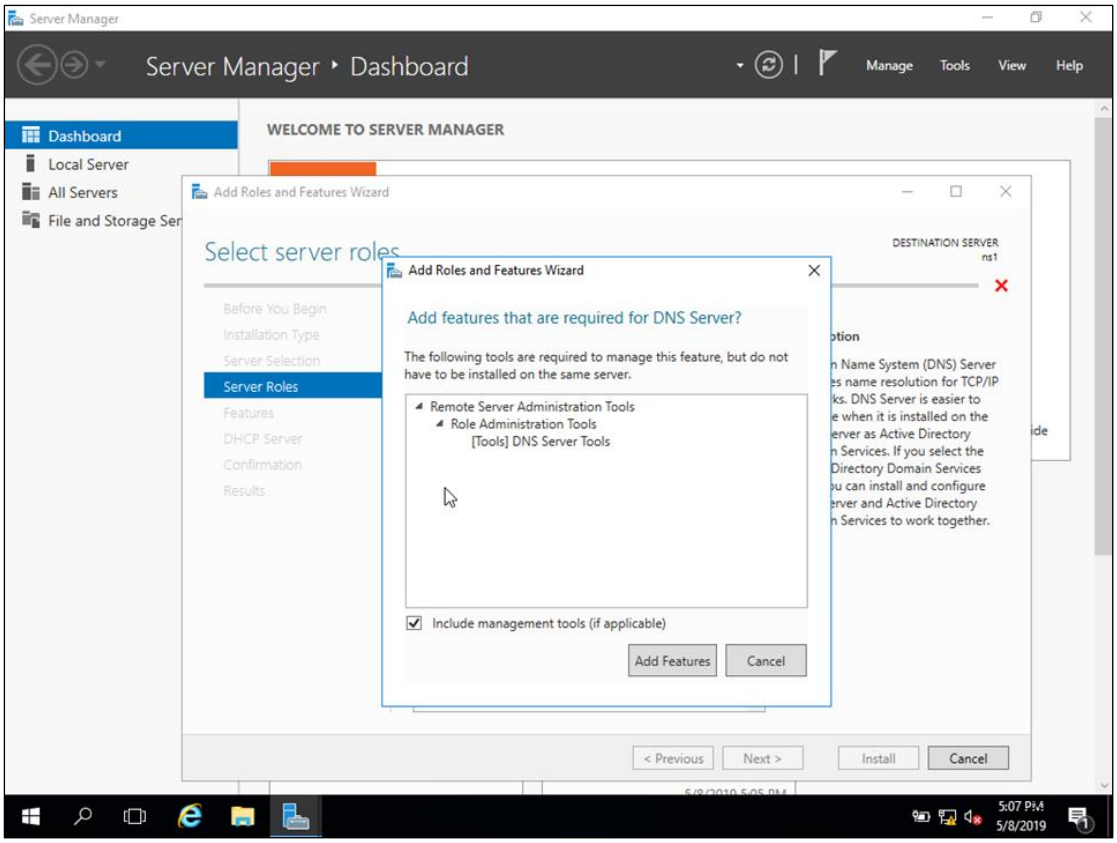

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
5:06 PM
5/8/2019

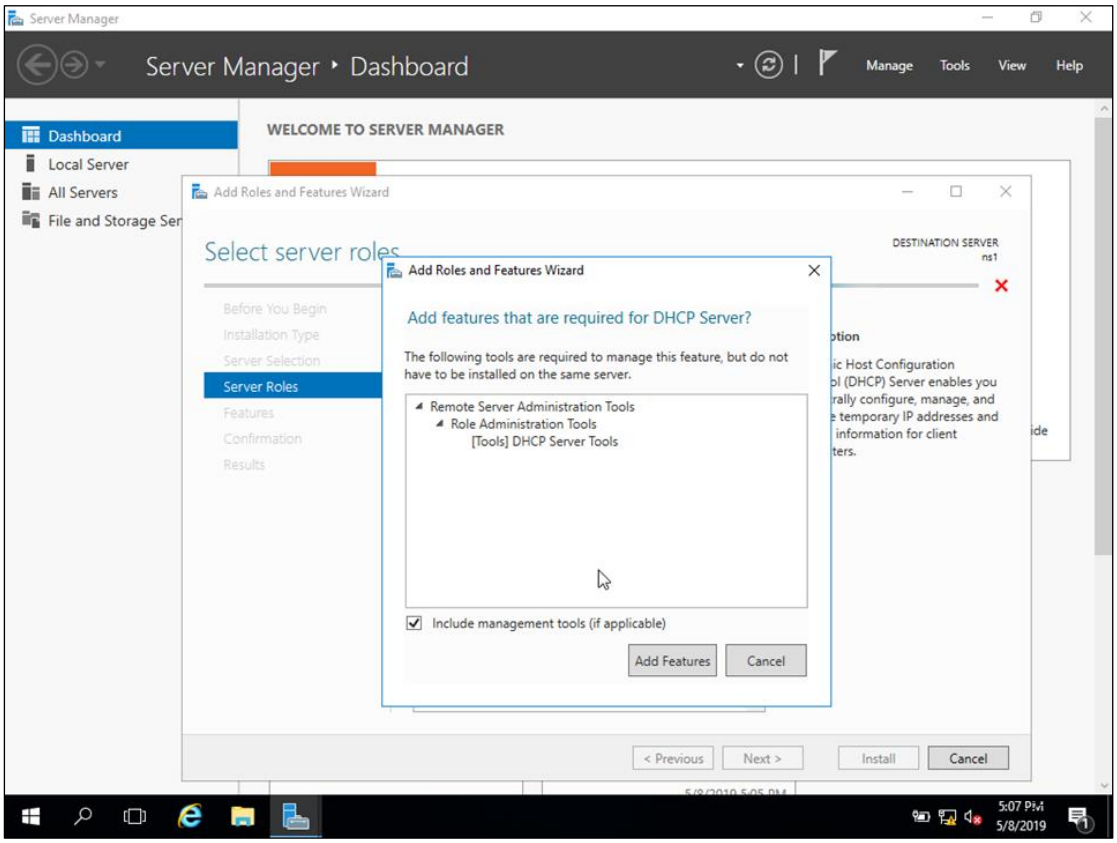

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

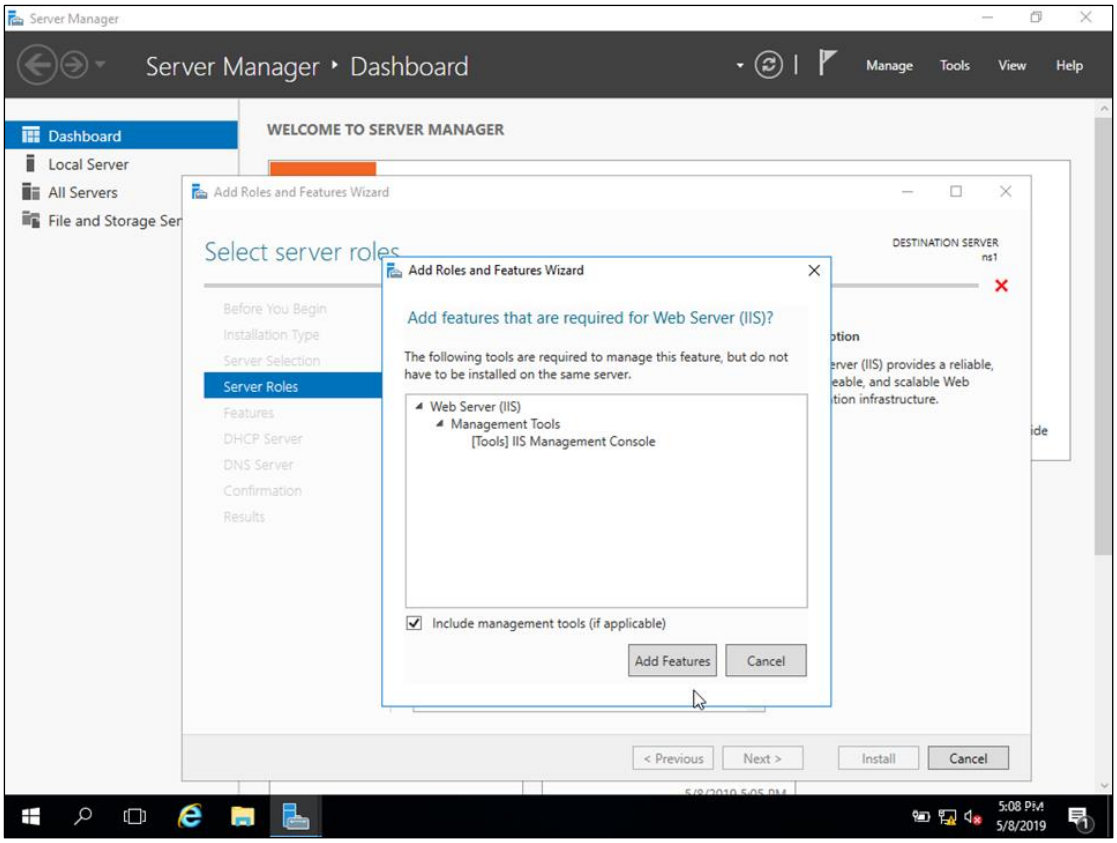

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

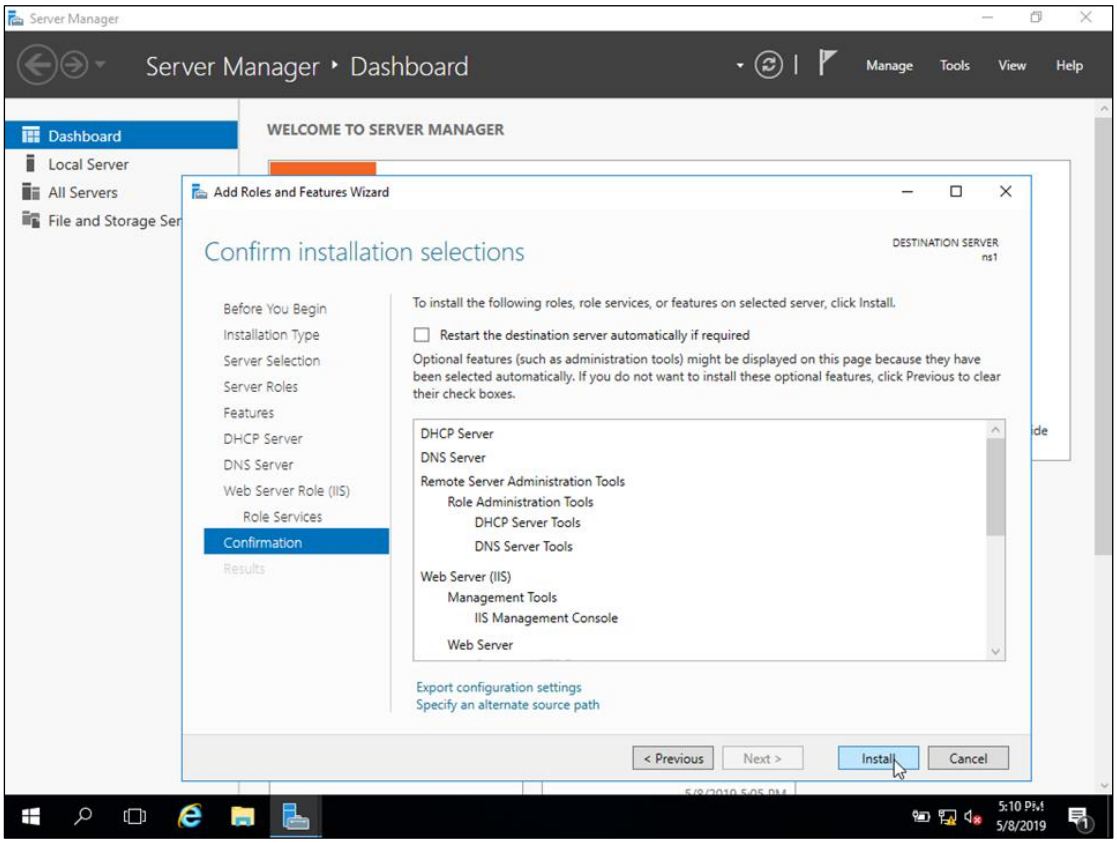

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
ns1
192.168.1.100
Microsoft Windows Server 2016 Datacenter Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

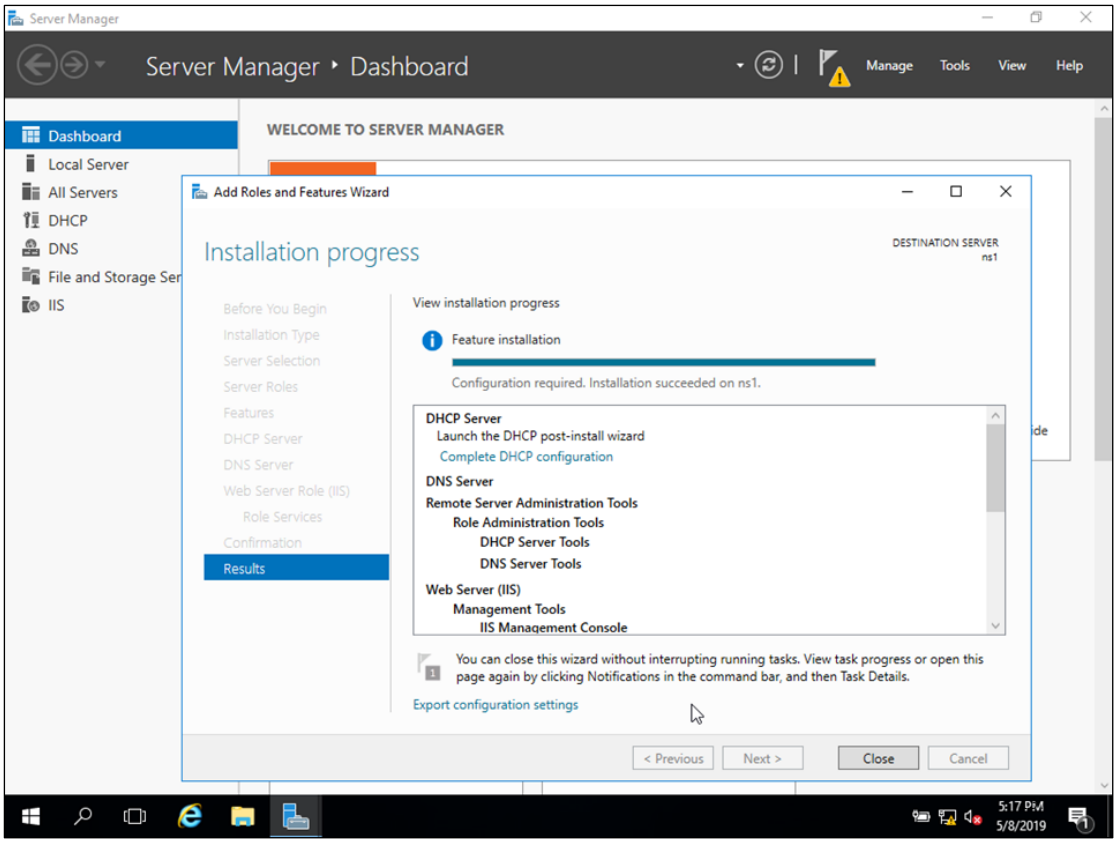

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

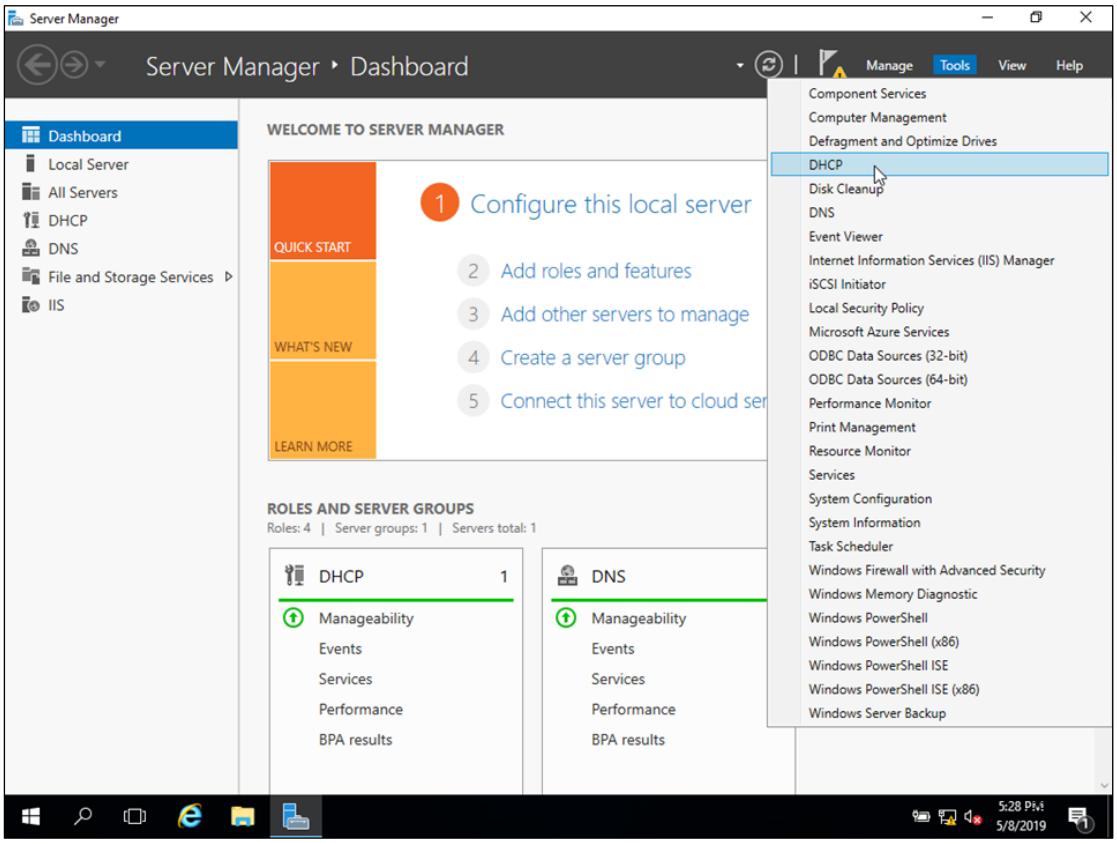

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

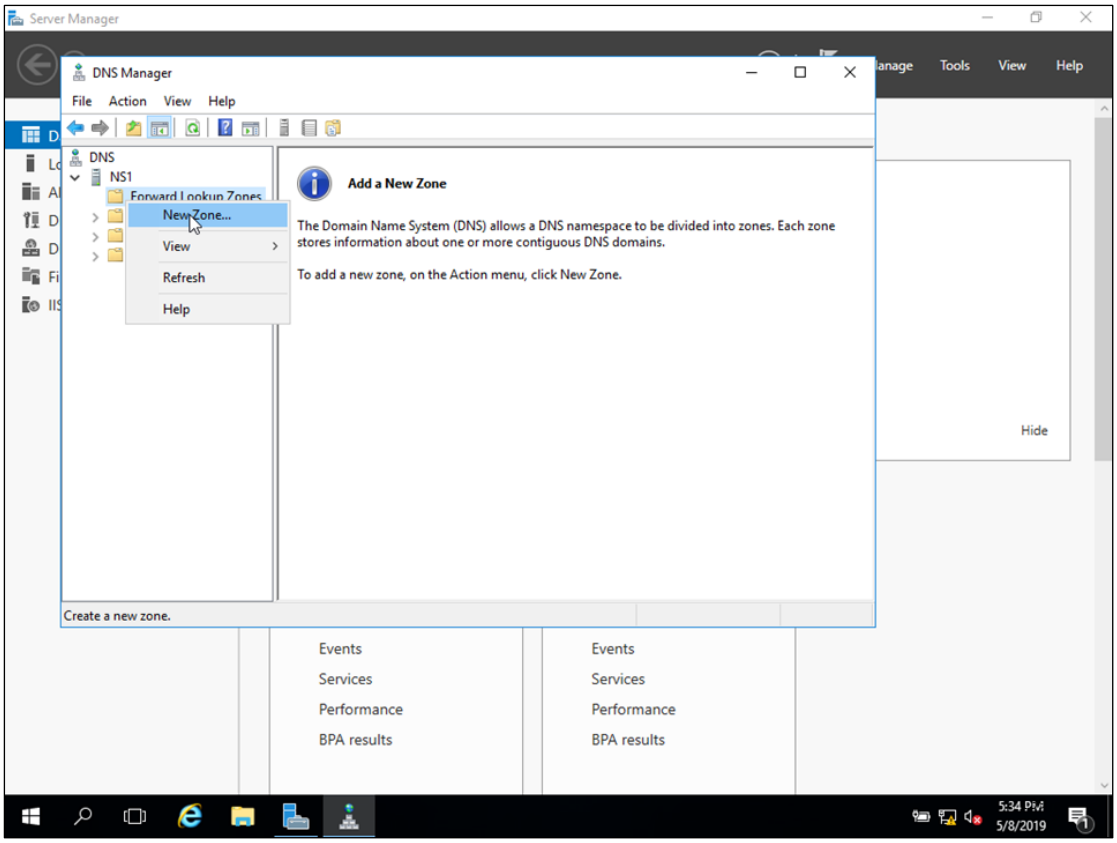

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

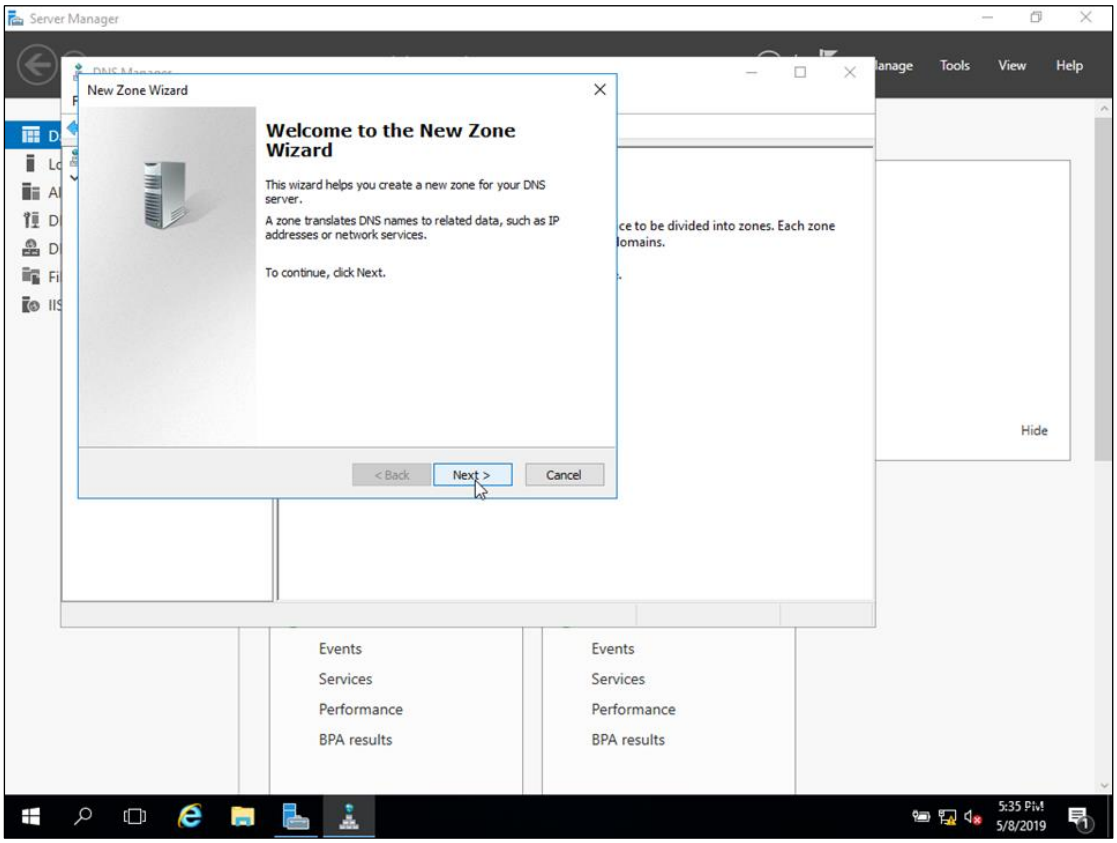

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

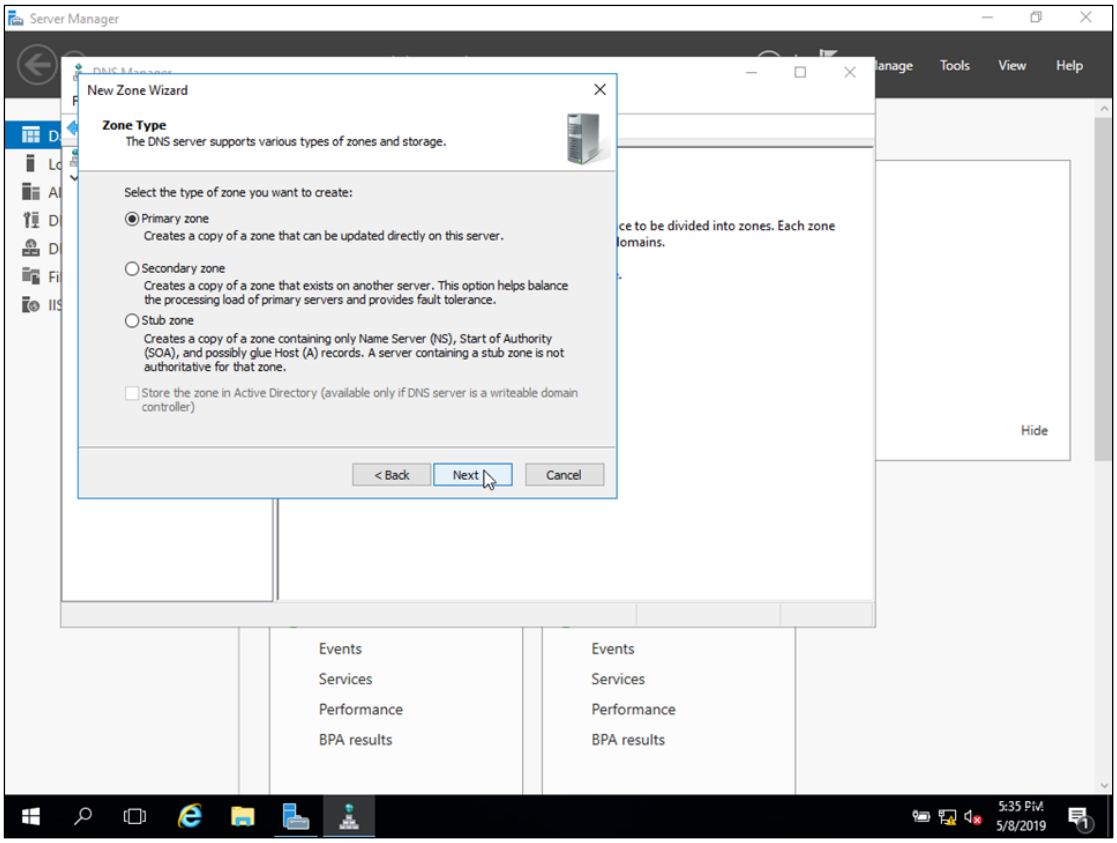

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
DHCP Server
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
5:10 PM
5/8/2019

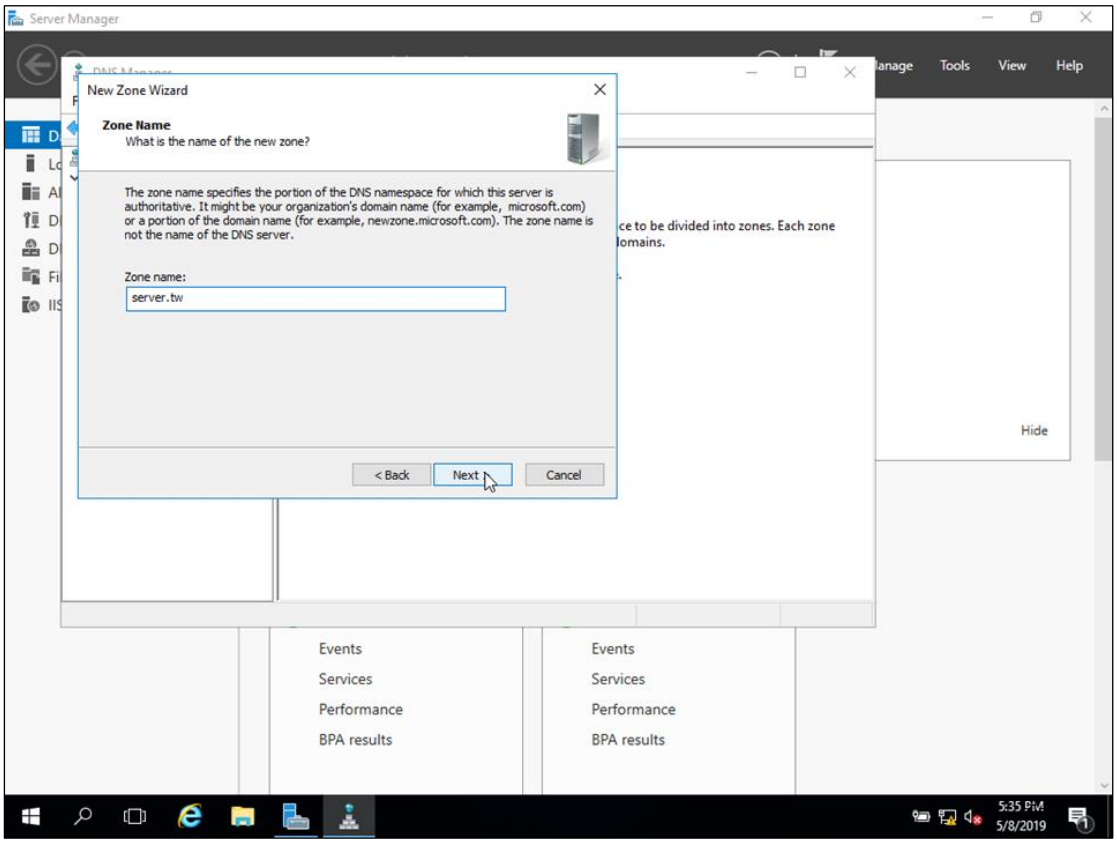

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Ser
IIS
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on ns1.
DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
5:17 PM
5/8/2019

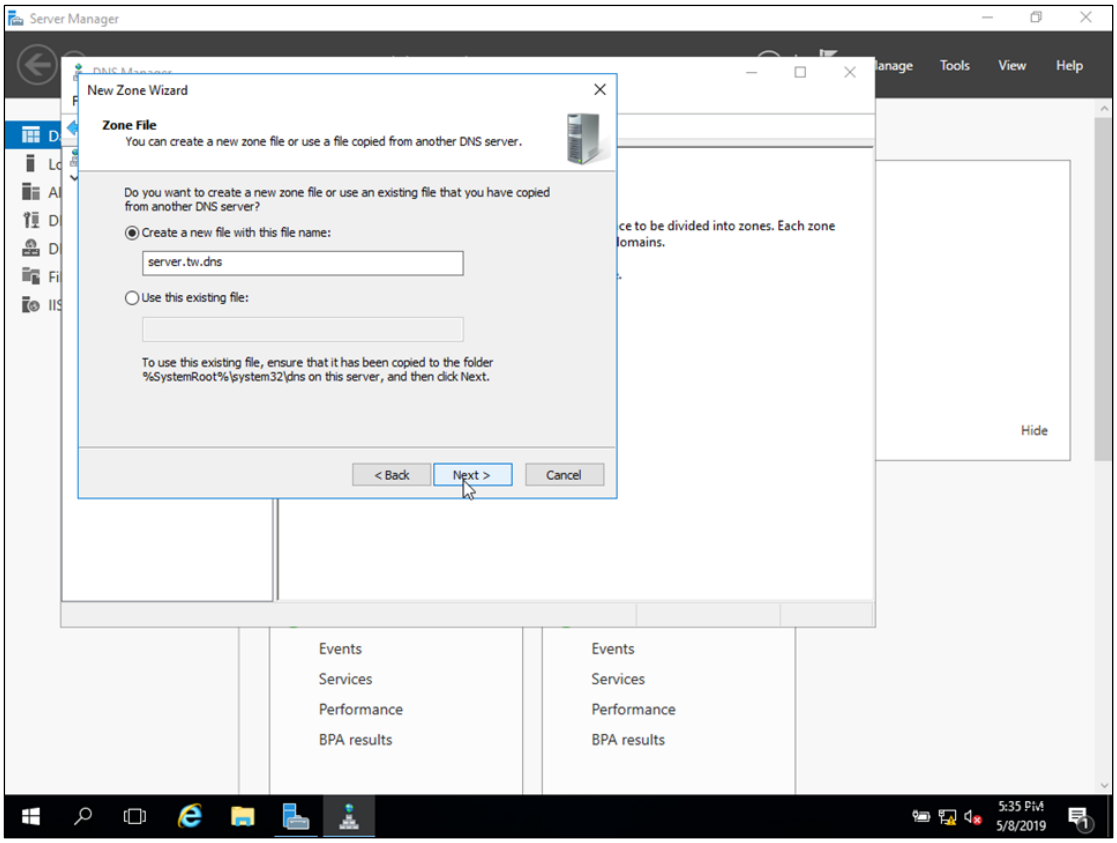

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud ser
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
DHCP 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
5:28 PM
5/8/2019

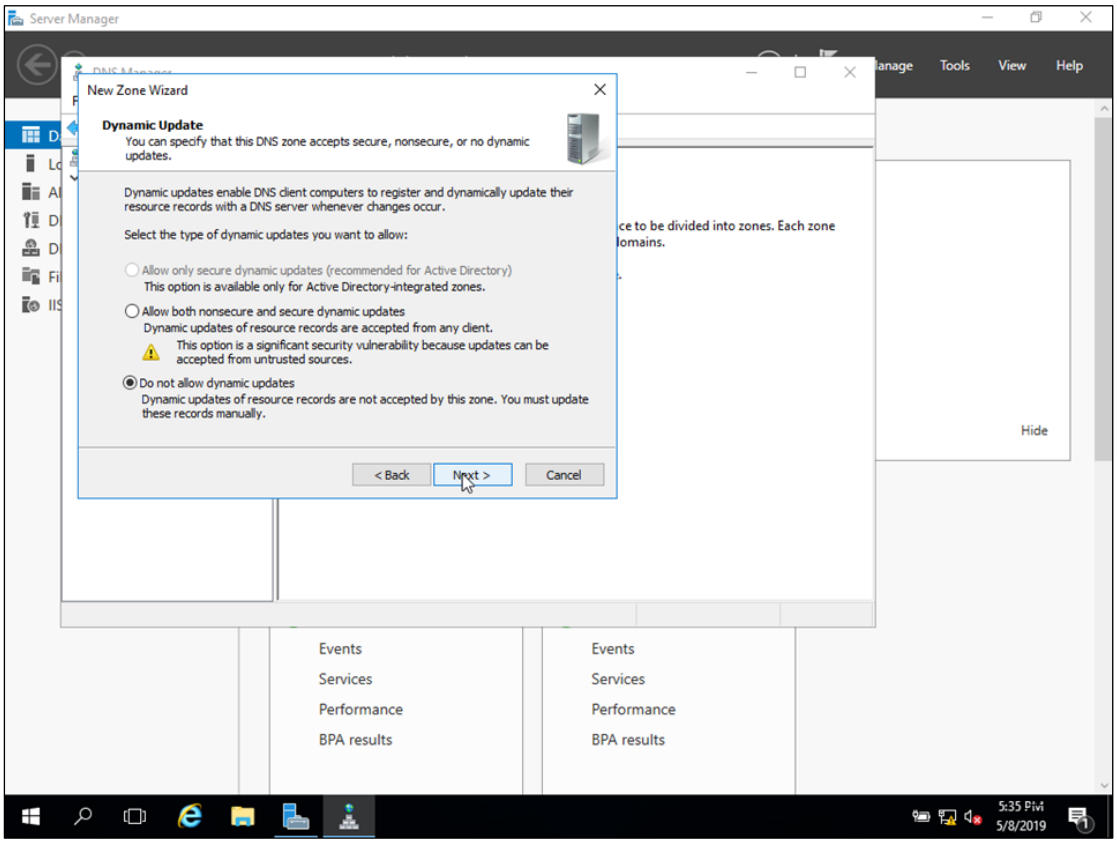

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
To add a new zone, on the Action menu, click New Zone.
Create a new zone.
Events
Services
Performance
BPA results
Hide
5:34 PM
5/8/2019

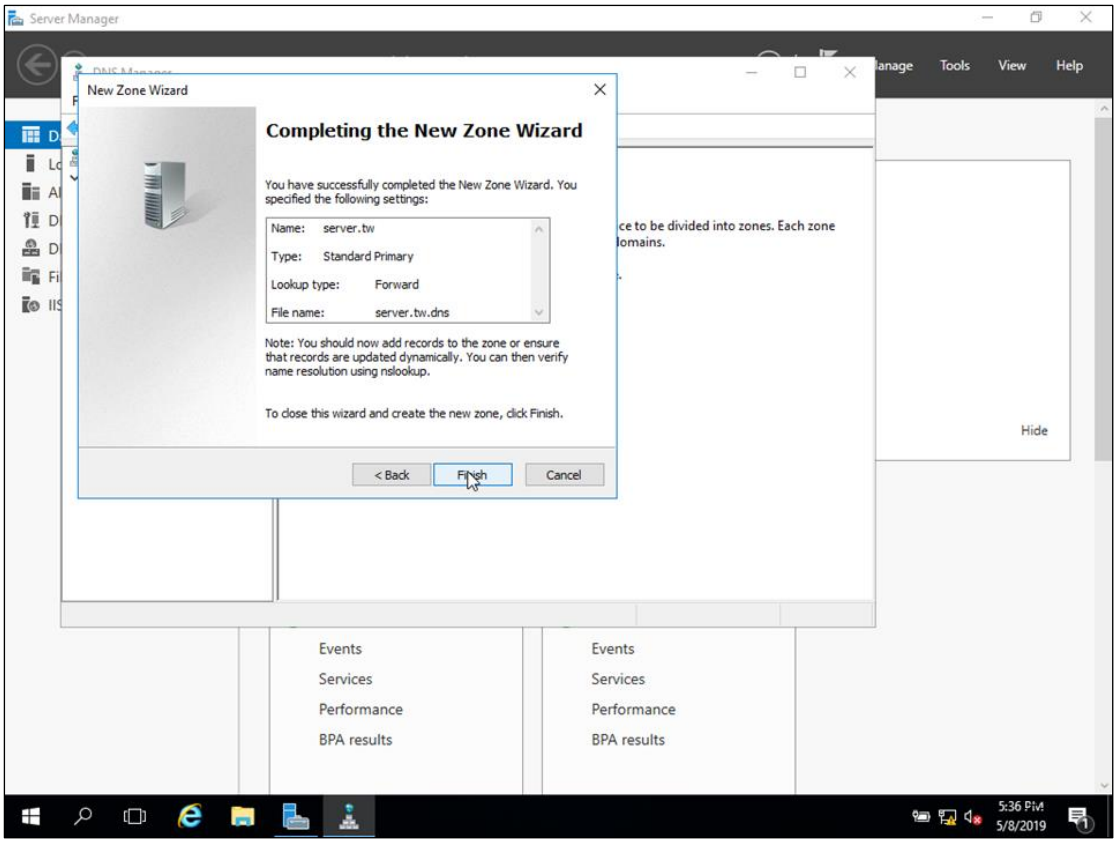

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Events
Services
Performance
BPA results
Hide
5:35 PM
5/8/2019

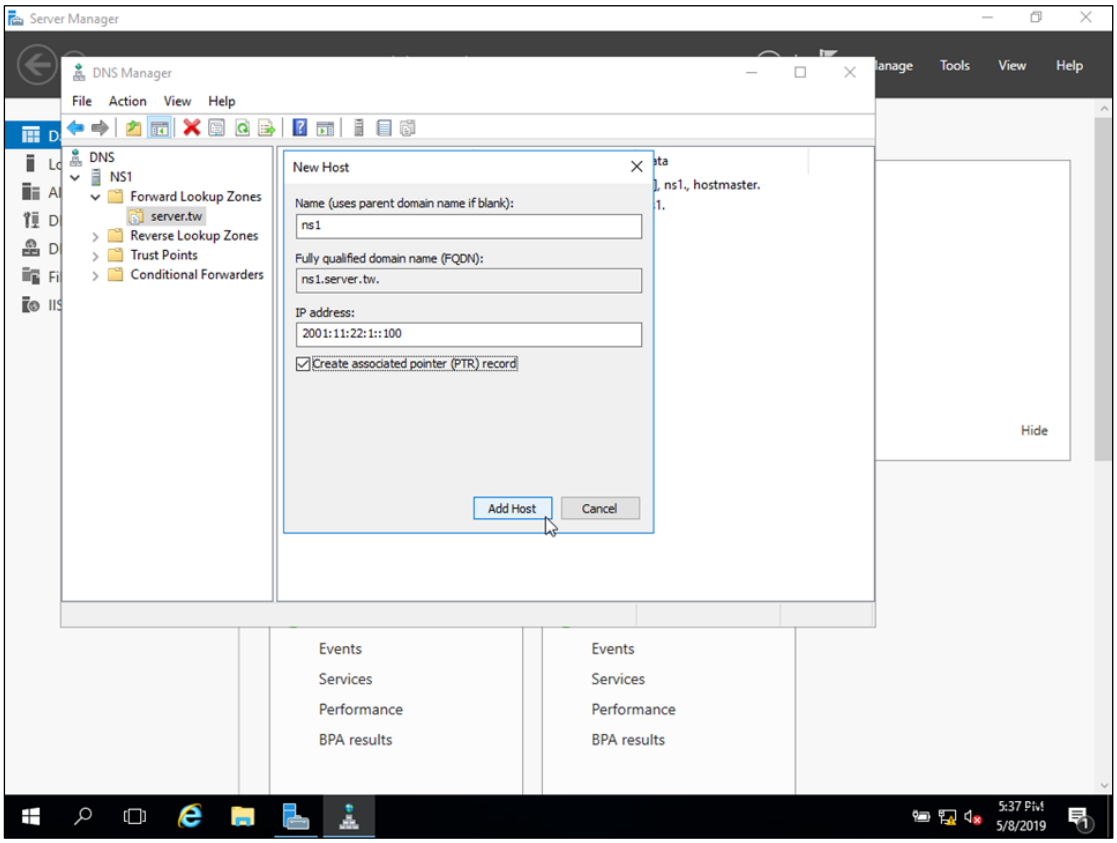

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

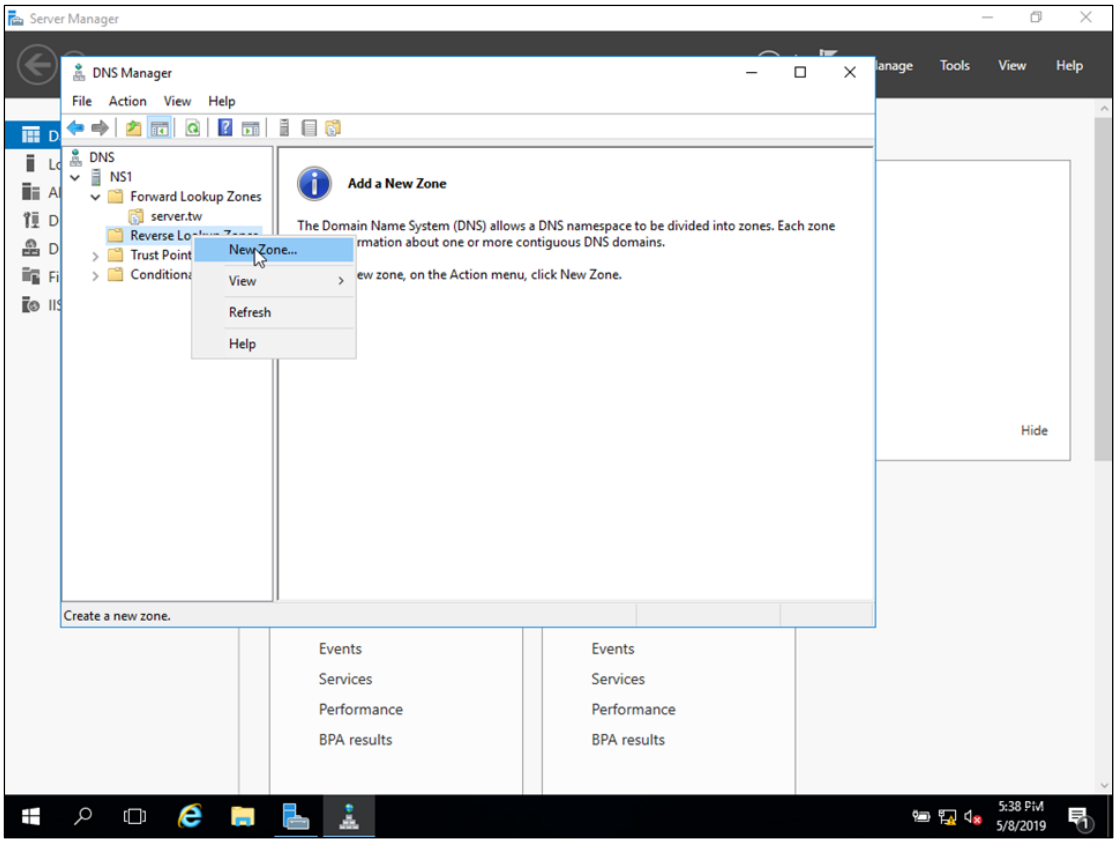

Server Manager
Tools
View
Help
New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
server.tw
< Back
Next
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

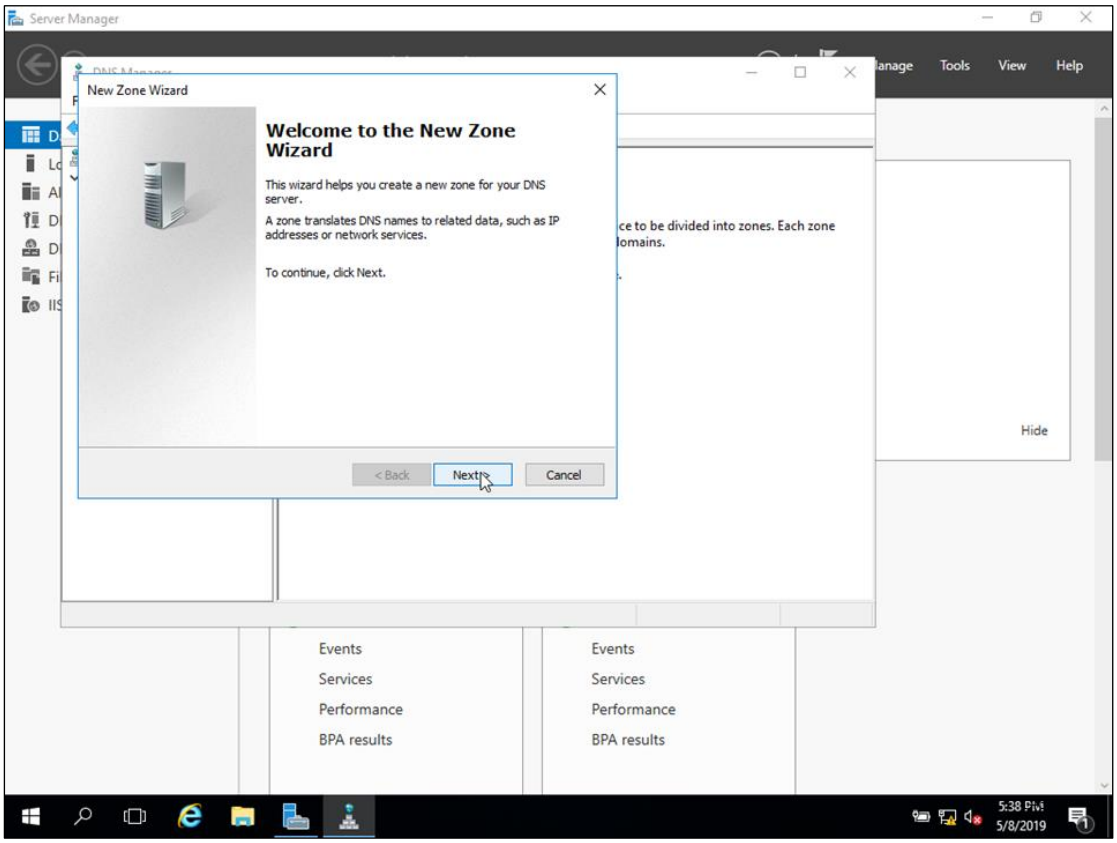

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
server.tw.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

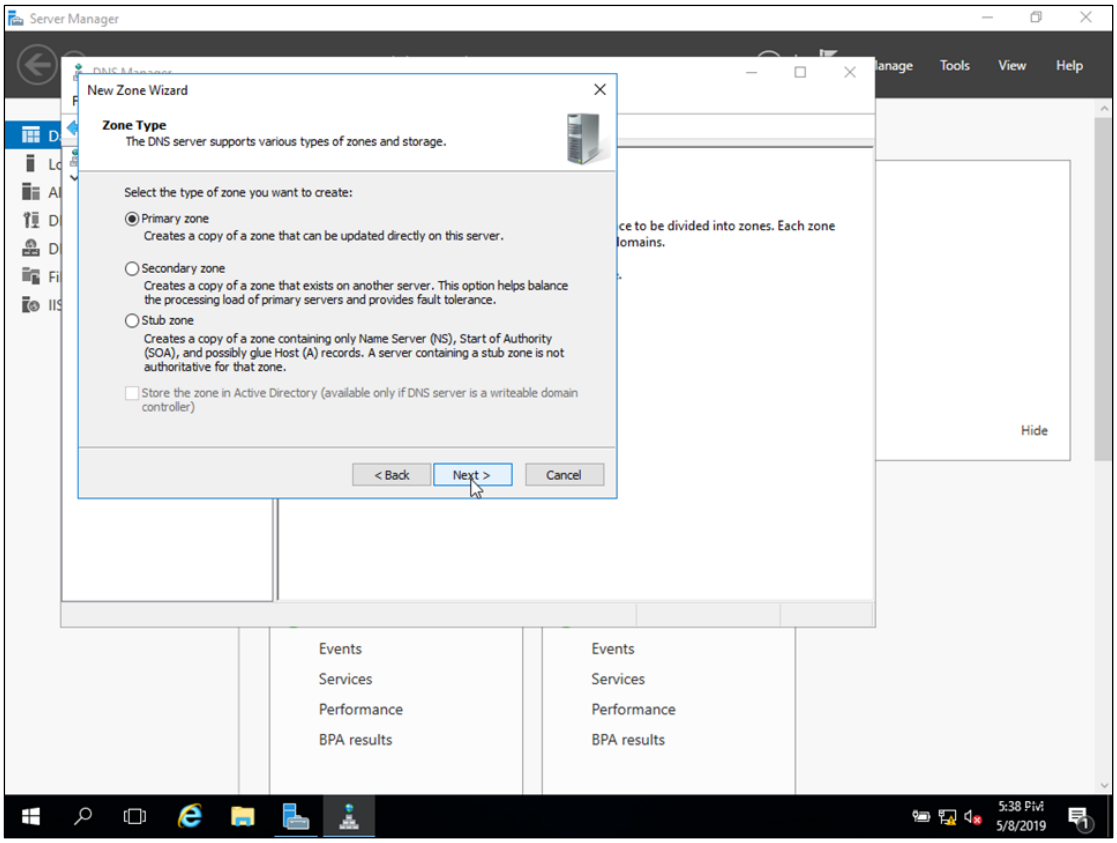

Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

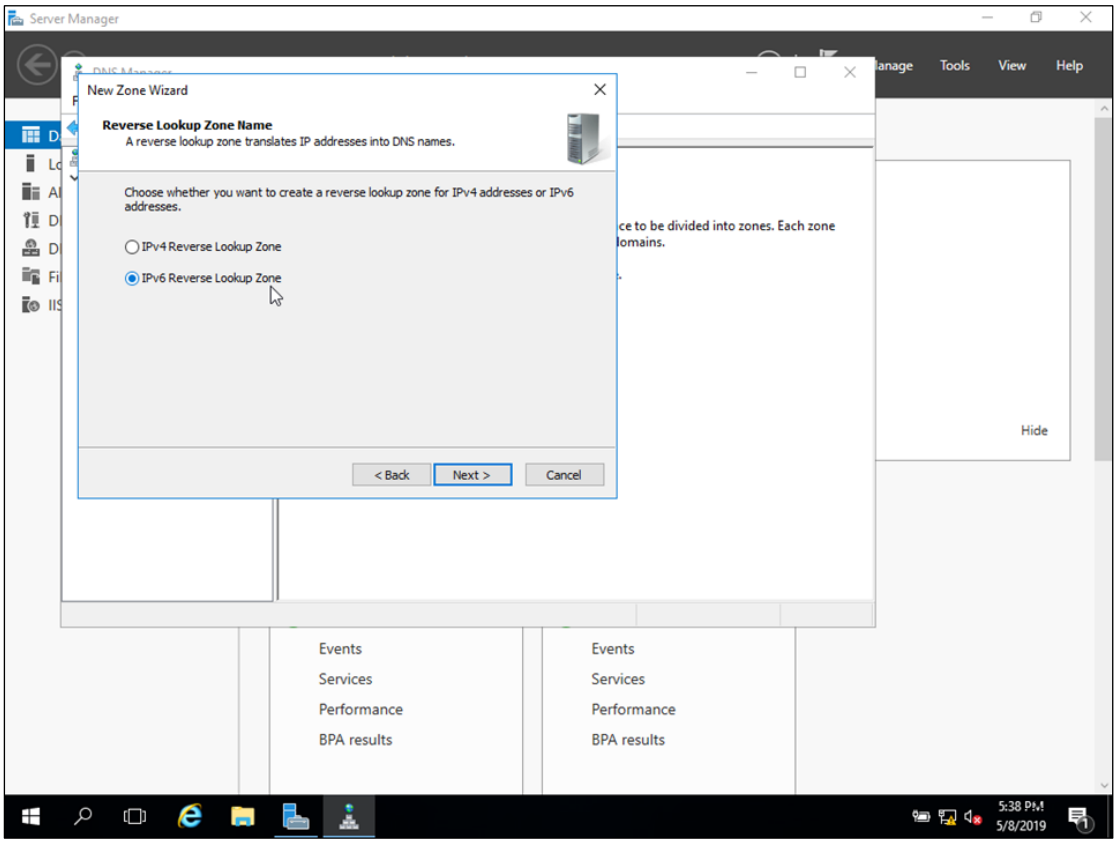

Server Manager
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

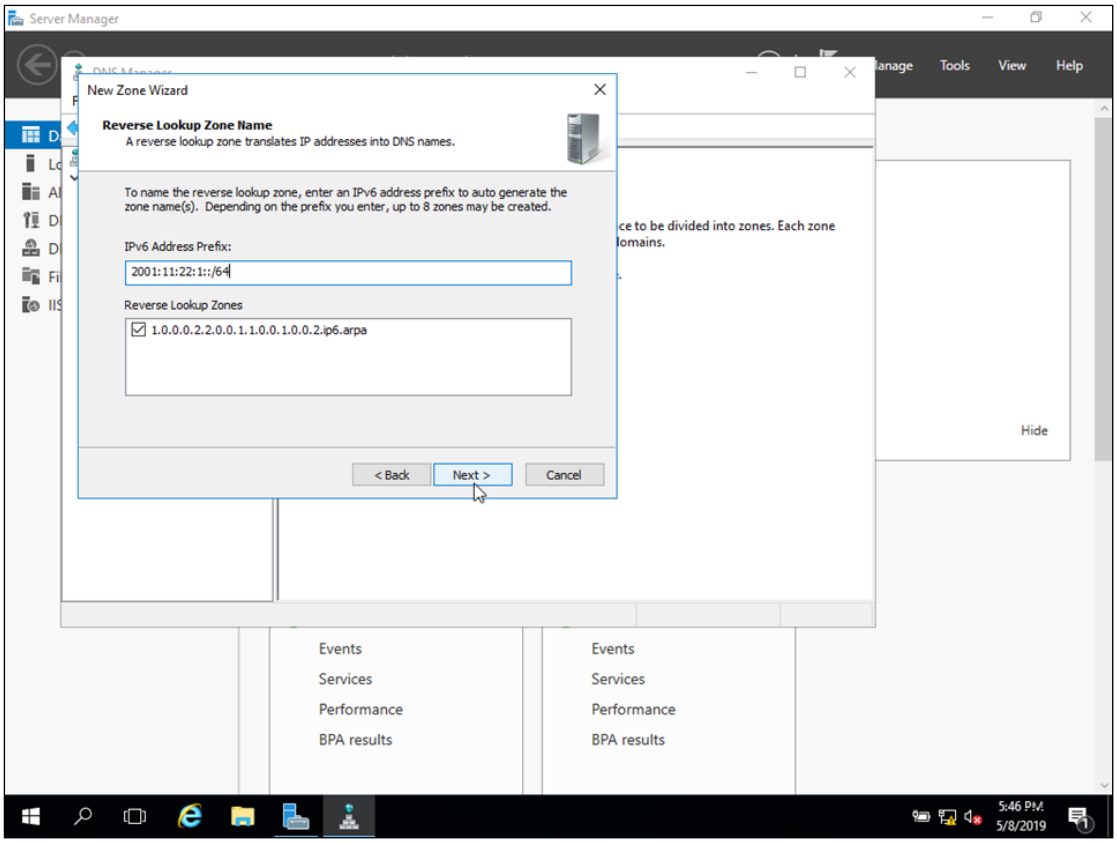

Server Manager
DNS Manager
File
Action
View
Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
Trust Points
Conditional Forwarders
New Host
Name (uses parent domain name if blank):
ns1
Fully qualified domain name (FQDN):
ns1.server.tw.
IP address:
2001:11:22:1::100
Create associated pointer (PTR) record
Add Host
Cancel
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:37 PM
5/8/2019

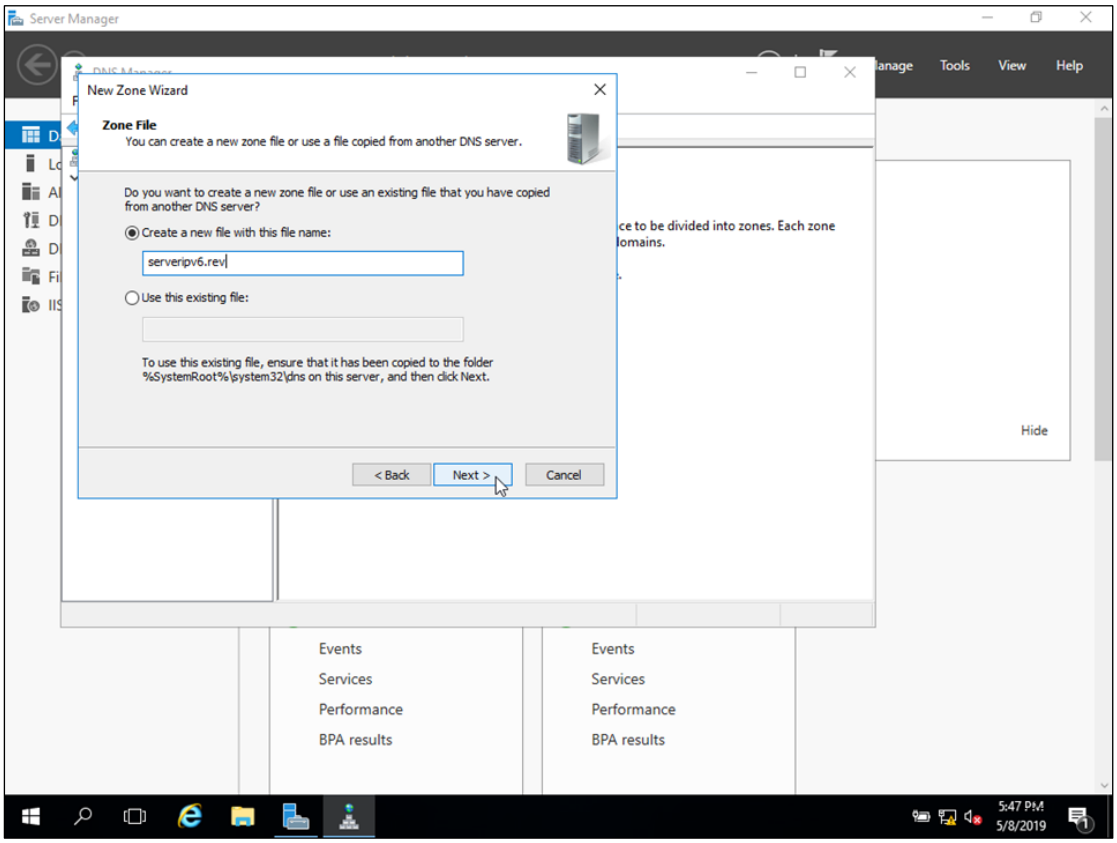

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lo
Trust Point
Conditiona
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone
rmation about one or more contiguous DNS domains.
ew zone, on the Action menu, click New Zone.
Create a new zone.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

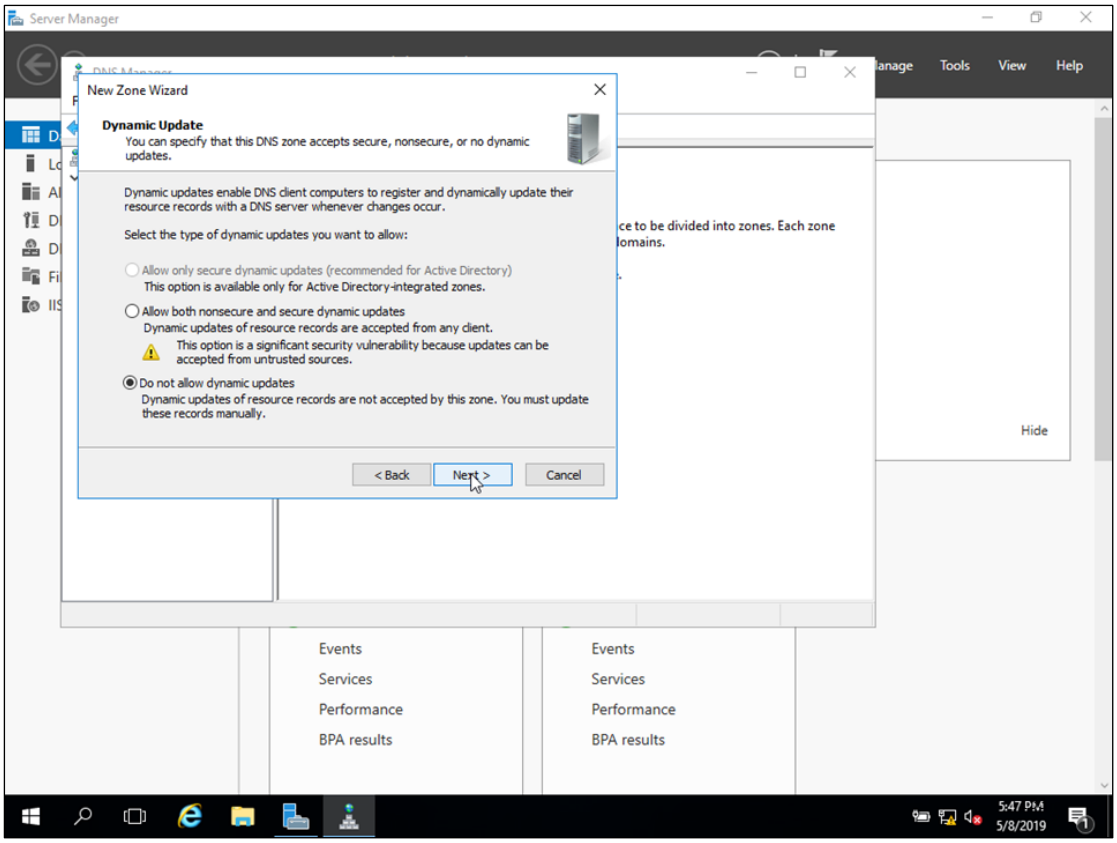

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
ce to be divided into zones. Each zone
domains.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5/8/2019

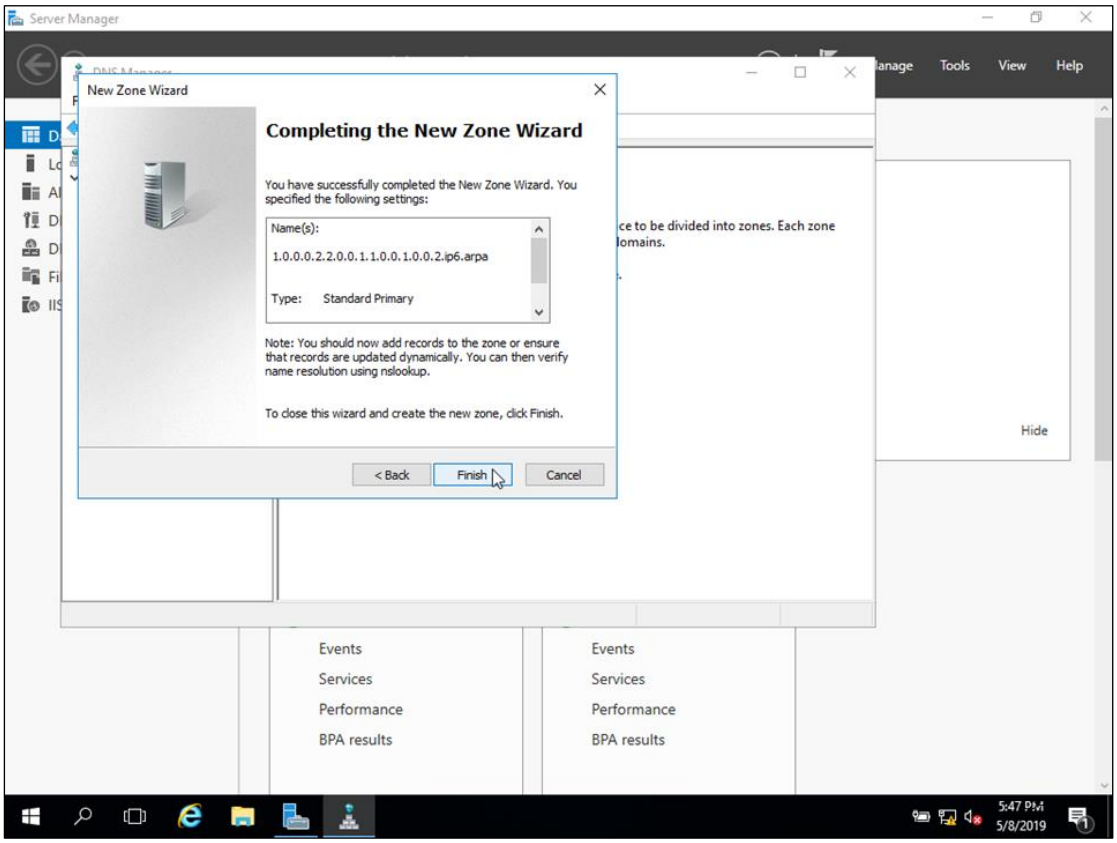

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

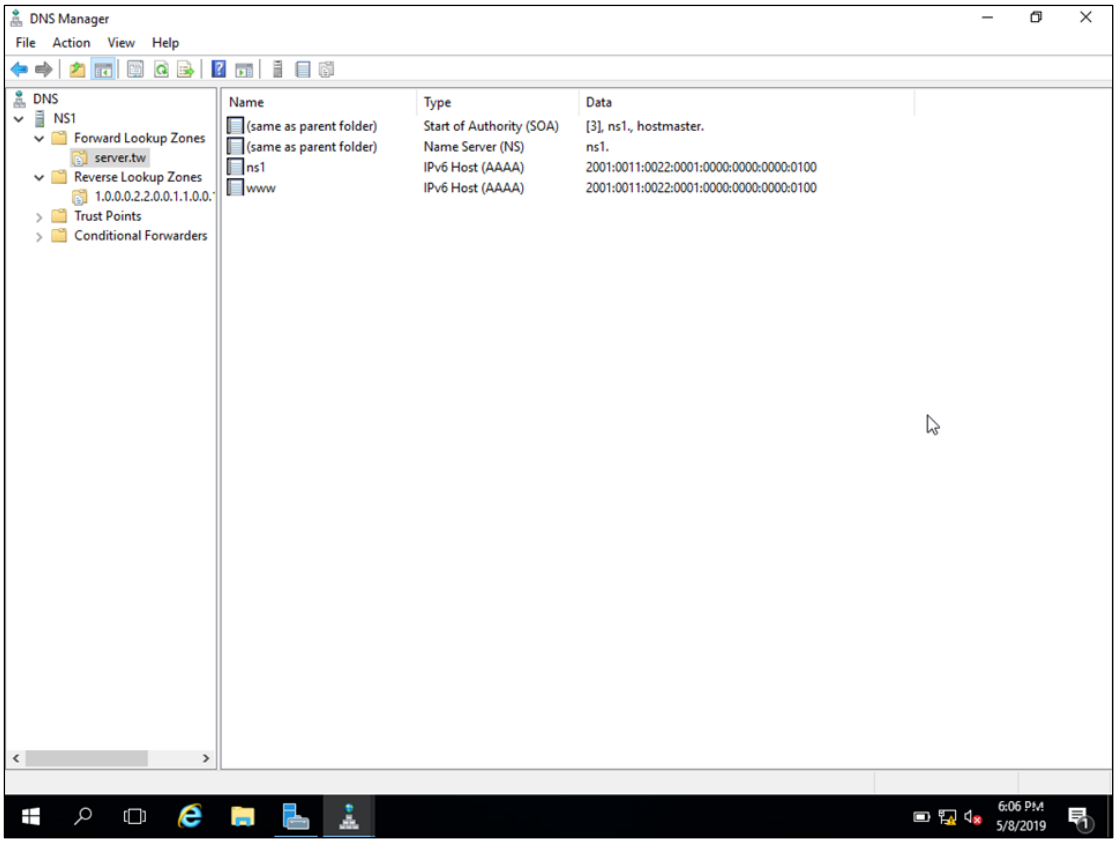

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.
IPv4 Reverse Lookup Zone
IPv6 Reverse Lookup Zone
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

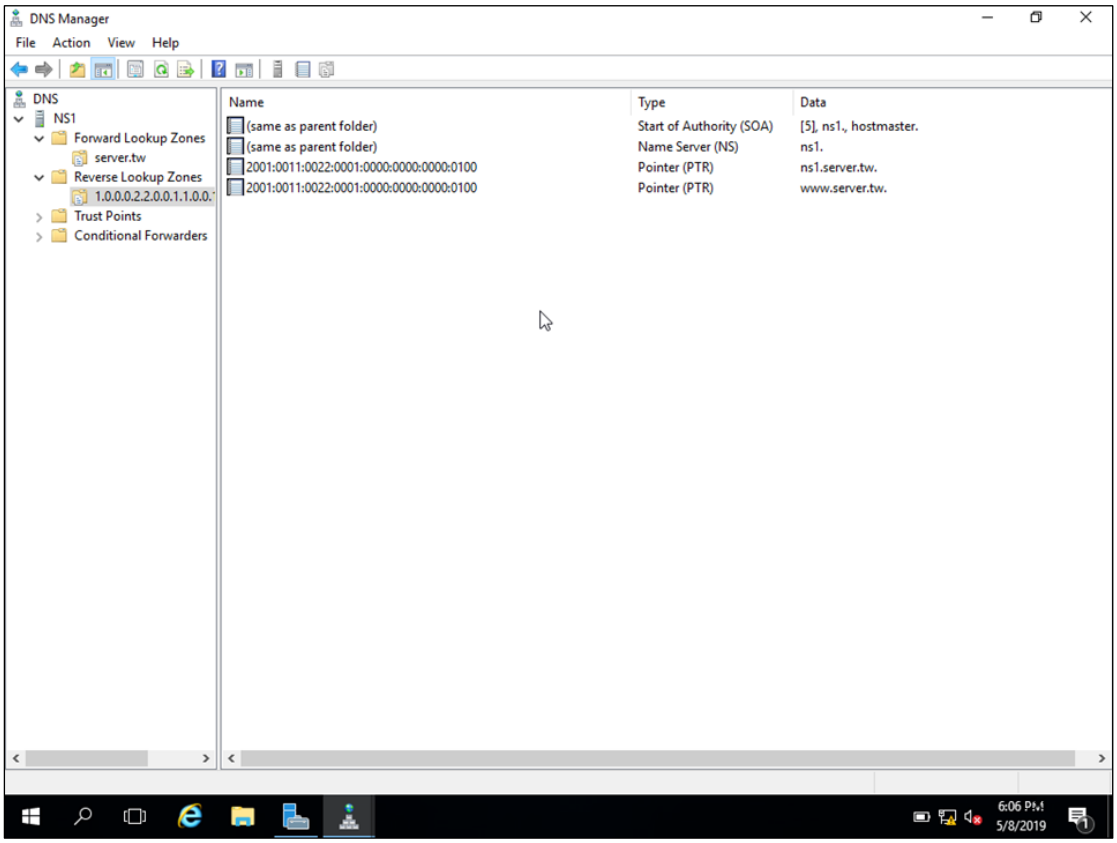

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.
IPv6 Address Prefix:
2001:11:22:1::/64
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.1.0.0.2.ip6.arpa
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:46 PM
5/8/2019

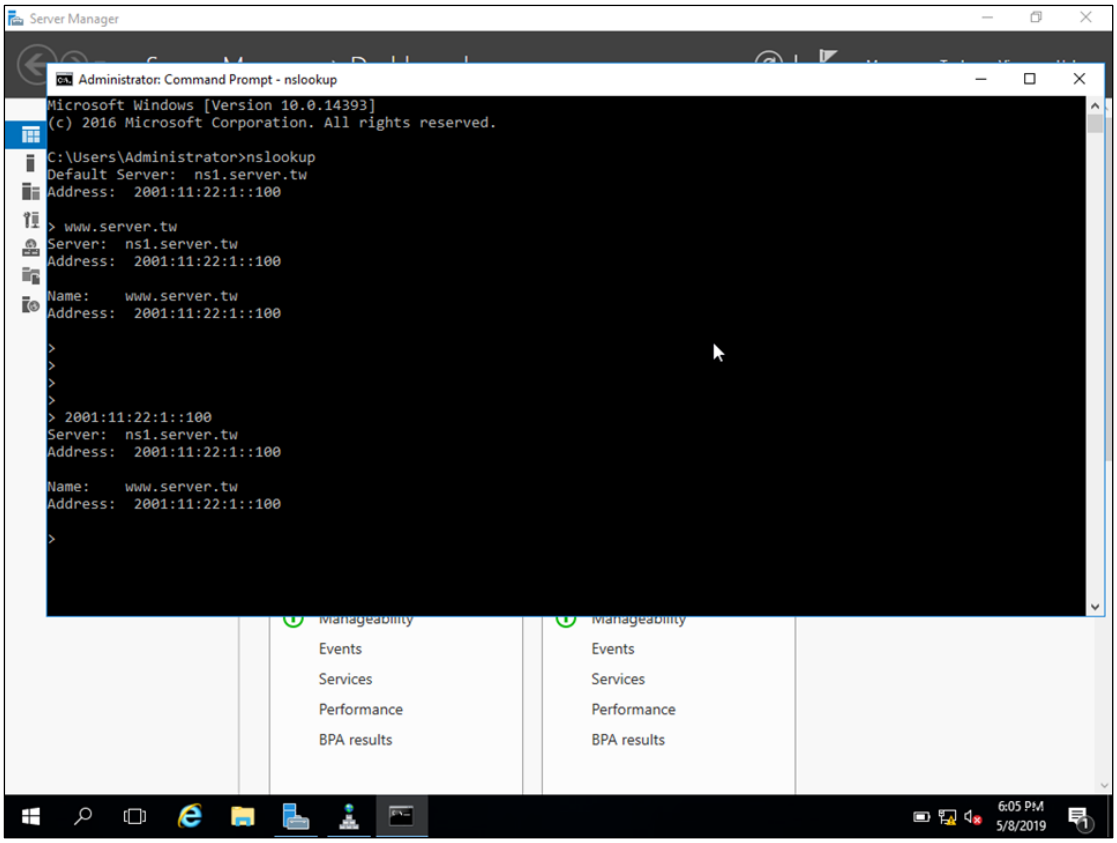

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
serveripv6.rev
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:47 PM
5/8/2019


Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:47 PM
5/8/2019

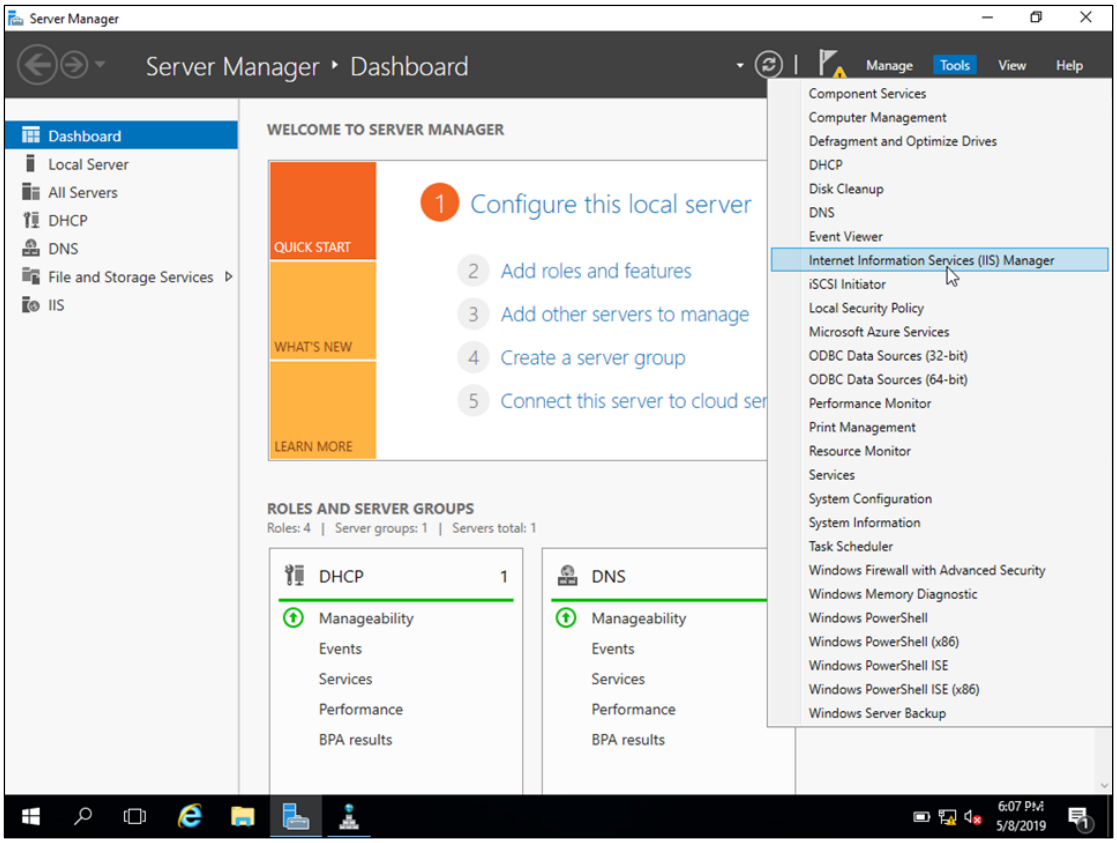

Server Manager
Tools
View
Help
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name(s):
1.0.0.0.2.2.0.0.1.1.0.0.1.0.0.2.ip6.arpa
Type: Standard Primary
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:47 PM
5/8/2019

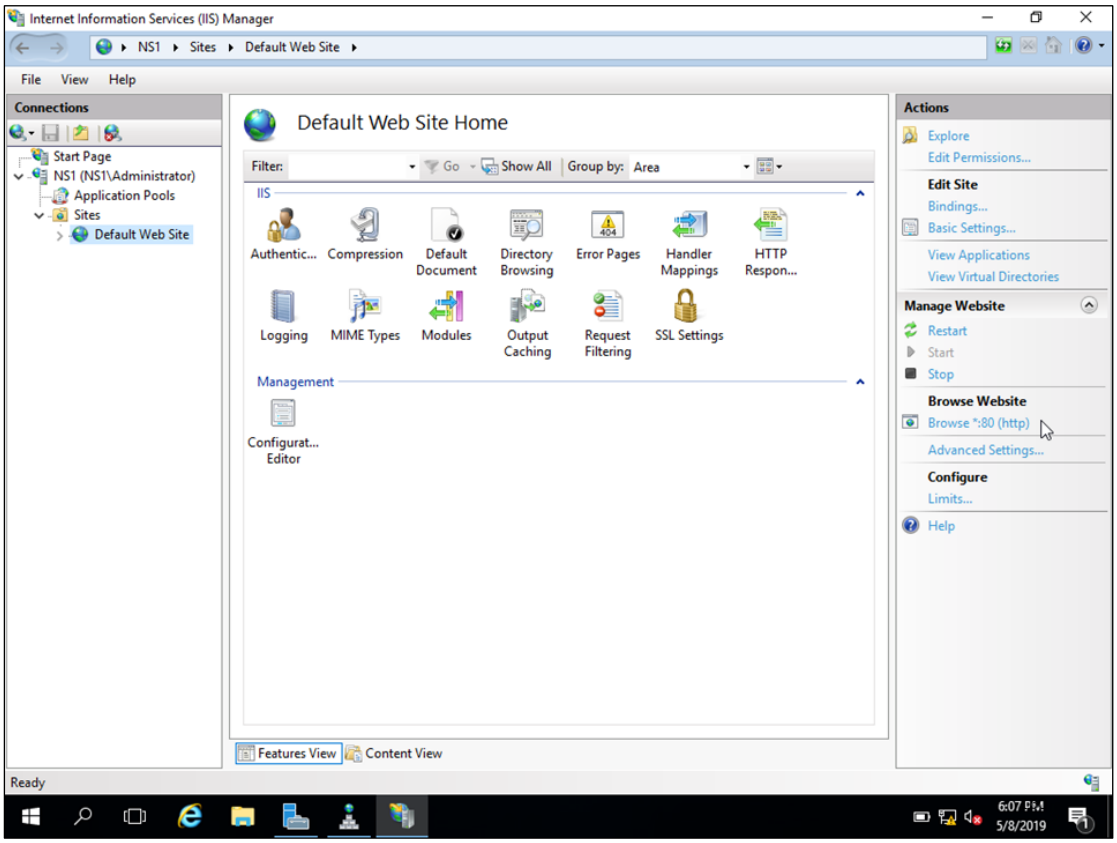

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[3], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
ns1
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
www
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
6:06 PM
5/8/2019

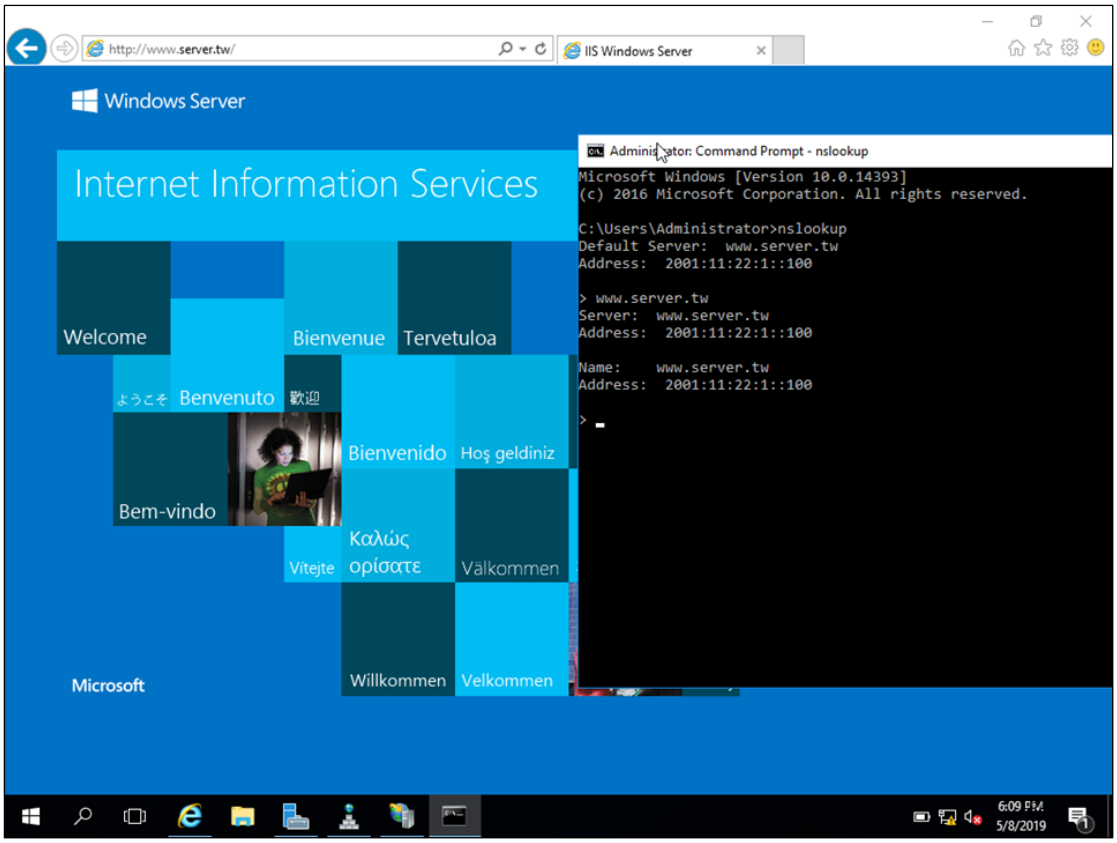

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[5], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
ns1.server.tw.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
www.server.tw.
6:06 PM
5/8/2019


Server Manager
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: ns1.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
>
>
>
> 2001:11:22:1::100
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
6:05 PM
5/8/2019

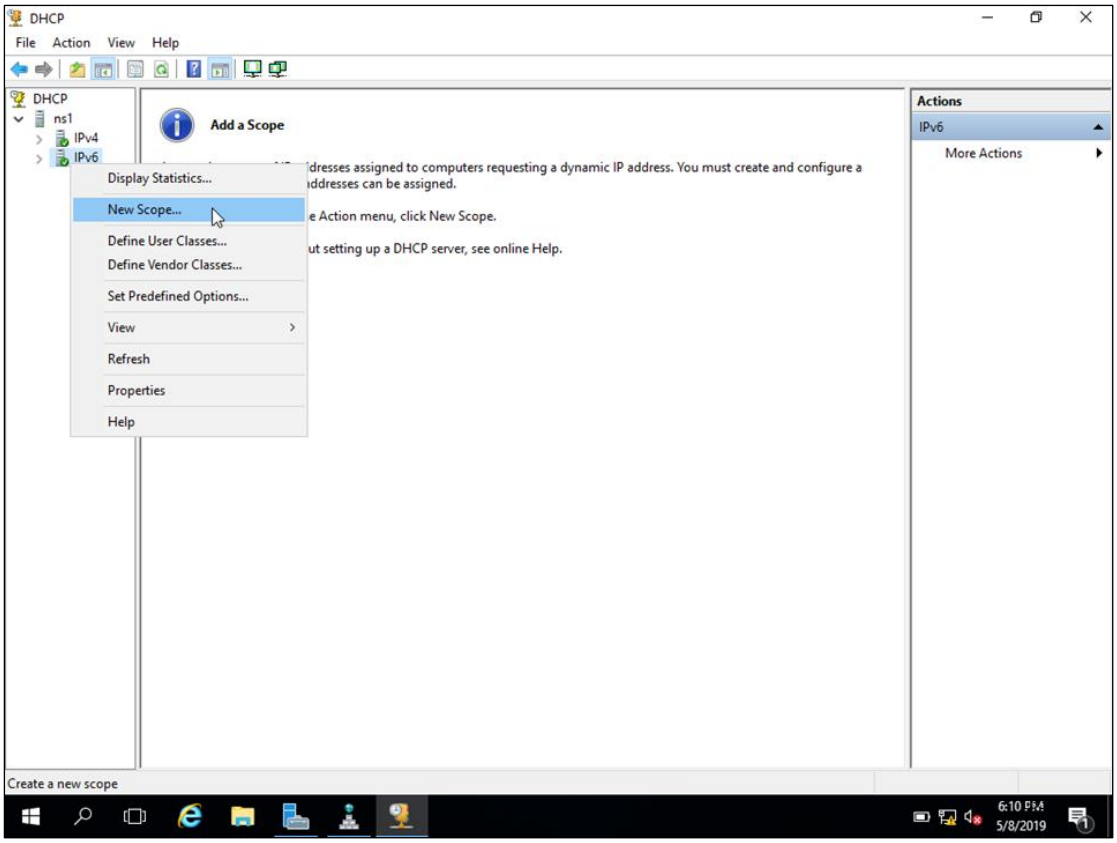

點進網域新視界！
IPv6建置
IIS 系統設定

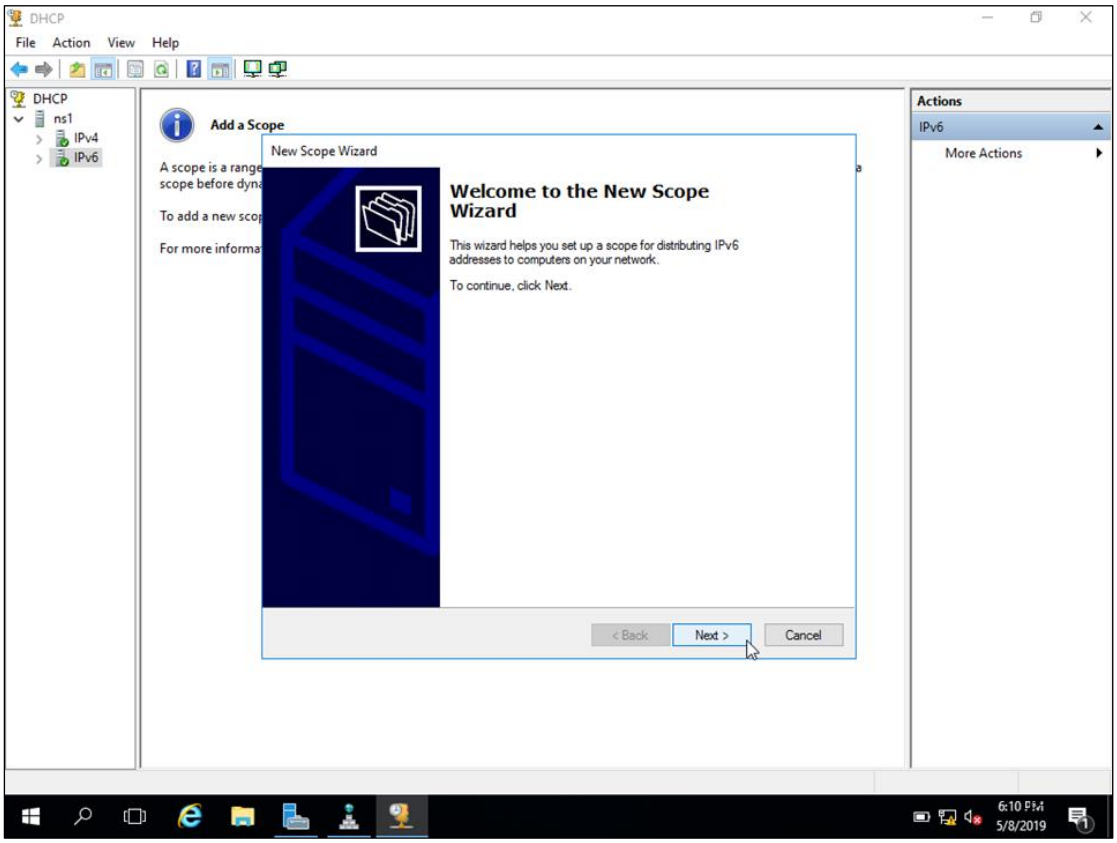

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud ser
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
DHCP 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
6:07 PM
5/8/2019

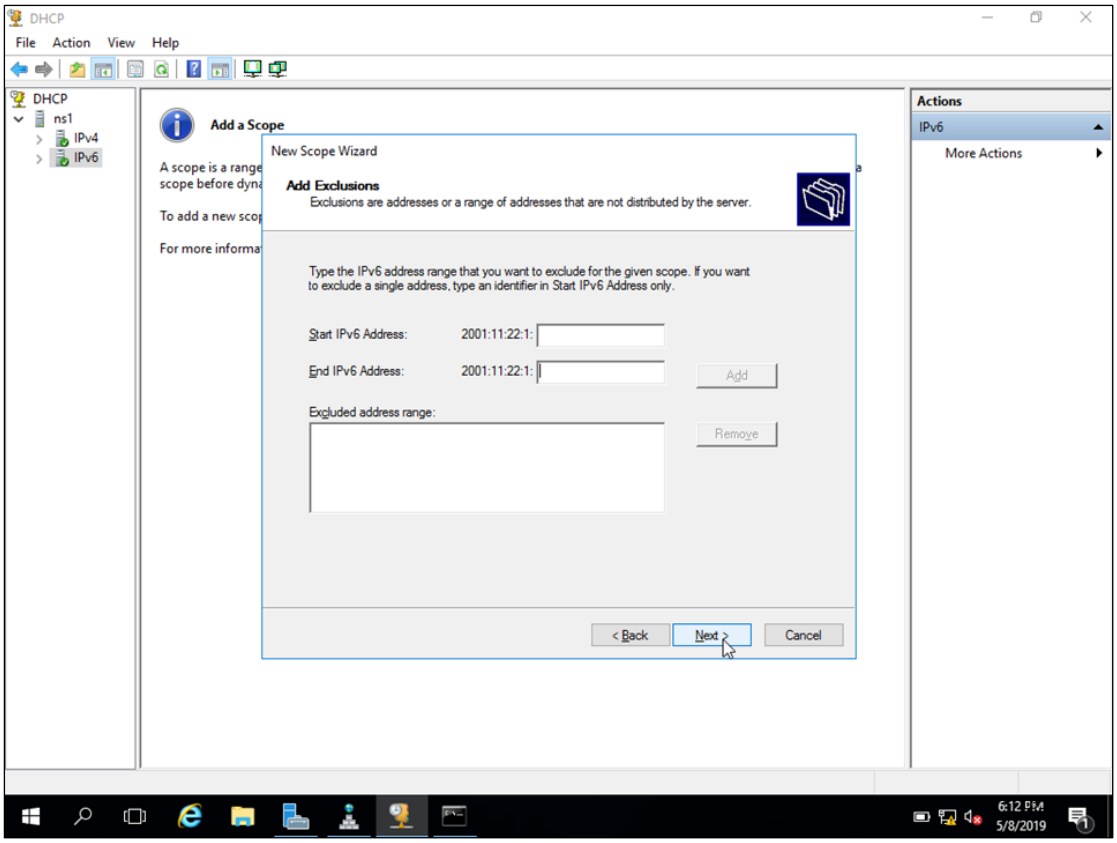

Internet Information Services (IIS) Manager
NS1 ‣ Sites ‣ Default Web Site ‣
File
View
Help
Connections
Start Page
NS1 (NS1\Administrator)
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
Help
Ready
6:07 PM
5/8/2019

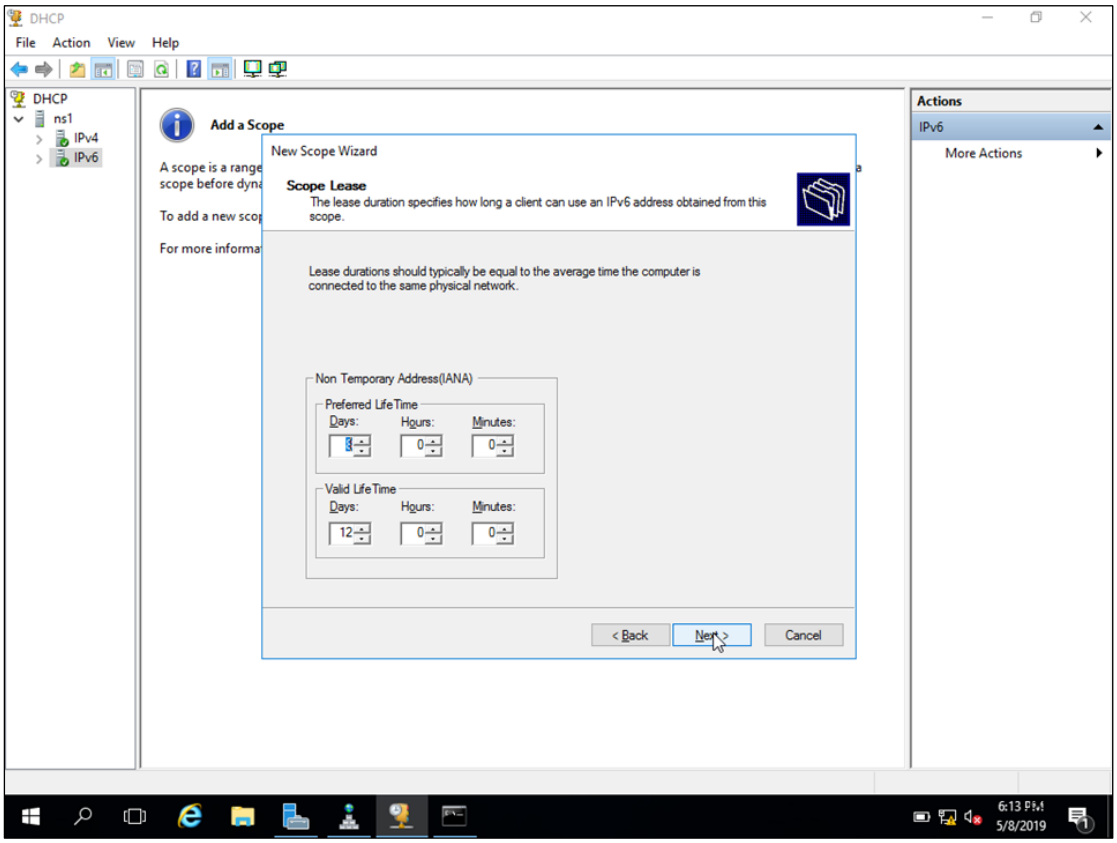

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
Willkommen
Velkommen
Microsoft
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: www.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: www.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
6:09 PM
5/8/2019

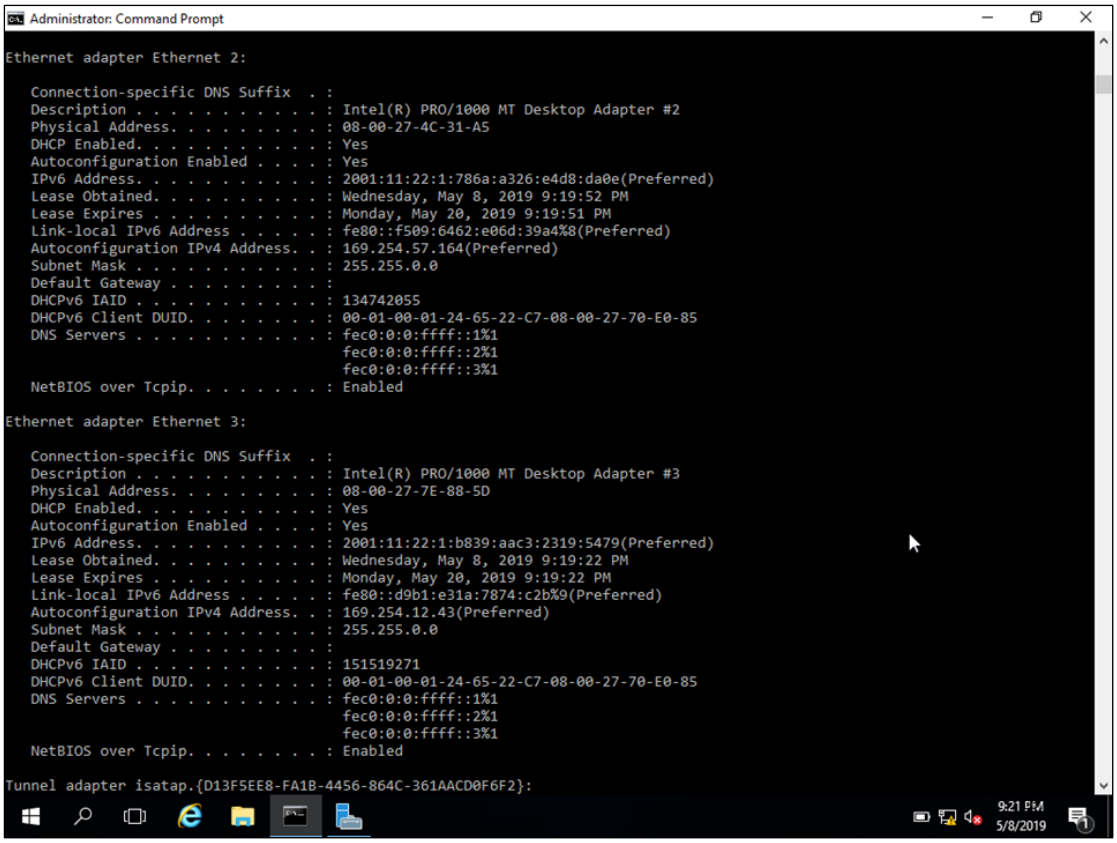

點進網域新視界！
IPv6建置
DHCP 系統設定


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
Display Statistics...
New Scope...
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
View
Refresh
Properties
Help
Actions
IPv6
More Actions
Create a new scope
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IPv6 addresses to computers on your network.
To continue, click Next.
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.
Start IPv6 Address: 2001:11:22:1:
End IPv6 Address: 2001:11:22:1:
Add
Excluded address range:
Remove
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:12 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Scope Lease
The lease duration specifies how long a client can use an IPv6 address obtained from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network.
Non Temporary Address(IANA)
Preferred Life Time
Days: Hours: Minutes:
8 0 0
Valid Life Time
Days: Hours: Minutes:
12 0 0
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:13 PM
5/8/2019



```
Administrator: Command Prompt

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
   Physical Address. . . . . . . . . : 08-00-27-4C-31-A5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:11:22:1:786a:a326:e4d8:da0e(Preferred)
   Lease Obtained. . . . . . . . . . : Wednesday, May 8, 2019 9:19:52 PM
   Lease Expires . . . . . . . . . . : Monday, May 20, 2019 9:19:51 PM
   Link-local IPv6 Address . . . . . : fe80::f509:6462:e06d:39a4%8(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.57.164(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 134742055
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #3
   Physical Address. . . . . . . . . : 08-00-27-7E-88-5D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:11:22:1:b839:aac3:2319:5479(Preferred)
   Lease Obtained. . . . . . . . . . : Wednesday, May 8, 2019 9:19:22 PM
   Lease Expires . . . . . . . . . . : Monday, May 20, 2019 9:19:22 PM
   Link-local IPv6 Address . . . . . : fe80::d9b1:e31a:7874:c2b%9(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.12.43(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 151519271
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{D13F5EE8-FA1B-4456-864C-361AACD0F6F2}:
```

在設定MySQL過程中需要設定

--bind-address= [IP/Hostname]

[IP/Hostname] 可以是

IPv4 address

IPv6 address

Hostname

在 my.cnf 設定檔中的[mysqld] 底下

設定 bind-address = ::

只要設定 :: 就可以接收 IPv4 or IPv6 的連接

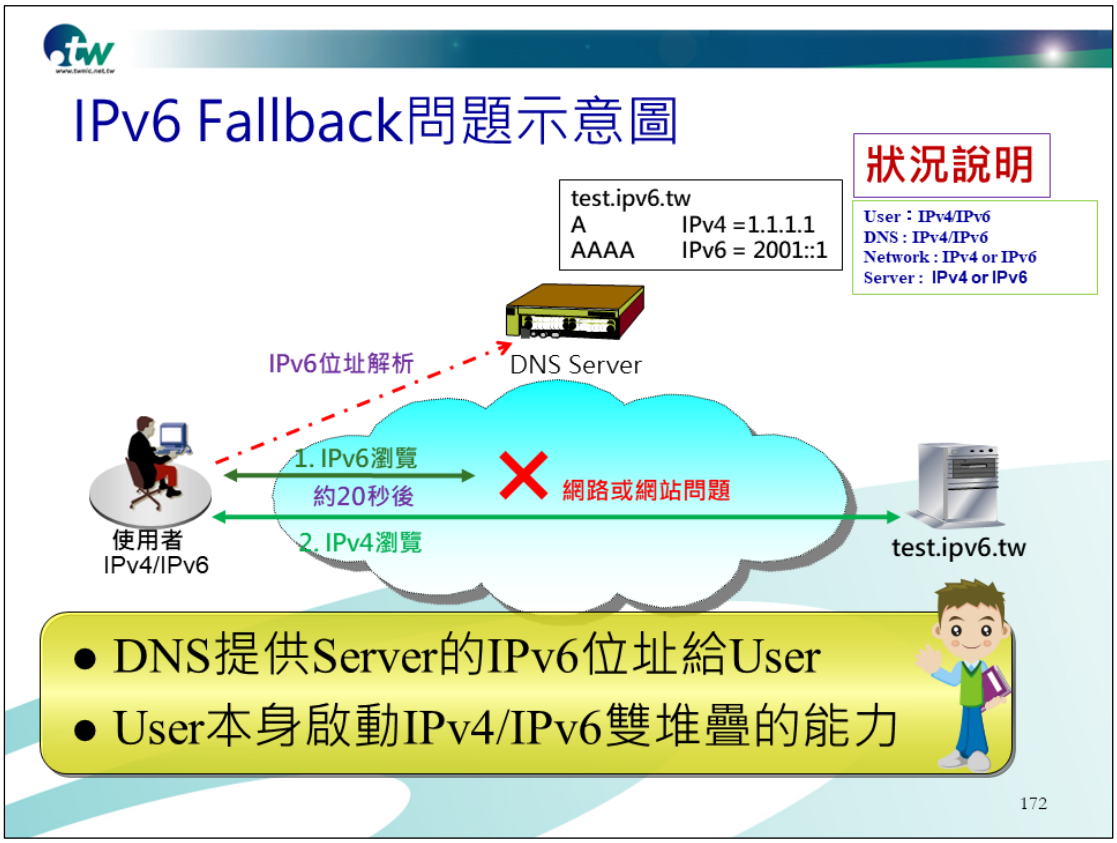
169

點進網域新視界！

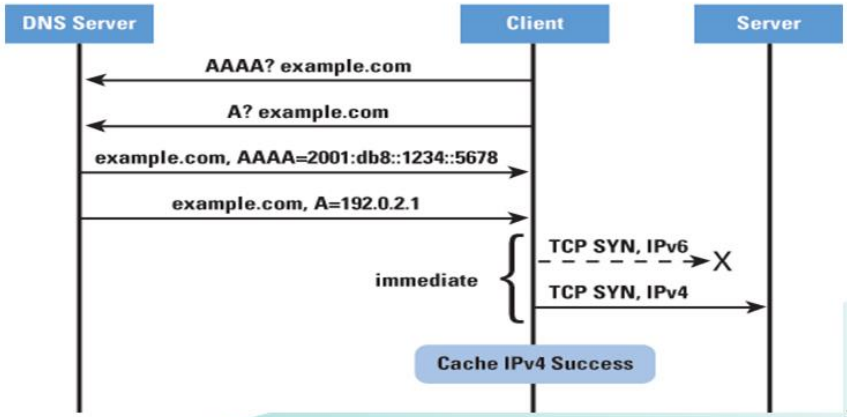
系統升級

流程步驟與檢查清單


網路/服務/終端IP使用對應情況
服務
Apache / Tomcat / IIS6 / IIS7
DNS / WEB / MAIL / SIP
網路
Router (Cisco , Juniper ---)
Routing (OSPFv3 , RIPng --)
終端
Windows Vista or 7
Linux Fedora ----
MAC OS
上網服務示意圖
使用IPv6連線至應用服務需使用者、網路、DNS伺服器與應用服務皆支援IPv6
1.詢問伺服器A的IPv4/IPv6位址
DNS 伺服器
2.傳回伺服器A的位址
使用者
IPv4/IPv6
3.使用IPv4或IPv6 瀏覽
應用服務伺服器
171


IPv6 Fallback問題示意圖
狀況說明
User：IPv4/IPv6
DNS : IPv4/IPv6
Network : IPv4 or IPv6
Server : IPv4 or IPv6
test.ipv6.tw
A IPv4 =1.1.1.1
AAAA IPv6 = 2001::1
IPv6位址解析
DNS Server
1. IPv6瀏覽
約20秒後
網路或網站問題
2. IPv4瀏覽
使用者
IPv4/IPv6
test.ipv6.tw
• DNS提供Server的IPv6位址給User
• User本身啟動IPv4/IPv6雙堆疊的能力
172

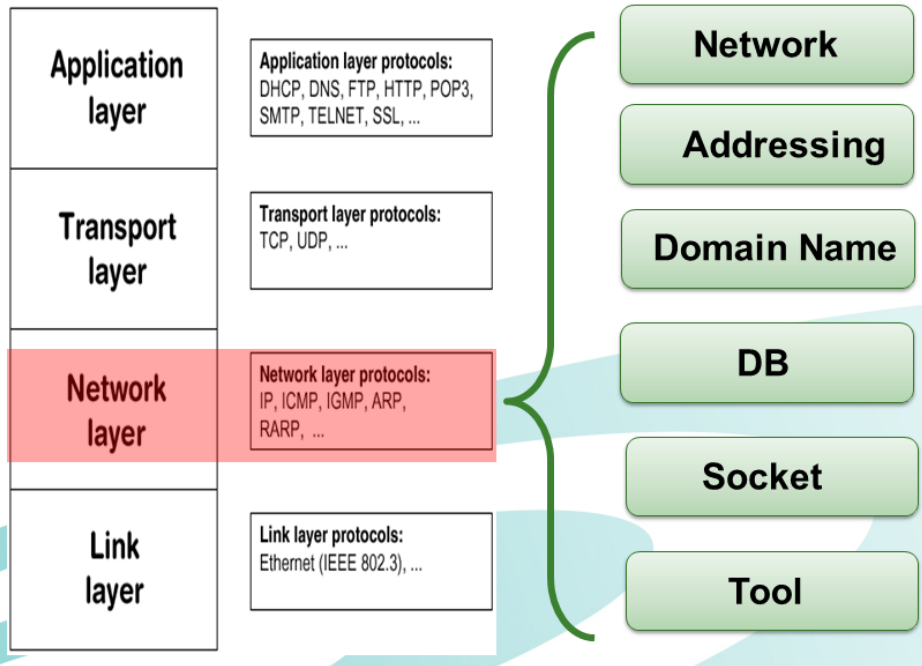
解決IPv6 Fallback問題->Happy Eyeballs



- 同時做IPv4及IPv6的連線量測，並優先選擇較快回應的網路，以達用戶端到服務端動態選擇效能較佳的網路路徑
- Google 's Chrome web browser, Opera 12.10, Firefox version 13, OS X可支援

173

開發環境IPv6注意事項



174

開發環境IPv6注意事項

- Network
  - IPv6 enabled (行動LTE/HiNET光世代或CHT WiFi)
    - 網路環境需支援IPv6，確保端對端IPv6封包能正常傳送
  - Support IPv6(Firewall, IDS, IPS, LB)
    - 網路架構中若包含其他設備(例如：Firewall, IDS, IPS 等)，需確保該設備功能已能支援IPv6，避免無法運作
- Addressing
  - IP Format
    - IPv6 address : 2001:b000::1/64 + DNS: 2001:B000:168::1
    - Subnetting
  - Auto-Configuration
    - Stateful Auto-configuration
      - DHCPv6
      - 集中管控IP相關對應資訊
    - Stateless Auto-configuration
      - 透過路由器通告網路Prefix對應資訊

175

開發環境IPv6注意事項

- DB
  - 若資料庫有儲存IP資訊的欄位，需注意Schema是否能同時儲存IPv6格式!
  - 與服務連線仍可使用內網(IPv4)來連接（選項）
- Domain Name
  - 可接受來自 IPv4 主機查詢某domain name的 IPv6 address
    - BIND 8.1 以後支援 AAAA 的 DNS 記錄
  - 可接受來自 IPv6 主機(該機器的連線 IP 是 ipv6)的 DNS 查詢
    - DNS本身需連線在 IPv6 的網路上
    - BIND 8.1.2 以上支援
- Socket
  - 使用到Socket之程式，使用函式可能有所差異!
    - 更換函數名稱或接收的參數格式
  - 需視程式需求與規格來檢視與修改!（RFC3493/3452/4038/5014）
    - 用戶不在乎是使用IPv4或IPv6來與server溝通
    - Server必須要能接受IPv4與IPv6連線

176

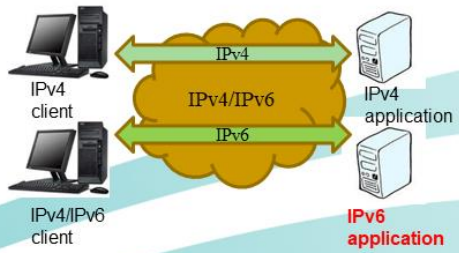
開發環境IPv6注意事項

- Tools
  - 測試網站：
    - http://ipv6-test.com/validate.php
    - https://test-ipv6.com/
  - 檢查IPv4 相關函數及參數，並提供相對應的IPv6 函數以供參考
    - IPv6 CARE, "IPv6 Compliant Automatic Runtime Environment "
      - 診斷IPv6 兼容的應用程式
    - checkv4.exe
      - Microsoft Windows Software Development Kit (SDK)
    - PortToIPv6
      - 開源框架，IPv4到IPv6編寫的自動化應用程序移植過程
  - 檢查工具均有安裝平台與檢查之程式語言限制，結果僅供參考

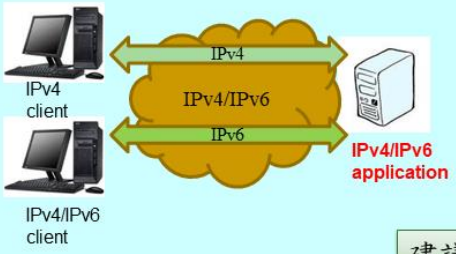
177

系統升級IPv6之方法 (1/2)

- 方法一：架設第二台伺服器，專門處理IPv6連線
  - 優點:不影響原本IPv4連線
  - 缺點:需維護兩台機器，有資料或程式碼不一致的可能性



- 方法二: 將原本應用程式啟用IPv6，同時接受IPv4與IPv6連線
  - 優點:維護容易
  - 缺 點:風險高，容易影響原本IPv4連線

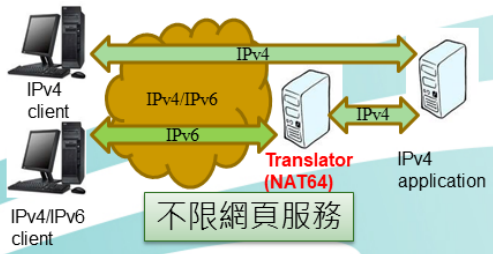


建議

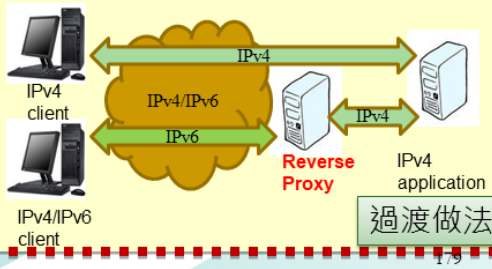
178

系統升級IPv6之方法 (2/2)

- 方法三:於原伺服器前架設一台轉換器(Translator)，用戶端用IPv6連線到轉換器，轉換器再使用IPv4連線到原伺服器讀取資料
  - 優點:可快速提供IPv6連線服務
  - 缺點:每一種通信協定需要一個轉換器，且擴展性不易，不是所有協定都可100%透通

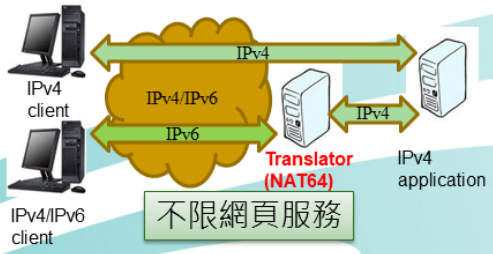


- 方法四:於原伺服器前架設一台reverse proxy，用戶端用IPv6連線到reverse proxy，reverse proxy使用IPv4連線到原伺服器讀取資料
  - 優點:可快速提供IPv6連線服務
  - 缺點:擴展性不易，不是所有協定都可100%透通，需作壓力測試，以確保運作無誤

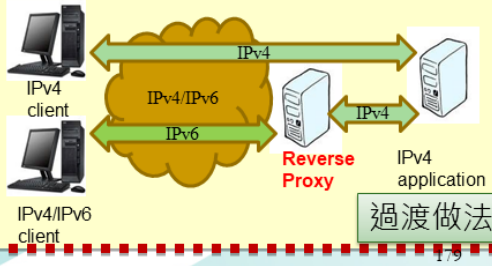


系統升級IPv6之方法 (2/2)

- 方法三:於原伺服器前架設一台轉換器(Translator)，用戶端用IPv6連線到轉換器，轉換器再使用IPv4連線到原伺服器讀取資料
  - 優點:可快速提供IPv6連線服務
  - 缺點:每一種通信協定需要一個轉換器，且擴展性不易，不是所有協定都可100%透通



- 方法四:於原伺服器前架設一台reverse proxy，用戶端用IPv6連線到reverse proxy，reverse proxy使用IPv4連線到原伺服器讀取資料
  - 優點:可快速提供IPv6連線服務
  - 缺點:擴展性不易，不是所有協定都可100%透通，需作壓力測試，以確保運作無誤



IPv6升級檢測

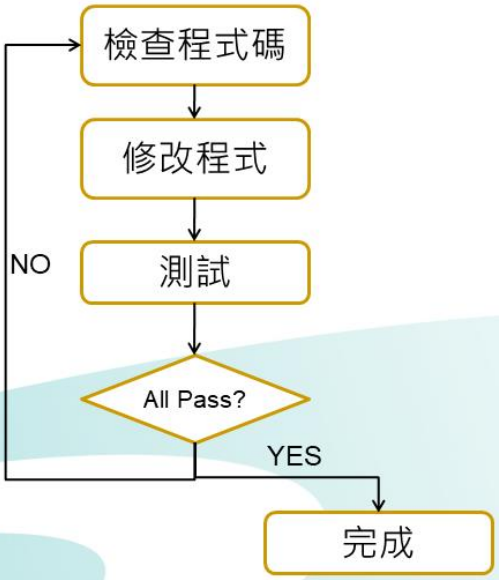
- 商用/免費/開源軟體
  - 預設支援

  - 預設不支援
    - 更新: 確認支援版本，規劃升版
    - 更換: 尋求其他支援IPv6軟體，規畫更換

180

IPv6升級檢測

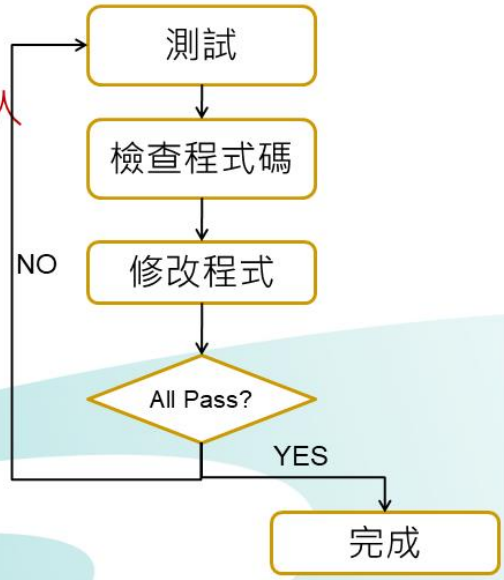
- 自行開發應用程式
  1. 開發語言支援度
     - C、JAVA、Perl、Python
  2. 使用函式庫類別
     - Non-Socket
     - Socket
- 修改程式與資料庫
  1. 調查系統程式與資料庫欄位需修改的清單
  2. 訂定開發修改時程
  3. 著手安排開發人員進行修改



181

IPv6升級檢測

- 複合式開發
  - 框架、程式語言、流程、人
    複雜!!
  - 透過測試來檢視



182

General CheckList

項次	說明	Remark
1	確認系統運作IPv6網路連線環境	
2	軟體清查與升級盤點(商用/免費/開源軟體/自行開發)	
3	確認系統開發相關設備/作業系統均支援IPv6功能 ➢ Firewall, IDS, IPS, LB ➢ 作業系統，應用伺服系統，網頁內容	
4	系統架構設計與轉移機制需求評估	
5	IPv6位址分配規劃/配置方式確認(伺服器/終端/網路/資安設備)	
6	檢查資料庫位址欄位需支援IPv6格式	
7	檢查程式碼IP 相關函數及參數	
8	註冊DNS IPv6 AAAA資源記錄	
9	檢測系統與終端IPv6連線能力 ➢ 系統：http://ipv6-test.com/validate.php ➢ 終端：https://test-ipv6.com/	
10	強化設備與系統IPv6防護能力避免惡意攻擊	

183

WEB伺服器如何取得用戶的IP位址

- Server端Web程式語言包含ASP, JSP, Perl, PHP等，可透過下列範例語法函式即可獲取使用者 IP 位址

PHP

```
<?php
 $ip=$_SERVER['REMOTE_ADDR'];
 echo 'Your IP Address ',$ip;
?>
```

ASP.NET

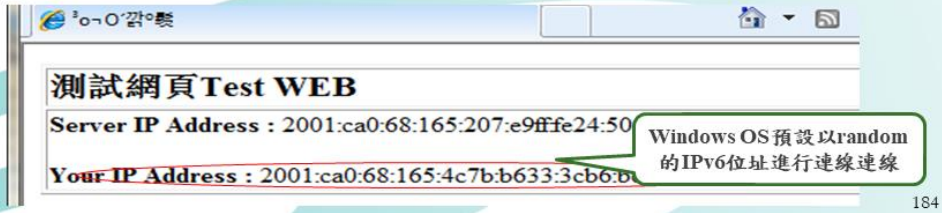
```
Your IP Address
:<%Reponse.Write(Request.UserHostAddress)%>
```

ASP

```
<%=Request.ServerVariables("REMOTE_ADDR")%>
```

JSP

```
RemoteAddr?<%request.getRemoteAddr()%?
RemoteHost?<%request.getRemoteHost()%?
```



網路服務升級 IPv6 檢測作法說明

https://is.gd/UCmheO

IPv6 網際網路通訊協定 升級推動方案

網路服務升級 IPv6 檢測作法說明

網際網路通訊協定升級推動辦公室檢測 DNS、Web、Email、以及 FTP 等各項外部網路服務是否升級至 IPv6 的檢測作法說明如下：

一、檢測 DNS 服務是否升級至 IPv6

(1). 檢測方式說明：

DNS 服務升級 IPv6 之檢測為透過純 IPv6 連線逐層檢查，從最上層的 root DNS 檢測起，再檢測 .tw DNS 以及 .com.tw/.gov.tw/.org.tw DNS 等，再到貴機關的 DNS 主機，一層一層的檢查，

a.檢測各層的 DNS 主機是否有支援 IPv6；

b.檢測各層的 Domain name 是否有設 AAAA 紀錄。

(2). 檢測作法：

逐層檢測時，若有發生檢測不通過的情形，可以在 Linux 環境下用下列 dig 指令的方式了解哪個部份有問題，指令如下：

dig -6 [填入欲檢查的 DNS] AAAA +trace

(例如：dig -6 www.gsnv6.tw AAAA +trace)

(3). 常見問題

線上檢測服務升級

https://www.gsnv6.tw/inventory/checkservicepub.cgi

線上檢測服務升級IPv6

檢測程式作法說明

若是檢測一般Web網站，前面請加 http://，例如 http://www.twnic.net.tw
若是檢測 https 網站，前面請加 https://，例如 https://www.gsnv6.tw
若是檢測 Email, DNS, FTP，請直接輸入主機名稱(domain name)，例如 dns2.twnic.net.tw
本網站 www.gsnv6.tw 的IPv6位址為：2001:c50:ffff:1::9016

系統分類	服務系統URL(例如：www.gsnv6.tw，請留意上面之說明文字)
Web ▼	

送出檢測

186

小結

- 發展與IP版本無關的程式碼，所有資料結構及APIs都應和IP版本無關
  - 使用網域名名稱而非IP，讓程式選擇使用IPv4或是IPv6
- 需確認應用程式是用IPv6或是IPv4連線
  - ISP IPv6連線狀態
  - Routing table狀態
  - 後台網路程式IPv6是否開啟
- IPv6 Web介面，顯示連線狀態，增加辨別度
- IPv6環境建置後，可透過純IPv6環境測試是否正常

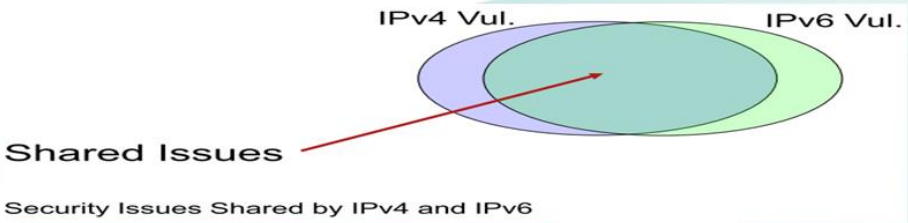
187

IPv4/IPv6雙軌環境下資訊安全規劃概述

點進網域新視界！

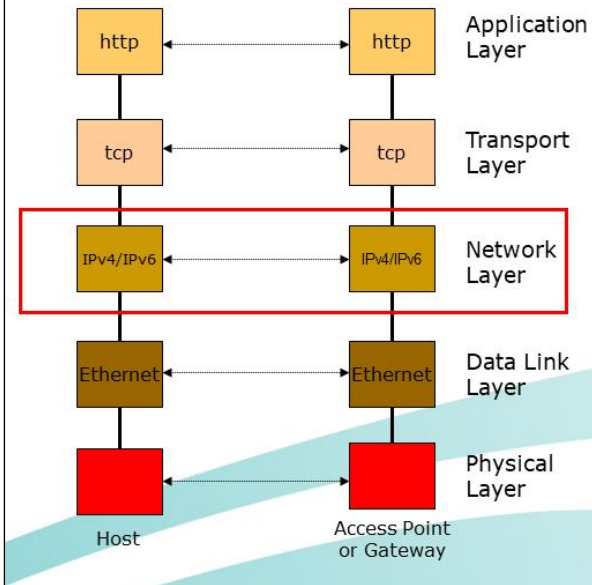
概述

- 面臨即將來臨的 IPv6 新一代網路，是否網路安全又再度即將暴露在危險當中？
  - IPv6無法像IPv4一樣去掃IP網段，因為IP太多了，每秒掃一千個IP位址，一個網段要掃五萬年才會完成。
- 在v4會發生的問題在v6也是一樣會發生。
  - 病毒和Worms的攻擊和威脅在IPv4和IPv6是完全沒有差別的，因為這是應用層的問題，不是網路層的問題。



189

At which layer security?



- **Layer 1:**
  - (Primarily physical) Wiretapping, Fiber tapping, console access, Rogue devices, etc.
- **Layer 2**
  - VLAN "hopping"; MAC, DHCP, ARP, Spoofing; Others
- **Layer 3:**
  - IP Spoofing, DoD/DDoS, routing, Smurf, Tunneling, Translation, Transition
- **Layer 4-7:**
  - Viruses, Worms, Application, Rogue software, Man in the Middle
- **Multiple Layers**
  - Reconnaissance, unauthorized access
  - Sniffing

190

IPv4 與 IPv6 之常見攻擊

- IPv6 無法解決所有的網路安全問題。基本上，IPv6 無法避免在對網路層以上各層之攻擊。IPv6無法處理的可能攻擊包括：

- 應用層（Application Layer）攻擊：在應用層（OSI 第 7 層）上所執行的攻擊，如緩衝溢出、電腦病毒與惡性程式碼，網上應用系統攻擊等等。
- 對認證模組的暴力攻擊與猜測密碼攻擊。
- 虛假設備（Rogue Device）：未經授權的裝置進入網絡中。裝置可能是一部個人電腦，但也可能是轉接器、路由器、領域名稱系統（DNS）伺服器、DHCP伺服器或甚至是一個無線接取點。
- 阻斷服務：阻斷服務攻擊的問題依然存在於 IPv6 裡。
- 社交攻擊：如濫發電子郵件、仿冒詐騙等。

191

IPv6 DDoS之攻擊案例

基於IPv6的分散式阻斷服務攻擊案例，可能只是下一波線上攻擊的開始，
如管理者未預先準備IPv6攻擊防護恐難以因應

It's begun: 'First' IPv6 denial-of-service attack puts IT bods on notice

Internet engineers warn this is only the beginning

By Kieren McCarthy in San Francisco 3 Mar 2018 at 09:30

Analysis What's claimed to be the first IPv6-based distributed denial-of-service attack has been spotted by internet engineers who warn it is only the beginning of what could become the next wave of online disruption.

Network guru Wesley George noticed the strange traffic earlier this week as part of a larger attack on a DNS server in an effort to overwhelm it. He was taking packet captures of the malicious traffic as part of his job at Neustar's SiteProtect DDoS protection service when he realized there were "packets coming from IPv6 addresses to an IPv6 host."

The attack wasn't huge – unlike this week's record-breaking 1.35Tbps attack on GitHub – and it wasn't using a method that is exclusive to IPv6, but it was sufficiently unusual and worrying to flag to the rest of his team.

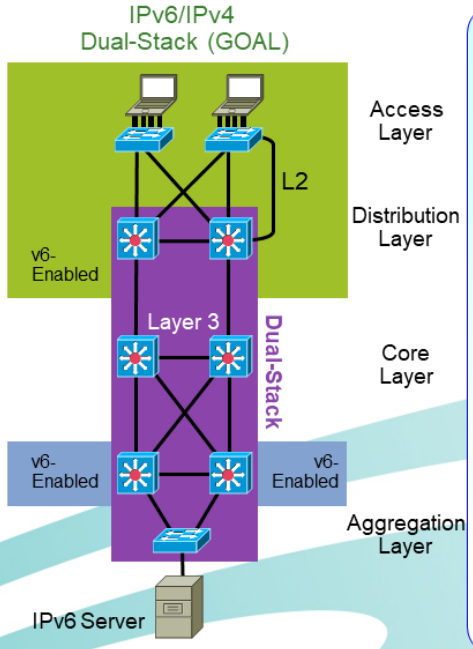
Computers behind 1,900 IPv6 addresses were attacking the DNS server as part of a larger army of commandeered systems, mostly using IPv4 addresses on the public internet. Anyone running an IPv6 network needs to, therefore, ensure they have the same level of network security and mitigation tools in place as their IPv4 networks – and fast.

"The risk is that if you don't have IPv6 as part of your threat model, you could get blindsided," Neustar's head of research and development Barrett Lyon told us.

With a few notable exceptions – like Facebook and LinkedIn – most companies that have started introducing IPv6 networks do so by running IPv4 and IPv6 in parallel, often with two different teams. Both Lyon and George warned that, in their experience, network engineers are getting their IPv6 networks up first and then worrying about locking down security later.

192

IPv6 網路安全架構



Source:ISP_security_best_practices_CS.pdf

Endpoints
- –Device integrity
- –Device and user AAA
- –Hosts: firewall (i.e. Black Ice), OS patches, AV,hardening
- –File system encryption
- –Vulnerability scanning

CPE Access/Perimeter
- –L3 filtering, L3 DDoS mitigation
- –L2 security (Firewall, AAA, device integrity)
- –URL filtering
- –IDS (Host/Network based)

Backbone/core
- –Device integrity
- –Route authentication

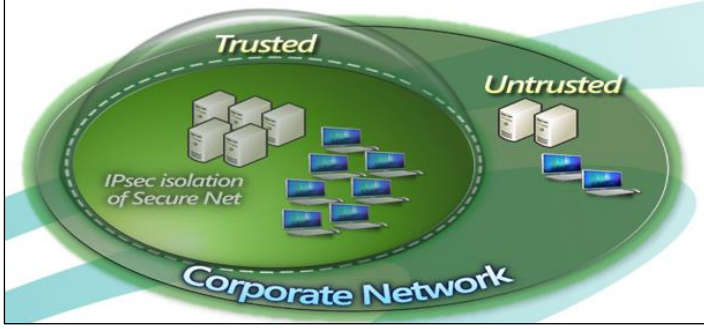
Aggregation/Distribution
- –Device integrity
- –Route authentication
- –Stateful/stateless firewall
- –Crypto
- –L3 filtering, L3 DDoS mitigation, L3 spoof mitigation

193

RFC 4942 IPv6 Transition/Co-existence Security Considerations

IPv6 Protocol-Specific Issues	Issues Due to Transition Mechanisms	Issues Due to IPv6 Deployment
■ IPv4-Mapped IPv6 Addresses ■ Increased End-to-End Transparency ■ IPv6 in IPv6 Tunnels	■ IPv6 Transition/Coexistence Mechanism-Specific Issues ■ Automatic Tunneling and Relays ■ Tunneling IPv6 through IPv4 Networks May Break IPv4 Network Security Assumptions	■ Avoiding the Trap of Insecure IPv6 Service Piloting ■ DNS Server Problems . ■ Addressing Schemes and Securing Routers ■ Consequences of Multiple Addresses in IPv6 ■ Deploying ICMPv6 ■ IPsec Transport Mode ■ Reduced Functionality Devices ■ Operational Factors when Enabling IPv6 in the Network ■ Security Issues Due to Neighbor Discovery Proxies

Confidentiality Integrity Accountability Availability



194

IPv4/v6共存環境的資安風險

網路駭客已在使用IPv6 — Attacker Community

- 駭客可利用IPv6同時攻擊IPv4/v6兩個網路
- 駭客也可利用IPv6 tunnel技術隱藏在IPv4流量中
- 目前大部分的OS預設支援IPv6
- Firewall與IDS無法辨識IPv6流量

IPv4環境中未授權的IPv6位 — Unauthorized IPv6 Clints

- 利用autoconfiguration是可以自行取得一個global的IPv6位址。
- 若網域內並無管制IPv6之流量，等若開啟一個不設防的後門。

IPv6通訊協定的弱點 — Vulnerabilities in IPv6

- IPv4在Layer 3的攻擊模式對IPv6依然有效。
- Subnet太大難以管理，攻擊者易匿蹤。

195

Source:NIST SP800-119 Guidelines for the Secure Deployment of IPv6

IPv4/v6共存環境的資安風險

IPv4/IPv6共存環境維運的複雜性較高

Dual Operations

- 管理者必須管理IPv4-IPv4; IPv4-IPv6; IPv6-IPv4以及IPv
  IPv6四種組合

IPv6部署solution與流程未臻成熟

Perceived Risk

- 缺乏標準的規範與明確細部的流程

未盡完善的廠商支援

Vender Suport

- 廠商對IPv6支援不如IPv4全面
- 對IPv6之支援尚無標準(NIST SP500-267)

Source:NIST SP800-119 Guidelines for the Secure Deployment of IPv6

196

IPv4 網路常見攻擊行為

IPv4 的設計主要考慮點對點傳輸模型，在網路安全的考量較少，因此導致 幾種下列常見的攻擊行為：

- 服務阻斷式攻擊(Denial of Service Attack, DoS)：此種攻擊為對服務提供 者進行大量非法要求，使得目標系統未處理這些非法要求而癱瘓正常服務提供
- 惡意程式散播(Malicious code distribution)：病毒或蠕蟲會藉由 IPv4 小位址空間裝載惡意 程式散播危及主機甚至遠端系統的安全性

197

IPv4 網路常見攻擊行為

- 分片攻擊(Fragmentation Attacks)：利用作業系統需大量重組 IPv4 封包 的特性，傳送不完全且不連續的片段封包導致主機當機
- 埠口掃描攻擊(Port Scanning)：利用端口掃描技術找出潛在的漏洞，由 於 IPv4 的位址空間很小，整個 ClassC 網路僅需四分鐘就可全部掃描
- ARP 欺騙及 ICMP 重導攻擊(ARP poisoning and ICMP redirect)：偽造的 ARP 回應通知網域中主機不正確的對應資訊可能導致封包傳送錯誤

198

IPv6常見/特有的安全議題

- 雖IPv6已增強安全性，但仍有不少挑戰，例如：
  - 雙堆疊安全性問題：如不適當的防火牆攔截、DNS區域記錄等
  - Rouge RA問題：入侵者假扮為路由設備並發出偽造的 RA 訊息
  - 標頭操作相關議題：多延伸性標頭 (Extension headers) 處理較複雜， 大封包可能被利用來癱瘓某些特定節點
  - Spoofing & Flooding議題：
    - 偽造網址仍然可能發生在IPv6網路中
    - IPv6 不使用廣播位址已大幅減少攻擊的可能性，但群播仍是問題
  - IPv6 Unsolicited Packet問題：缺乏NAT/FW阻隔，公眾網路未知的流量與惡意攻擊

199

IPv6網路安全防護考量

- IPv6不引進NAT，防火牆在IPv6資安上更形重要。防火牆必須支援IPv6，並確認IPv6功能之完整性及效能
  - 過濾掉不必要的封包訊務
  - 不使用IPv6之主機或網路設備，關閉IPv6功能
- 以IPv4網路安全防護為基礎，配合IPv6設計的差異，進行規劃設置
  - IPv4的最佳實作建議仍適用於IPv6，但必須確認IPv6資安設備可提供對等的IPv6防護機制 (L3 Spoofing、NDP Spoofing…等)
- IPv6相關協定及產品實作可能因安全議題陸續修定，須定期追蹤設備/軟體商、CVE等發佈之弱點公告，即時修補可能的安全弱點或漏洞

200

常見網路安全管理機制

- 封包過濾防火牆
  - 依據預設好的規 則，對流入或流出的 IP 封包是否放行進行管制，以決定是否允許或阻止 網路連線存取的行為
- NetFlow 流量監測
  - Netflow 以網路介面為單位呈現分析的結果
  - 包含各服務流量的資訊、各 IP 位址的流量資訊，甚至各種傳輸協議之流量高低排序…等等
- IDS或DPI 資安防禦設備
  - 經由接收路由器介面端口複製的鏡像(Port Mirror)封包
  - 經由封包的內容的特徵比對，進行第三層到第七層的資安風險分析

201

ICMPv6協定管控

- ICMPv6 在 IPv6網路扮演很重要的角色
  - 必須開放的 ICMP：Types 1, 2, 3, 4, 128, 129, 130, 131, 132, 143, 148, 149, 151, 152, 153, 133, 134, 135, 136, 141, 142
  - 通常開放的 ICMP：Types 3 -Code 1, Type 4 -Code 0
  - 必須過濾丟棄的 ICMP：Types 138,144,145,146,147
  - 視需要判斷過濾丟棄的 ICMP：Types 137,139,140,5-99,102,126
- IPv6網路運作依賴ICMPv6，傳統預設阻擋不再可行，防火牆 ICMPv6 政策需做修改

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

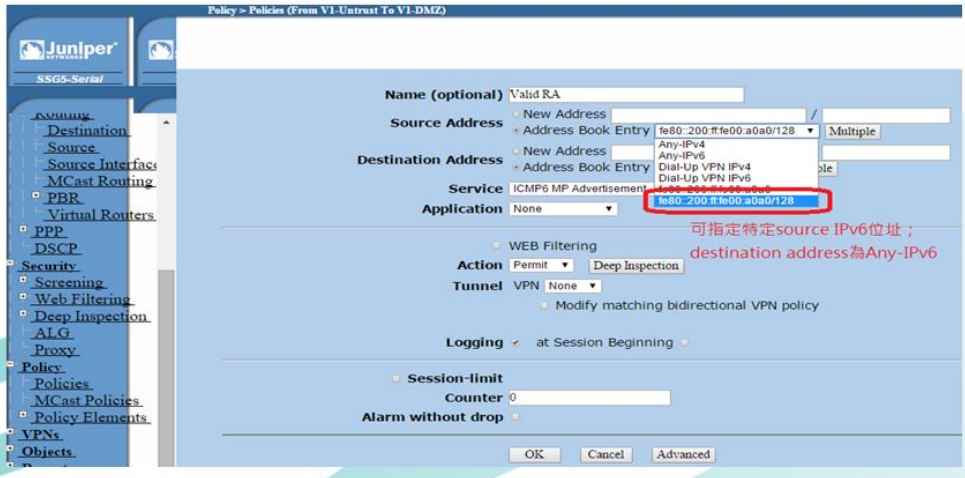
202

點進網域新視界！

IPv4/IPv6雙軌環境之資訊安全軟體與硬體設定

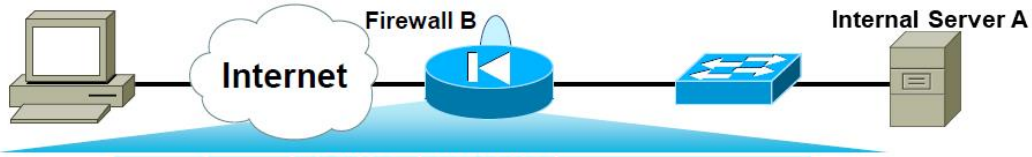
IPv6防火牆資安防護

- 清查既有防火牆是否支援IPv6，如尚未支援，應經由韌體升級或重新採 購，取得支援IPv6 的能力
- 防 火牆支援 IPv6 後可參考 IPv4 既有規則設定 IPv6 的過濾方式，再依據監 控蒐集的 IPv6 流量資訊進行觀察，逐步補足 IPv6 的防禦規則



204

防火牆ICMPv6 Policy範例



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	135/136	0	Neighbour Solicitation and Advertisement
Deny	Any	Any			

- IPv6所需的firewall防護，與IPv4不盡相同，不可全部套用
  - 針對ICMPv6及multicast的細部篩選過濾
  - 因為ICMPv6 ND/NS/RA/RS訊息所需的額外Layer-2 firewalls

205

Linux IPv6軟體防火牆

- 範例：僅允許特定IPv6 位址可以連線
  - ip6tables -I INPUT -p tcp -m tcp --dport <port> -s 2b00:x:x:x::/64 -j ACCEPT
- 範例：禁止特定IPv6 位址不能連線
  - ip6tables -I INPUT -p tcp -m tcp --dport <port> ! 2b00:x:x:x::/64 -j DROP

206

NetFlow IPv6流量統計

- 建議以不同時間排程將 IPv6 與 IPv4 流量資訊的抓取與分析時間錯開，以降低設 備負載度
- 依服務類別統計流量
  - 依據 Inbound、Outbound、SSH 連線、FTP 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計
  - 統計的項目包括連線流量、封包數目、封包大小等
  - 觀察送出該流量的 IP 位址、總流量數、總封包數、總封包大小
- 個人 IPv6 流量資訊查詢
  - 統計與記錄使用者 IPv6 位址統計網路流量資訊

207

IDS 或DPI System

- 主要目的為觀察封包 Payload 並比對出可疑流量特徵，進行紀錄與告警
- 可配合 Netflow 的統計，針對異常流量進行 Payload 的觀察，以蒐集建立異常流量的特徵值數據庫

動作　Protocol　IP　Ports　記錄在log裡的訊息

```
alert icmpv6 any any -> $HOME_NET any (msg:"ICMP6 connection detected!!!";\
sid:1000006; classtype:misc-activity; rev:1;)

alert any any any -> $HOME_NET $NOT_USUAL (msg:"Suspicious connection detected!!!";\
sid:1000007; classtype:misc-activity; rev:1;)
```

規則編號　行為分類　規則版本編號

208

點進網域新視界！

IPv4/IPv6雙軌環境下資訊安全檢查建議

資安設備IPv6防護建議

- 防火牆
  - 清查既有防火牆是否支援IPv6，透過汰舊換新過程逐步更換
  - 取得支援IPv6的能力如以韌體升級方式支援IPv6，須注意檢查CPU負載及記憶體的消耗狀況，避免效能不足防火牆
  - 支援IPv6後可參考IPv4規則設定IPv6的過濾方式(ACL)，再依據觀測的IPv6流量資訊，逐步完善IPv6的防禦規則
  - 參考附錄過濾政策Checklist
- 流量與Logs
  - 依服務類別/個人使用統計流量：Inbound、Outbound、FTP連線、SSH連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP等進行統計
  - OS本身可正常支援IPv6，System Log一般均可正常顯示;AP Log則需視AP對IPv6支援度而定，建議先行測試

210

網路設備IPv6防護建議

- 路由器：
  - 對外建議使用/127點對點連線
  - 僅允許正面表列的訊務流量通過，其餘禁止
  - 關閉發送RA
  - 過濾非必要之ICMPv6訊息，只處理合法網段訊務轉送
  - 依據scope範圍過濾群播封包
  - 禁止Routing Header Type 0(RH0)與未知IPv6延伸表頭
  - 啟動unicast Reverse Path Forwarding (uRPF)
  - 啟動Secure Neighbor Discovery (SEND)
  - 停用IPv6轉移機制，如6to4, ISATAP, Configured Tunnel等
- 交換器：
  - IPv6 First Hop Security
    - 啟動RA guard，DHCP guard，IPv6 Snooping，Source/Prefix Guard以及Destination Guard

211

伺服器與終端設備IPv6防護建議

- **伺服器**
  - 不要使用容易猜測的位址，並禁用自動組態配置功能
    - 例如：2001:ca0:164:6f::1
  - 部署入侵偵測系統來監督Link-local的流量，監督一些可疑流量型態的門檻值(threshold)
  - 強化主機系統及應用程式本身之安全
    - 定期做作業系統之patch、安裝主機型/網路型的入侵偵測系統、主機型防火牆及防毒軟體等
  - 停用IPv6轉移機制，如6to4, ISATAP, Configured Tunnel等
  - 主動監測資安防護狀態，偵測到異常攻擊儘快通報

212

伺服器與終端設備IPv6防護建議

- **終端主機**
  - 避免將每個用戶的IP位址指定成連續的IP位址，應該儘量分散其IP的指定，及使用隨機產生的位址前綴
  - 使用私有擴展位址（Privacy extensions），來達到防禦外部對內進行偵蒐攻擊的目的
  - 使用代理伺服器，如HTTP Proxy，以避免Web客戶端的IP被Cache，或使用暫時的Privacy Address
  - 所有電腦支援IPv6與host-based防火牆
  - 強化主機系統及應用程式本身之安全，如定期做作業系統之patch、安裝主機型的入侵偵測系統、主機型防火牆及防毒軟體等
  - 建議使用IPSec AH來作為兩端連線的相互認證
  - 停用IPv6轉移機制，如6to4, ISATAP, Configured Tunnel等
  - 主動監測資安防護狀態，偵測到異常攻擊儘快通報

213

小結

- 由於IPv6與IPv4網路將會長期共存，網路必然會同時存在兩者的安全問題，或由此產生新的安全漏洞
- IPv6已增強安全性，但仍有不少挑戰，較好的方式是過濾掉不必要的IPv6封包訊務/不使用IPv6之主機或網路設備，關閉IPv6功能
- 以IPv4網路安全防護為基礎，配合IPv6設計的差異，進行規劃設置
- 建議IPv6網路安全防護策略應配合RFC 4942與NIST-SP800作為參考基礎

214

結論

- **IPv6對網路創新和業務的持續成長非常重要**
- IPv6 是5G/IoT、SDN/NFV以及SR等新興技術發展的基礎
- 發展與IP版本無關的程式碼，所有資料結構及APIs都應和IP版本無關
  - 使用網域名名稱而非IP，讓程式選擇使用IPv4或是IPv6
- IPv6環境建置後，可透過純IPv6環境測試是否正常
- 建議IPv6網路安全防護策略應配合RFC 4942與NIST-SP800作為參考基礎

215


Thank You
216

三、 第三場教材


ICP IPv4/IPv6
雙協定網路安全防護
技術人才培訓
教育訓練
點進網域新視界！
國立高雄科技大學 資訊管理系
鄭進興 副教授
jscheng@nkust.edu.tw
1


TWNIC
財團法人
台灣網路資訊中心
簡介
點進網域新視界！

- 財團法人台灣網路資訊中心(TWNIC)是一個非營利性之財團法人機構，在交通部電信總局及中華民國電腦學會的共同捐助下，TWNIC於民國88年12月29日完成財團法人設立登記事宜，『財團法人台灣網路資訊中心』正式成立

- 主管機關原為交通部，民國106年12月22日完成主管機關變更為國家通訊傳播委員會。捐助章程中規定TWNIC為我國國家級網路資訊中心(National Network Information Center)

3

服務宗旨如下：

- 非以營利為目的，以超然中立及互助共享網路資源之精神，提供註冊資訊、目錄與資料庫、推廣等服務。
- 促進、協調全國與國際網際網路(Internet)組織之間交流與合作，並爭取國際網路資源及國際合作之機會。
- 協助推展全國各界網際網路應用之普及，以及協調資訊服務之整合、交換。
- 協助或支援政府辦理各項事務，並推動網路資訊相關公益事務。

4

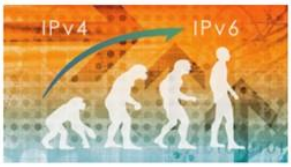
- TWNIC是目前國內唯一統籌網域名稱註冊及IP位址發放之超然中立之非營利性組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。

- 期盼更多人的參與及不斷檢討改進，為我國網際網路事業提供最佳服務，是TWNIC成立為財團法人之最大目的。希望各界也能不斷給予TWNIC更多的支持予鼓勵，使我國網際網路事業能更健全、更快速的發展。

5

域名服務

.tw/台灣10大類型網域名稱，註冊與管理服務。



IP/ASN申請

提供IP位址與AS Number申請，分配與管理服務。

Blog

掌握網路最新發展，政策，技術，趨勢與觀點。

研討會

參與TWNIC年度研討會，認識網路發展趨勢。

教育訓練

參與TWNIC系列教育訓練課程，認識最新網路應用課程。

社會責任

推動符合TWNIC服務宗旨之公益活動，協助推展全國各界網路應用之普及，以建立在地服務的品牌精神。

6


TWCERT/CC
近期監控到四種惡意程式的感染趨勢增加，提醒大家注意防範
TWCERT/CC
TWCERT近期監控到四種惡意程式的感染趨勢增加，提醒大家注意防範
2020-06-08 | 訊息發佈
台灣網路講堂
隱私保護美意 如何變成網路惡棍？
7/2
歡迎報名7/2(四)「DNS-over-HTTPS與網路治理：隱私保護美意如何變成網路惡棍？」座談會
2020-06-12 | 活動訊息
ICANN|68
VIRTUAL POLICY FORUM
APNIC 50
IETF 108 Online
多場國際網路組織會議將採用線上會議形式進行
2020-06-08 | 活動訊息
Domain Name
COVID-19
新冠病毒COVID-19 對網域名稱之影響
2020-05-22 | 訊息發佈
ICANN
Universal Acceptance
Case Study
//*.*/
透過普遍適用性提高網際網路的包容性與多樣性
2020-05-13 | 訊息發佈
台灣網路講堂
釐定隱私界線 與 打擊假訊息
6/2
台灣網路講堂第四講活動資訊更新
2020-05-06 | 活動訊息
7


IP/DNS 論壇
IP / DNS 論壇
@IPv6up.tw
首頁
貼文
關於
已說讚
追蹤中
分享
IP / DNS 論壇
傳送訊息
域名之友
@twnicNEWS
首頁
貼文
影片
讚
追蹤
分享
Marco TeaLand
竹籃裡的山茶園
傳送訊息
8

點進網域新視界！

IPv4/IPv6雙軌運作概念介紹

什麼是IP?

IP (Internet protocol) 電腦在網際網路上用來辨認溝通彼此的方法， IP位址就像是每家都有的門牌地址。

當我們上網或送email時，所打的網域名稱(如www.twnic.net.tw)會轉換成210.17.9.228網址，根據這個網址，網際網路就可以將訊息送到指定的主機。

10

IP的角色

網路的門牌號碼：IP address

位於網路堆疊的中心位置，兼容不同的網路介面

對 Transport Protocol 或 Application

提供統一的通訊方式。

11

擁擠的IPv4網路世界！？

目前分配給電腦的位址稱為IPv4位址
其位址格式是由4組 0~255的數字排列組成的
210.130.1.1

算算看，總共有2的32次方個位址可以使用
4,294,967,296看起來很多嗎?

新的電腦就再也擠不進網路世界了?

12

IP位址分配的組織

以紐約的IANA為中心（現委由ICANN管理）
其下再依區域分成五個區域註冊中心(Regional Internet Registries)

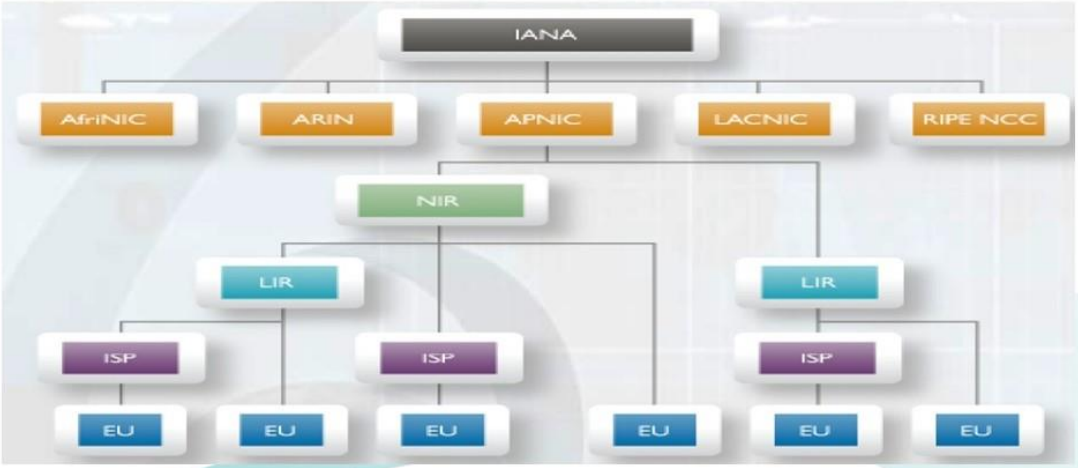
–歐洲地區：RIPE NCC
Réseaux IP Européens Network Coordination Centre
–北美地區：ARIN
American Registry for Internet Numbers
–亞太地區：APNIC
Asia Pacific Network Information Centre
–拉丁美洲：LACNIC
Latin American and Caribbean Internet Addresses Registry
–非洲: AfriNIC
Africa Network Information Centre

13

全球網際網路號碼管理架構

14

位址指派機構之階層式架構圖



以亞太地區來說，可透過 NIR (National Internet Registry) 將資源發放給LIR (Local Internet Registry，一般皆為ISP) ，LIR 再將資源指定分發給其客戶。

如此階層式的組織不但使得資源分配及管理更有效率
可避免資源過度集中，避免不公平的資源分配

15

IPv4 位址定址方式

1994年以前 Classful

分類網路（Classful Addressing）或稱「分級式定址」，是在 1993年左右用於描述網際網路的網路體系的一個術語。 它將IPv4的IP位址分成五個類別

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^{7} (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^{8} (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

1994年以後 Classless

16

IPv4 位址的分配類別

類別	網路位址	主機位址	最多主機數量	可分配的組織數
A	8位元	24位元	16,777, 214	128
B	16位元	16位元	65,534	16,384
C	24位元	8位元	254	2,097,152

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

17

IPv4位址枯竭影響與衝擊

- 影響
  - 無IPv4位址來提供新型態網路服務
  - 既有網路服務無法擴展
- 衝擊
  - 將造成網際網路發展停滯
- 解決方案
  - 使用NAT技術
  - IPv4 to IPv6位址移轉技術
  - 回收未使用的IPv4位址
  - 全面佈署IPv6
  - 其他

18

IPv4位址枯竭因應措施

- 開源
  - 開放保留的IP位址
  - IP位址的移轉或交易
  - IP位址的回收等等
- 節流
  - 調整現行的IP位址發放原則
  - 使用NAT相關技術延緩
- 進行IPv6的佈署
  - 分階段實行

19

IPv4位址枯竭因應建議策略

因應措施	開源(回收、移轉)	節流(使用NAT)	部署IPv6
優勢 (Strengths)	無技術門檻與實施費用	屬於現有成熟技術，可大量節省IP位址的使用，花費比部署IPv6相對便宜	擁有大量的位址，可根本解決位址不足問題
劣勢 (Weaknesses)	無確實可行的方法(回收或移轉均無好的實行經驗)，也非長期可行政策	NAT本身對一些應用的連線所有限制、每一個網路使用者需要的連線數正快速增加中，減少可共享一個IP的使用者數	對於大量實施在一些技術上仍有顧慮(如設備能力不足、安全性尚未完整考量)且部署費用相對較高

20

IPv4位址枯竭因應建議策略

因應措施	開源(回收、移轉)	節流(使用NAT)	部署IPv6
機會 (Opportunities)	有不少可回收位址(約有50個/8未出現在BGP routing table中、36個/8是歷史或特殊用途位址)	短期內有可能是唯一便宜可行的技術	唯一長期的解決方案，極有可能是未來會被全面採用的協定
威脅 (Threats)	合法擁有的IP位址要回收不容易，需擁有者願意配合	非長期解決方案且對於大量的使用者、電信等級的NAT均仍有待市場考驗	尚無明顯看到IPv6使用者市場，讓大部份的公司採觀望態度

21

IPv4所遭遇的挑戰

- IP位址有限，多人(戶)共用一個位址
- NAT雖可減緩位址之消耗，但是
  - 終究抵擋不住新興市場需求(如金磚四國)爆發性需求。
  - 2010年全球上網人口約16.9億　仍迅速增加中！
- 行動上網需要更多IP位址及行動能力(Mobility)支援
  - IPv4位址不足外，Mobility支援能力先天不足。
- 資源分配不均
  - 2010年1月底美國上網人口2.2億，擁有超過50%以上之IP位址
  - 2010年1月底中國上網人口3.6億，僅擁有不到6%的IP位址

22

IPv4技術本身的缺陷

- 數目限制：
  - IPv4的網路位址只有32位元
  - 採用Class的方式劃分區域較缺乏彈性
- 效能問題：
  - 在IPv4上面實做「QoS」服務極為困難。
  - CIDR的出現導致網路管理上的困難。

23

IPv4技術本身的缺陷

- 安全問題：
  - IPv4無法在基本網路層提供安全的加密通訊
- 組態設定：
  - DHCP伺服器安裝、設定、維運不易
  - 全自動化的組態設定

24

IPv4技術本身的缺陷

IPv4不只無法支應快速成長的位址需求
它的缺點是無法支援網路安全及國際漫遊的能力

IPv4 需要利用網路位址翻譯器
(Network Address Translator；NAT)

對經營者而言，它就增加了成本及管理上的負擔

25

為何需要IPv6？

解決 IPv4 的問題

–發生 IPv4 位址不足
–NAT 的應用增加
–對等式 (Peer-to-Peer) 網路技術問題
–行動設備的支援性

26

為何需要IPv6？

下一代 Internet 的標準

–IETF 已完成 IPv6 核心網路的標準
–全球將邁入 IPv6 新世紀 (例如：4G、 5G)
–行動裝置、 P2P 軟體應用
–IPv6的安全性

27

為何需要IPv6？

IPv6與物聯網社會

–P2P通信、無國界通信
– End2End security
–與雲端運算特性結合
–利用IPv6實現物聯網服務與應用

28

IPv6的發展 (1/2)

1992年，IETF之IPv4的Address空間不足的問題開始被檢討

1994年，下一代的網際網路協定開始被提案，包括三項
CATNIP (Common Architecture for the Internet)
TUBA (TCP/IP with Bigger Addresses)
SIPP (Simple Internet Protocol Plus)

1995年，SIPP被更名為IPv6
IPv6的規範將被RFC1752公開
(The Recommendation for the IP Next Generation Protocol)

29

IPv6的發展 (2/2)

1998年，IPv6之位址架構與通訊協定之規範分別在RFC2373 (IP Version 6 Addressing Architecture)與RFC2460 (Internet Protocol Version 6(IPv6) Specification)公開。

1999年，全球第一個業界團體(共有42個單位加盟)成立了「IPv6 Forum」。ARIN 將全球第一個之IPv6 Prefix：2001:400::/35授予給 Esnet (能源科學網)。

2002年，全球各區域性的Internet Registry RIR(Regional Internet Registries)實施新的「IPv6 Address Allocation and Assignment Global Policy」

30

IPv6之優點與支援狀況

- IPv6 發展之優勢(相對於IPv4)
  - 足夠的位址空間
  - 彈性的聯網機制 (Plug & Play)
  - 安全機制
  - QoS功能增強
  - 強化的 Mobility 與 Multicast 能力等

31

IPv6之優點與支援狀況

- 標準已臻完備

  2007年底止 IETF通過191項RFC標準，幾乎涵蓋所有IPv4既有標準。

- 軟硬體設備支援已漸成熟

  各式作業系統皆支援IPv6

32

IPv6之優點與支援狀況

•尚未蓬勃發展的主要因素

–IPv4位址尚未迫切短缺，普遍以不變應萬變
–發展期過長，不斷在IPv4技術上尋求解決方法
–許多IPv4 applications均將NAT issue考慮在內

–尚無法找到有明確利基的IPv6 Business Model
(IPv6 應該是標準，而不是應用)

33

什麼是IPv6?

v = version= 版本
IPv6 就是第六版的IP規範

IPv6總共有2的128次方個可以使用，IPv6位址寫法為八組四個位數，每位數是由16進位的0,1,2,3,4,5,6,7,8,9,a,b,c,d,e,f 所組成，中間用冒號分隔 2001:0c50:ffff:0001:02e0:18ff:fe95:b229

34

什麼是IPv6?

別擔心這麼一大串背不起來

我們日常上網還是以使用網域名稱

例如 www.twnic.net.tw

系統會自動轉換網域名稱為IPv6位址

所以一般使用者不需要直接輸入IPv6位址

35

IPv6 位址表示法

IPv6使用128 Bit的位址空間

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

用以下位址為例

20030000000000B30000000000001234

(太長容易記錯)

36

IPv6 位址表示法

>2003:0000:0000:00B3:0000:0000:0000:1234

(分為八段，以冒號分隔)

簡寫規則:

1.每 32 Bit 如開頭之 4bit 表示為 0，即可省略

2.若 32 Bit 全為 0，則可簡寫為0

3.若連續完整之32Bit 段落皆為 0000，則可全省略，簡寫為::，但以一次為限

>2003:0:0:B3::1234 (簡寫)

37

IPv6 位址表示法

請還原

2001:e09:6910:100::1

請用簡寫寫法表示

2001:0f08:5800:0009:0052:0000:0000:0101

38

IPv6位址範例

www.ipv6.hinet.net
  2001:b000:180:3::5
  202.39.224.5

www.twnic.net.tw
  2001:c50:ffff:1::9999
  124.9.9.9

39

使用IPv6的理由

- 提供更多的IP位址空間
  - 滿足未來IPv4可能不足的危機。
- 更好的資料傳送品質管理(QoS)
  - 對於多媒體影音有更好的QoS支援。
- 更契合無線行動通訊的協定
  - 利用Mobile IPv6協定，增加IP定址的便利性與縮短資料傳送延遲的時間。
- 強化的安全機制(IPSec)
  - 確保End-to-End(端點到端點)的安全。

40

IPv6的五個主要優點

1. 數量多，非常多
2. 服務品質保證(QoS, Quality of Service)
3. 隨插即用
4. 點對點傳輸
5. 使用更安全

41

優點一：數量多，非常多

• IPv6位址總共有2的128次方個可以使用，也就是有340282366920938463463374607431768211456個IPv6位址可以使用

•一平方公尺能有多少IPv6的位址呢？以地球總面積來算算看，地球總面積約5億1仟萬平方公里，每平方公尺將有655570793348866943898599個IPv6的位址(約有6仟5佰萬兆個)

42

優點二：服務品質保證(QoS)

•QoS是一種控制機制，傳統的IPv4 網路並未提供完整的QoS機制，訊息的傳遞未被分類，全部擠在網路上爭先恐後是造成網路擁塞的主因之一。

•IPv6的應用主要特色有：提供順暢、有秩序的網路傳輸將網路資源分級與分類，通過流量控管保持網路傳輸的順暢。

43

優點二：服務品質保證(QoS)

•這就像車輛走在道路上，不同的車種走不同的通道，快速而有秩序的通過以保待通道的順暢性。提供特定標籤給特殊需求者優先的服務權，如緊急醫療服務系統、119、110…等社會緊急資源的應用。

•透過IPv6與建全的QoS機制能確保即時線上的連線、防止服務中斷以及提高網路的效能，讓訊息傳輸達到一定的水準。

44

IPv6優點三：隨插即用

•在未來世界裡具有IPv6功能的家電及設備，只要啟動開關立即可變成IPv6網路的一員。

• IoT 的大量運用

45

IPv6優點四：點對點傳輸

在IPv6的世界裡，每個上網的人都有專屬的位址，這使得點對點的運用變得更便利，如網路電話、視訊傳輸，可即時快速的傳送給對方。

46

IPv6優點五：使用更安全

IPSec是過去為了解決IPv4的安全性問題所產生的IP安全協定

IPv6將IPSec納入其架構中

讓IPSec直接可以鑲嵌在IPv6的封包中

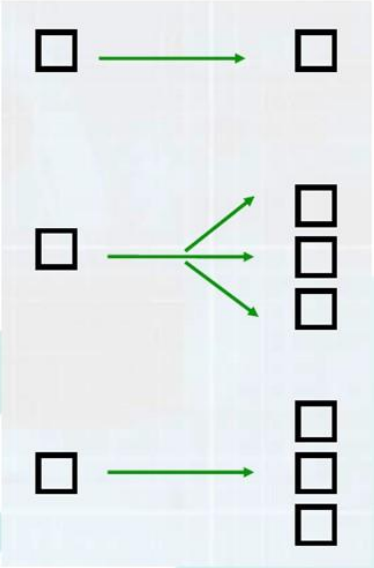
47

Basic Address Types

•Unicast (點對點傳輸)

•Multicast (群播傳輸)

•Anycast (多點備援傳輸)



48

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

49

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

```
|          n bits          | 64-n bits |        64 bits              |
+--------------------------+-----------+-----------------------------+
| global routing prefix    | subnet ID |        interface ID         |
+--------------------------+-----------+-----------------------------+
```

50

Network ID 設定與配送機制

1.採用Neighbor Discovery (ND)指派 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)

51

Interface ID

- Unique to the link
- Identifies interface on a specific link
- Can be automatically derived
  - IEEE addresses use MAC-to-EUI-64 conversion
  - Other addresses use other automatic means
- Can be used to form link-local address
- Can be used to form global address with stateless autoconfiguration

52

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)

53

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 02C0:3FFF:FEBB:9391

54

Global Unicast Address

•Global routing prefix: The global routing prefix is designed to be structured hierarchically by the RIRs and ISPs.

•Subnet ID: An identifier of a link within the site. The subnet field is designed to be structured hierarchically by site administrators.

•Interface ID: Identify interfaces on a link. They are required to be unique within a subnet.

```
|          n bits          |   m bits  |        128-n-m bits          |
+-------------------------+-----------+-----------------------------+
| global routing prefix   | subnet ID |        interface ID          |
+-------------------------+-----------+-----------------------------+
```

```
|          n bits          | 64-n bits |        64 bits               |
+-------------------------+-----------+-----------------------------+
| global routing prefix   | subnet ID |        interface ID          |
+-------------------------+-----------+-----------------------------+
```

55

Global Unicast Address 分配表(部份)

Prefix	說明
2001::/16	IPv6 Internet, ARIN, RIPE NCC, LACNIC
2002::/16	6to4 Tunnel 專用
2003::/16	IPv6 Internet RIPE NCC
2400:0000/19 2400:2000::/19 2400:4000::/21	IPv6 Internet APNIC

56

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

57

IPv4 vs. IPv6

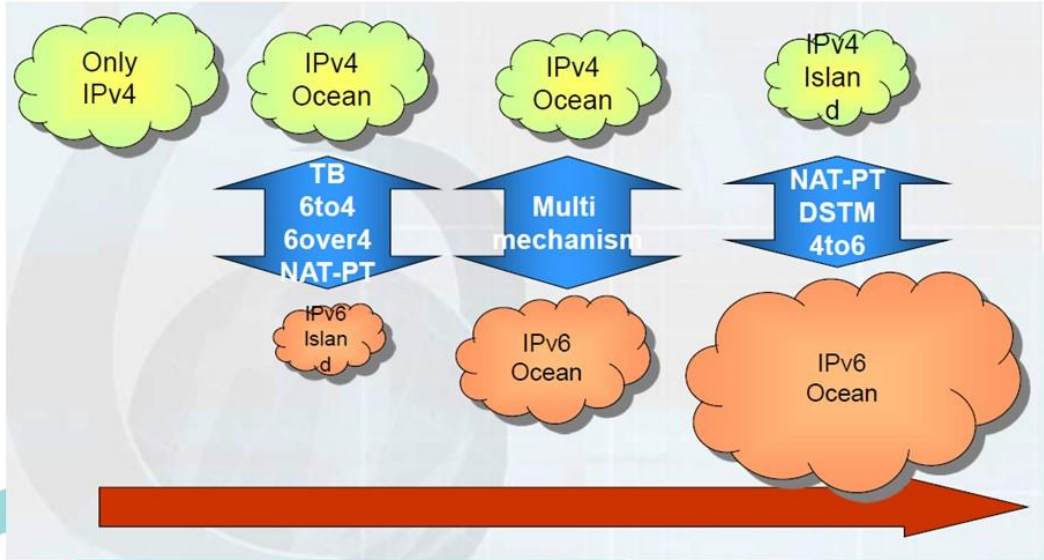
Version	IPv4	IPv6
位址空間	2^32 ＝4,294,967,296	2^128 ≒3.4*10^38
ICMP發放方式	以廣播(Broadcast)方式	以群播(Multicast)方式
QoS策略	推測遺失資料與暫存器	資源保留與優先等級
協定的可擴充性	沒有彈性(最多提供1個Option欄位的擴充)	較有彈性(具有延伸標頭)
IPSec的支援	本身沒有支援，需額外設定	將IPSec納入本身協定中
Plug and Play	需透過DHCP分配IP	具有Statefull (透過DHCPv6)與Stateless (自動組態)分配IP
繞回位址	127.0.0.1	::1
表示方式	十進位表示，以點分隔	十六進位表示，以冒號分隔

58

點進網域新視界！

IPv4/IPv6雙軌環境建置概述

轉型趨勢



60

現有IPv4服務環境的限制

- 無法提供目前網際網路連線所需要的位址空間
- 依靠Broadcast的機制，對網路及伺服器效能產生Overhead
- 沒有普遍被公認而應用於網路設備及應用系統的Quality of Service管理機制。
- 在傳輸時的資料安全性不足

61

現有IPv4服務環境的限制

以上所提之限制，只包含了IPv4缺點之一部份

但已足夠說明IPv4是一個無法滿足現在與未來

網際網路需求的通訊協定

IPv6對於以上的缺點，均內建了解決方案。

62

IPv6可解決的問題

- 在技術問題上，可消除IPv4位址不足，移動性不足的限制，並使用QoS及IPSec的機制提高重要服務的傳輸品質與資料傳輸安全。
- 在經營問題方面，可降低ISP業者的營運成本與克服NAT障礙而產生的技術成本，並可為使用者創造新的服務。

63

IPv6可解決的問題

使用IPv6來解決目前IPv4所產生的問題

會比研發IPv4的新技術來解決IPv4的問題

採用 IPv6 會更為有效

並對ISP業者的投資更有保障

64

三大類過渡技術

1. IPv6/IPv4 Dual Stack

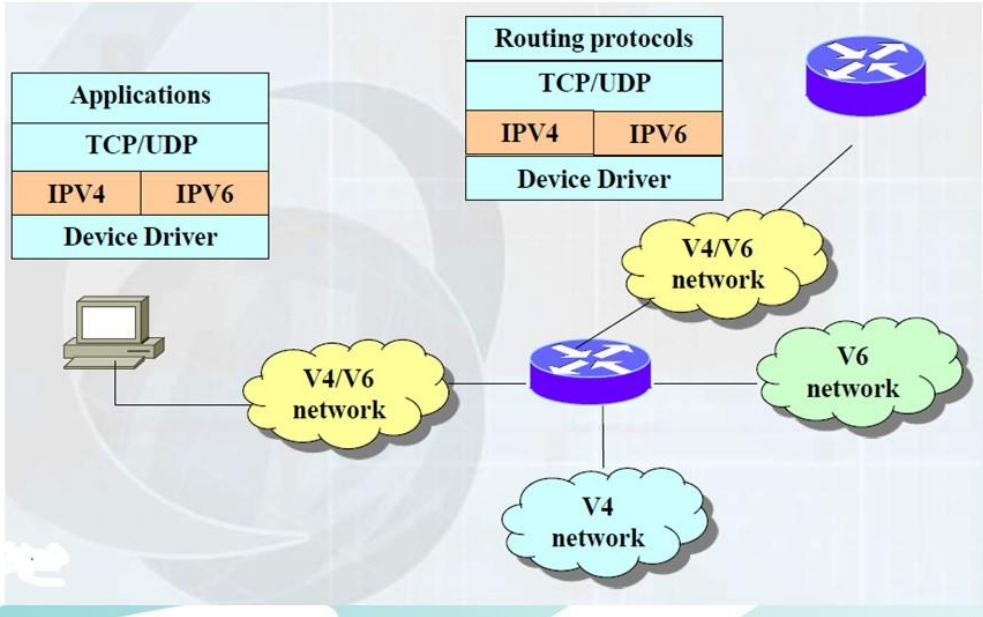
即在同一條線路上

同時提供IPv6及IPv4的通訊協定

最為推薦的方案

65

Dual Stack Mode 示意圖



66

三大類過渡技術

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

67

Tunneling 系統的元件

Tunnel 大致包含了下列元件

- Tunnel Server: 提供Tunnel 服務之局端設備
- 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
- 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

68

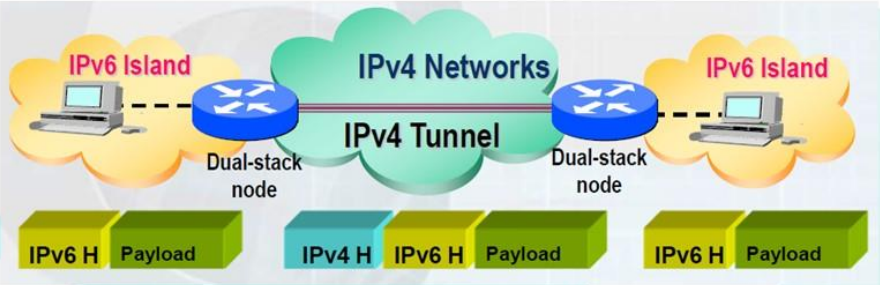
Tunnel 的種類(一)

• Configured Tunnel: 手動設定之Tunnel

適用於ISP與企業用戶間的IPv6 Tunnel連線

優點:安全性高，可支援IPv6 Multicast

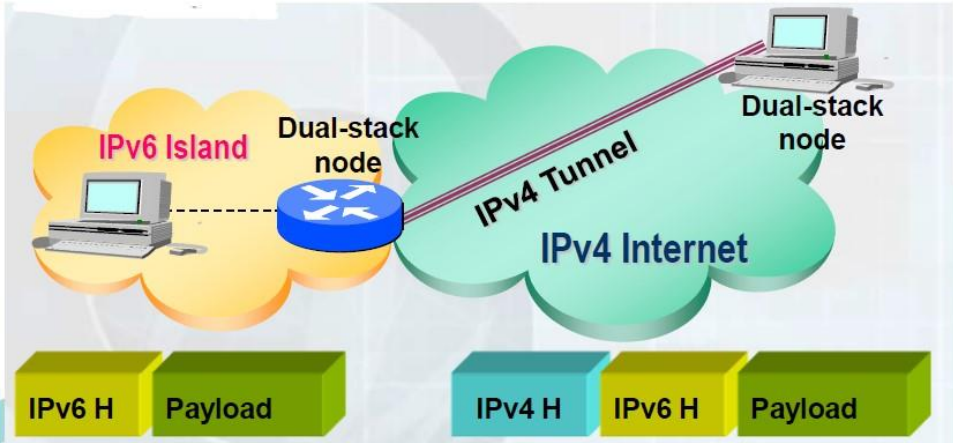
缺點:設定之工作負擔很重



69

Tunnel 的種類(二)

• Automatic Tunnel



70

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部署。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。

71

Tunnel Broker System

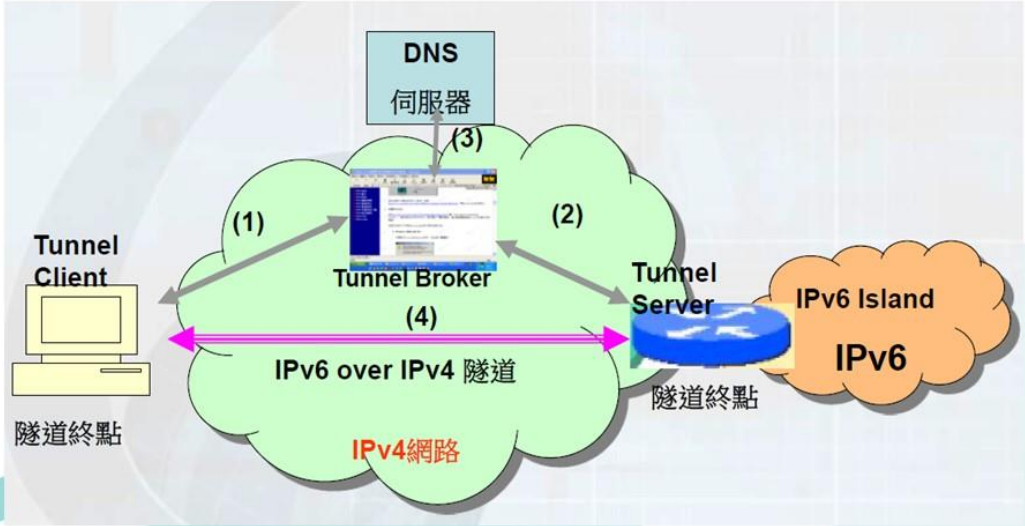
由於Automatic Tunnel 無法有效進行安全管控，而Configured Tunnel 需要太多的手動設定。

而造成ISP不願意提供IPv6 Tunneling Service. Tunnel Broker 可為Configured Tunnel及網管人員提供較佳的管理方式，使IPv6 Tunneling Service 的商業化提供了可行的途徑。

但對一般使用者而言，仍然不夠方便

72

Tunnel Broker 系統示意圖



三大類過渡技術

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

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

75

Translator 技術之限制

事實上，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。

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

76

IPv4/IPv6雙軌網路環境建置

點進網域新視界！

Router, Firewall, Load Balance

第一部分

DHCP

IPv4網路位址指派方式主要有
固定位址指派及動態位址指派兩種

固定位址配置需要手動設定，主要應用於伺服器主機及網路設備，動態位址配置大多透過 DHCP 協定 (Dynamic Host Configuration Protocol)

由 DHCP 伺服器進行位址指派。

78

IPv6同樣提供固定位址指派
在自動位址指派的作法上則有三種方式

- 無狀態位址自動指派
  (Stateless Address Autoconfiguration, SLAAC)
- 無狀態
  DHCPv6(Stateless DHCPv6)
- 全狀態
  DHCPv6(Stateful DHCPv6)。

79

在實際運用上，辦公室環境建議使用Stateful DHCPv6，對資訊安全可以得到最佳管控

家用網路則建議使用Stateless DHCPv6，系統簡化又符合使用需求，純粹的物件感測網路則可以使用SLAAC，設定最為簡單

針對各種不同的IPv6位址指派技術進一步說明

80

人工指派位址

與IPv4網路設定固定位址的做法相同，逐台主機人工指派IPv6位址、預設閘道與DNS伺服器位址

一般而言，路由器與DMZ伺服器的IPv6位址建議採用人工指派，以方便於防火牆設定資安政策，IPv6位址尾碼可以選擇與IPv4位址相同，便於管理及記憶

在使用固定位址的DMZ網段，建議要關閉RA (Router Advertisement)的發送，以避免成為資安漏洞。

81

SLAAC或SLAAC+RDNSS

無狀態位址自動指派(Stateless Address Auto-configuration, SLAAC)

做法是路由器會透過 Multicast 定期發出路由公告 (Router Advertisement) 的封包給用戶端主機，RA的資訊包含 /64 Prefix (Network ID) 及Default Gateway的資訊，主機收到Prefix會與自行產生的Host ID(主機識別碼)組合成為該主機的IPv6位址

82

SLAAC或SLAAC+RDNSS

由於位址指派後即不再持續管理這個位址的使用情形，所以稱為「無狀態」。

上述提到的主機識別碼(Host ID)有兩種產生方式，一種是使用EUI-64運算法，從主機的MAC address轉換而來，另一種是使用亂數法產生

83

SLAAC或SLAAC+RDNSS

早期SLAAC不支援指派DNS伺服器位址

後來的標準解決了這個問題

稱為SLAAC + RDNSS

84

Stateless DHCPv6

這個做法是結合 SLAAC 及 DHCPv6 指派DNS的功能，進行無狀態位址自動指派，以解決前述無法獲得DNS資訊的問題。

在分工上 SLAAC負責 IPv6 位址及 Default Gateway指派，DHCPv6則提供DNS伺服器位址及其他資訊，如NTP

85

Stateless DHCPv6

實作上是透過設定RA封包的一個控制位元(稱為O-bit)來協調用戶端主機的作業。

如果主機收到O-bit為0的RA，就是前述SLAAC的作法；如果O-bit為1，用戶端主機就會再向DHCPv6伺服器請求指派DNS伺服器位址。

86

Stateless DHCPv6

透過SLAAC指派IPv6位址時，並不會進行IPv6位址的定時更新維護及使用追蹤，所以稱為無狀態DHCPv6位址自動指派

在資安管理上不易由IPv6位址追蹤到使用者，因此比較適合不須嚴格進行資安查核管理的場所使用，例如私人家裡。

87

Stateful DHCPv6

在這個做法裡RA只負責提供Default Gateway，而IPv6位址(包括Prefix、Host ID)及DNS伺服器位址的指派均由DHCPv6負責，實作上是透過RA封包的兩個控制位元進行協調。

當用戶端主機收到M-bit及O-bit均為1的RA，主機就會再向DHCPv6伺服器請求指派IPv6位址及DNS伺服器位址。

88

Stateful DHCPv6

由於經由DHCPv6指派IPv6位址時會記錄IPv6位址與MAC位址的對應表，並經由定期更新位址以維護使用紀錄，所以稱為全狀態DHCPv6位址自動指派，對於需要嚴格進行資安查核管理場所是比較恰當的做法。

由於DHCPv6無法指派Default Gateway的資訊，所以Stateful DHCPv6仍需要與RA配合運作，將來DHCPv6可能會發展出提供Default Gateway的機制，這樣就不需要RA的協助。

89

派址方式	預設閘道	Prefix 指派	Host ID 指派	DNS 位址指派	說明	適用環境
人工配置位址	手動設定	手動設定	手動設定	手動設定	穩定可靠、較無資安疑慮，但無彈性、設定麻煩	伺服器及網路設備
SLAAC + RDNSS	RA 指派	RA 指派	EUI-64 或亂數法自動產生	RA 指派	簡單方便，但無法管理位址指派原則及使用紀錄，但大部分作業系統尚未支援 RDNSS	物件連網應用服務
Stateless DHCPv6	RA 指派	RA 指派	EUI-64 或亂數法自動產生	DHCP 指派	簡單方便，但無法管理位址指派原則及使用紀錄，另外，Windows XP 不支援 DHCPv6(可外掛)	家用網路環境
Stateful DHCPv6	RA 指派	DHCP 指派	DHCP 指派	DHCP 指派	可管理位址指派原則及使用紀錄，但 Prefix 與 Gateway 分由 DHCP 及 RA 指派，增加偵錯難度，另外，Windows XP 不支援 DHCPv6(可外掛)	辦公室網路環境

90

IPv4/IPv6雙軌網路環境建置

點進網域新視界！

Router, Firewall, Load Balance

第二部分

防火牆升級IPv6

網際網路的盛行，越來越多的攻擊技術也不斷的產生，如何有效的阻隔外在的威脅，「防火牆」便是一個重要的基本資安元件

「防火牆」(Firewall)是指架設在不同網路之間（例如需要保護的內部網路和公共的網際網路之間）的一系統設備，可能是硬體式的或軟體防護式的安裝於提供服務的設備上。

92

防火牆升級IPv6

在功能上，防火牆可有效地監控內部網路和網際網路之間的任何活動，提供基本的內部網路安全防護

通過監測、限制、更改要通過防火牆的「封包」或「Packet」，屏蔽內部需要受保護的網路資訊、結構和運行狀況，防止資訊洩露，以此來保護網路的安全

93

(一) 防火牆的基本原理

IP位址好比是電腦的「門牌號碼」，一部電腦便可比喻成一棟大廈，連接埠就像這大廈不同的入口，負責各種不同的業務，住戶，行人訪客，駕車的住戶或訪客，以及送貨的貨車等各有不同入口

所有的連接埠都會按通訊協定，被賦予不同編號，防火牆的功能就像大門的警衛保安員，監視進出大廈的訪客，禁止可疑人或物通過

94

(一) 防火牆的基本原理

最基本的防火牆型態是僅由單一的封包過濾器組成，防火牆網路外部的使用者在透過防火牆的封包過濾之後，才能接觸到網路內部的網際網路伺服器。

這種配置下，防火牆管制必須非常嚴格，只讓已經對外開放服務的流量通過，如對電子郵件傳遞，公司公開網站的存取等，合理安全的訪問才能進入防火牆所保護的內部網路系統，而一些危險性較高，不必要的服務如遠端載入等可阻檔在外，並且可以根據可疑份子建立黑名單，禁止這些可疑份子或是 IP address 的封包加以攔阻，不得通過

95

(二) 防火牆的重要性

常有人問「安裝了防毒軟體，還需要加裝防火牆嗎？」其實，防毒軟體與防火牆是相輔相成的

諾大的電腦網路就如同我們生活的國度，防火牆便如同在電腦系統執勤的海關人員，所有入境者，包括惡意程式想透過外部網路侵入內部系統，都要先經過防火牆的查驗，這也是防止駭客的基本防務

96

(二) 防火牆的重要性

防毒軟體其功能就像是機場內的緝毒犬以及操作X光機的檢驗人員，各司其職，構成雙重的保護網，希望能夠有效防止駭客的惡意病毒程式，達到

- 機密性(Confidentiality)
- 完整性(Integrity)
- 可用性(Availability)

避免境內的電腦或資料受到損傷。新型病毒為達到擴散的目的，也經常利用隱藏的連線來感染系統，所以正確設定防火牆也能有效地阻止病毒的攻擊

97

(三) 防火牆的限制

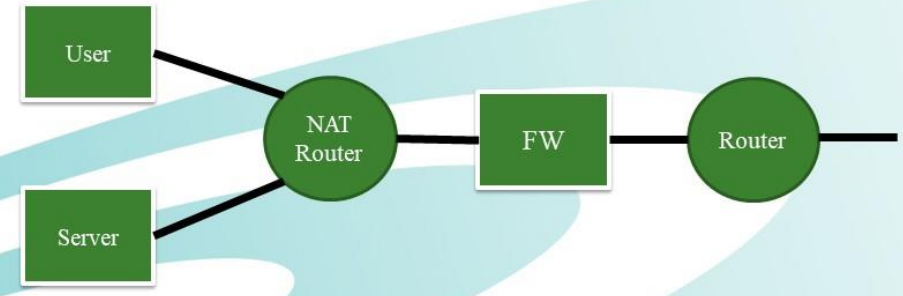
防火牆無法抵擋所有型態的訪問與攻擊，尤其傳統的防火牆運作在網路的第三層與第四層為主，對於應用層的攻擊或是session layer的攻擊往往需要搭配其它資安設備與策略進行防堵

新型態防火牆 Layer 7 Application Firewall

98

(一) 透通模式Transparent Mode

機關IPv4防火牆位置如設置於ISP 路由器與內部NAT路由器之間，並採用Transparent 透通模式進行運作，內部路由器最少有三個介面，一個與防火牆介接，一個與內部一般使用者連接，一個與伺服器區塊連接



99

(一) 透通模式Transparent Mode

採用本架構可以限制外來的訪客對於內部網路的存取，並且在不改變內部原有的設備設定，以提供內部使用者安全的IPv4/IPv6對外存取服務。

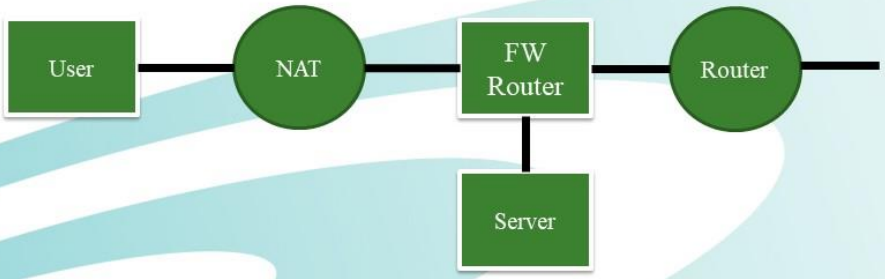
內部使用者若採用IPv6 Public IP address，不再經由NAT或PAT位址轉換，可直接提供IPv6接取服務。

防火牆可抵擋外部IPv4/IPv6對於內部使用者的所有連線訪問。

100

(二) 路由模式Route Mode

機關IPv4防火牆位置如設置於ISP 路由器與內部路由器之間，並採用Route Mode路由模式進行運作，防火牆最少有三個介面，一個與外部ISP業者介接，一個與內部路由連接，一個與DMZ伺服器區塊連接



101

(二) 路由模式Route Mode

採用本架構可以限制外來的訪客對於內部網路的存取，並且限制DMZ區對於內部使用者的存取，可以提供內部使用者安全的IPv4/IPv6對外存取服務。

內部使用者若採用IPv6 Public IP address，不再經由NAT或PAT位址轉換，可直接提供IPv6接取服務。

防火牆可抵擋外部IPv4/IPv6對於內部使用者的所有連線訪問。

102

點進網域新視界！

網路升級流程
步驟和檢查項目清單

網路升級流程步驟和檢查項目清單

升級清查目的在針對各項網路應用服務系統進行IPv6支援能力調查，藉以評估網路升級需進行之工作內容、作業程序及時程規劃。

升級清查作業從服務系統角度出發，逐一填寫對外提供服務的應用服務系統，其次應依據各服務系統逐一清查相關之軟硬體設備，包括伺服器、服務系統或軟體、基礎網路設備及其他相關設備等，參考步驟如下。

104

(一) 評估現有網路環境

網路設備種類甚多，唯有釐清設備功能，才能規劃IPv6升級優先順序，其中需調查項目如下：

- 技術人員IPv6相關能力調查
- 資訊應用服務系統(自行開發、委外設計或市購套裝軟體)
- 網路架構圖(區域網路、DMZ、連外網路、接取網路、核心網路、機房等)
- 硬體設備(使用年限與IPv6支援程度)
- 評估現有網路設備之屬性

105

大多數網路設備可分類成下列四項

1. 主機(Host)

2. Layer 2 交換器

3. Layer 3 網路設備

4. 網路安全防護設備

106

1. 主機(Host)：

單埠接收與傳送IPv6封包
個人電腦、筆記型電腦、伺服器
平板、手機

以下分類不屬於 Host
Layer 2交換器
Layer 3網路設備
網路安全防護設備

107

2. Layer 2交換器：

根據網路封包的Layer 2標頭執行網路封包交換技術，大多數設備不需要進行IPv6升級，亦即無需更換或進行韌體升級，如消費者等級Layer 2交換器和企業等級Layer 2交換器等。

但是部分企業/ISP等級Layer 2交換器功能較強，仍會偷偷看到網路封包的Layer 3標頭處理，如網管IP、Multicast Snooping或Protocol-Based VLAN等，亦需將此類設備納入IPv6升級考量。

108

3. Layer 3網路設備：

根據網路封包的目的位址欄位進行IPv6封包轉送處理之節點，例如：

路由器Router

Layer 3交換器

此為提供IPv6網路運作的基礎

109

4. 網路安全防護設備

此為選擇性地攔阻威脅性之網路封包或者限制網路流量的IPv6節點，例如：

防火牆(Firewall)

入侵偵測系統(IDS)

入侵防護系統(IPS)

110

(二) 規劃IPv6升級策略

根據上述調查結果，可大致掌握現有網路設備特性與屬性。接著需制定IPv6導入之網路範疇與時程，本步驟僅提供3個升級重要參考指標，作為規劃參考依據：

1. 降低導入成本：網路設備升級至IPv6非一蹴可幾，礙於導入預算成本之限制，需針對現有網路設備規劃階段性的升級工作

111

(二) 規劃IPv6升級策略

2. 規劃重要網路應用服務升級：

網路管理員可針對網路流量大或重要之網路應用服務，調查其服務之主要網路傳輸設備，並評估運作模式是否與IP層有關，以作為未來導入IPv6首要升級重點

3. 規劃升級時程與順序：

有些重要的網路設備，流量雖不大，但是卻有立即性的升級需求，如IDC機房的服務，因IPv4位址已經用鑿，且此類型服務大多直接提供對外服務，因此較有機會進行，則規劃上建議優先考量此設備

112

(三) 評估重要依據

建議以雙協定(Dual Stack，同時支援IPv4與IPv6)為首要目標，IPv6部署先由骨幹單一網路節點下手，逐步擴增支援IPv6功能的網路節點，最後連接成IPv4/v6網路，並達到全面性的IPv6網路佈建。

113

(三) 評估重要依據

下列提供三種主要準則
作為網路設備升級模式之參考：

準則1：

原有網路設備已內建支援IPv6功能，網路管理員需要執行基本IPv6指令，如設定、啟動與測試等步驟。此升級方式成本較低廉，技術人員僅需熟悉IPv6設定，即可達到IPv6之目的。

114

(三) 評估重要依據

準則2：

原有網路設備未支援IPv6，但透過官方所釋出之新版本韌體，僅需根據官方標準升級程序，更新升級後即支援IPv6。

115

(三) 評估重要依據

準則3：

原有網路設備未支援IPv6，且未來新版也不支援IPv6；可採取下列步驟：

(1) 要求網路設備廠商修改程式碼以支援IPv6

(2) 找尋其他的替代網路設備

116

經由詳細評估後，應明訂硬體設備與資訊應用服務系統支援IPv6所需工作項目，例如

- 韌體升級
- 硬體更換
- 修改網路架構
- 軟體修改
- 重購軟體

並進行軟硬體升級之經費估算。

117

網路應用服務清查表

服務系統編號	1
服務 類別	DNS
服務系統名稱	DNS
服務內容說明	提供DNS解析服務
網站名稱(URL)	dns.info.gov.tw
重要國際服務	N
具指標性服務	Y
行動服務應用	N
服務使用率高	Y
年度規劃改版	N
主/次要服務	主要
負責 單位	資訊中心
負責 人員	XXX
建議升級年度	2019年

118

服務系統編號
軟硬體編號
品名
硬體廠牌型號或軟體供應商
作業系統/軟體版本
距離報廢/授權年限
已內含IPv6能力
已導入IPv6
建議升級年度
硬體升級方式
軟體升級方式

119

網路升級檢測

網路除錯通常使用 ping6 與 tracert6

如要進行此類測試，應事先檢查網路上相關設備是否已開放此類封包訊息傳送，如路由器、防火牆、伺服器、終端電腦等

如無法排除封包阻擋的問題，可以改用應用服務層協定(如port 80)進行測試

以下提供檢測IPv6能力的測試網站：

120

https://test-ipv6.com/

121

Chrome瀏覽器-擴充功能

122

行動網路IPv6設定

- 手機網路設定說明

123

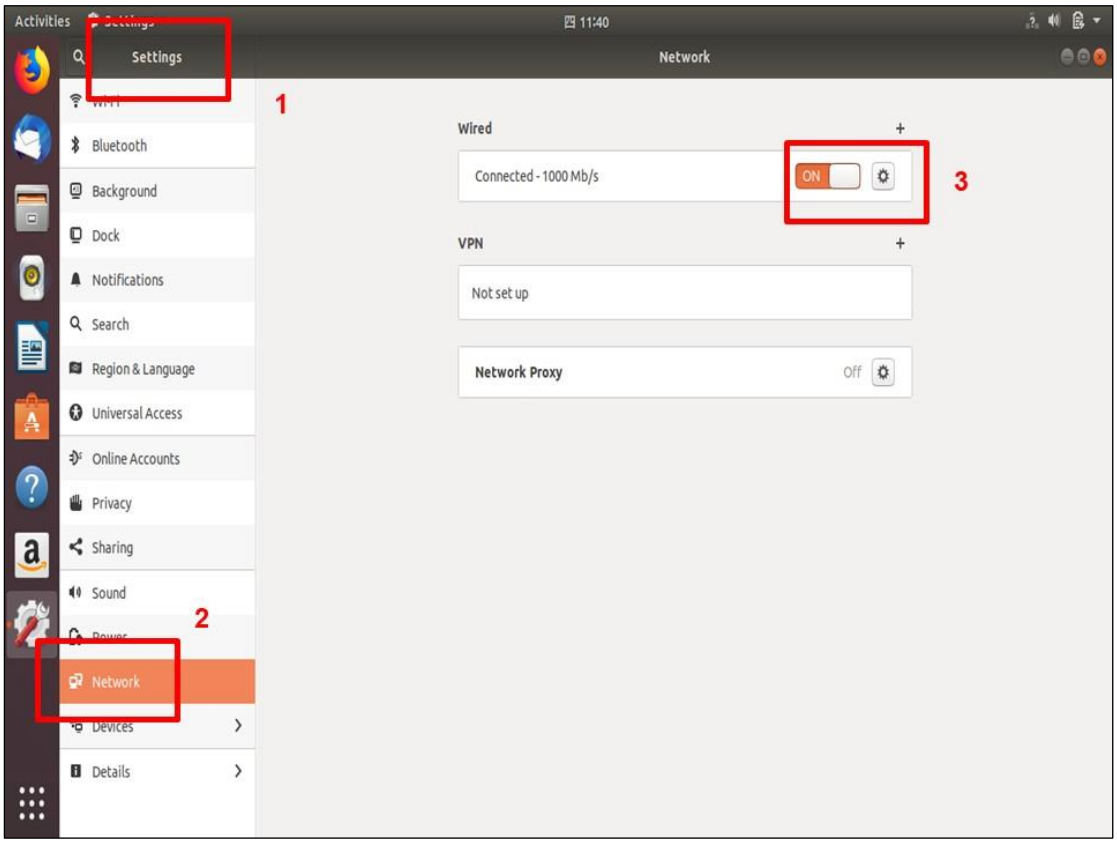
點進網域新視界！

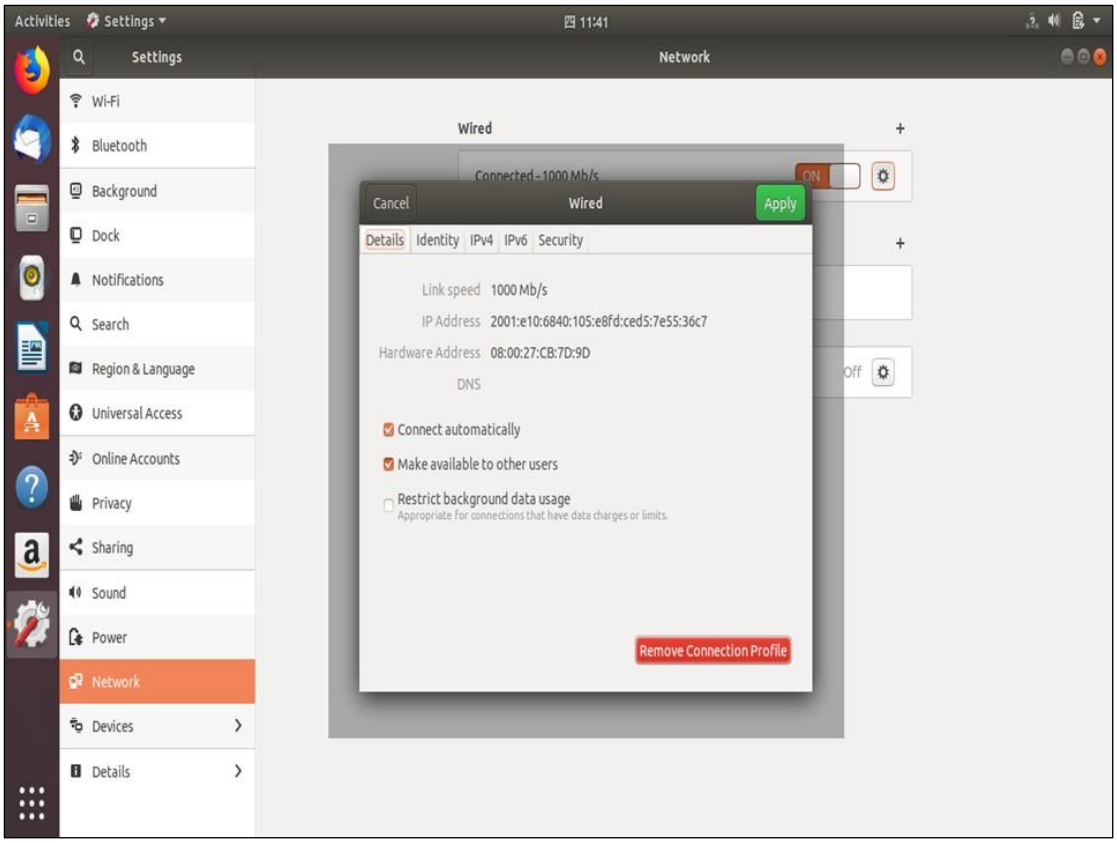
IPv6建置示範
Ubuntu
作業系統

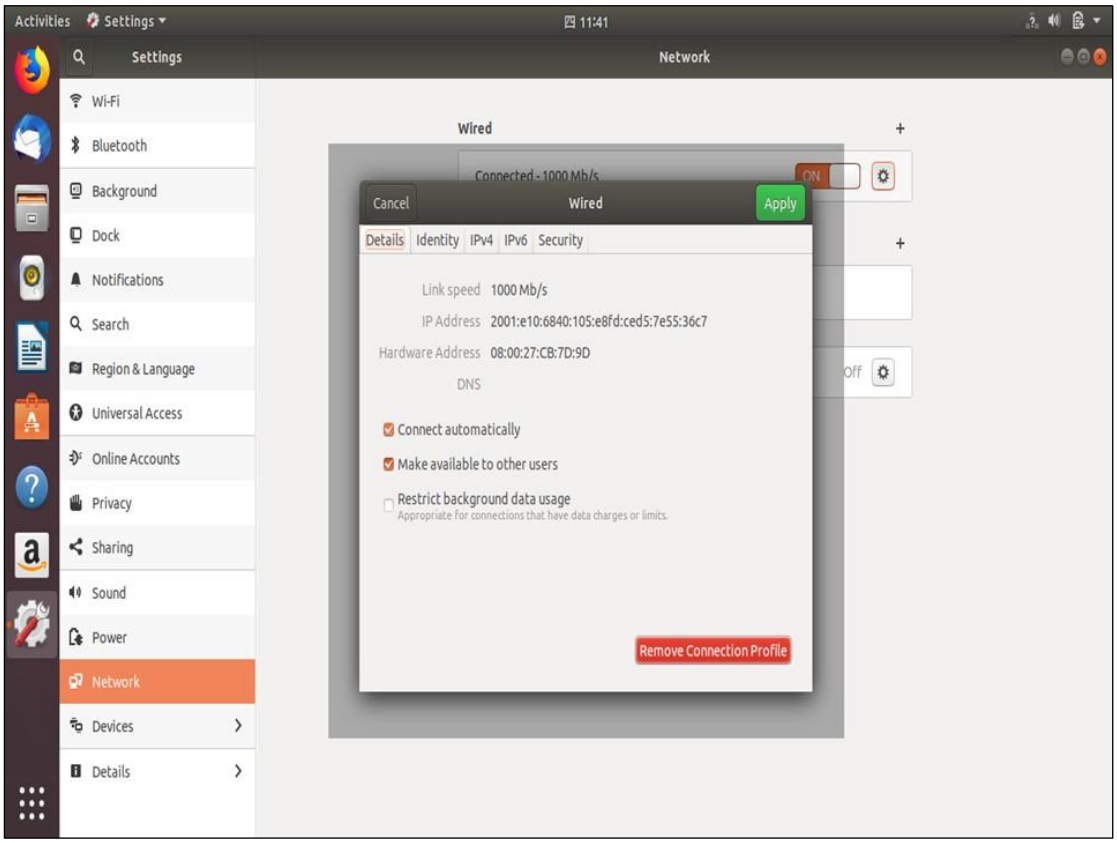
Ubuntu 20.04 server

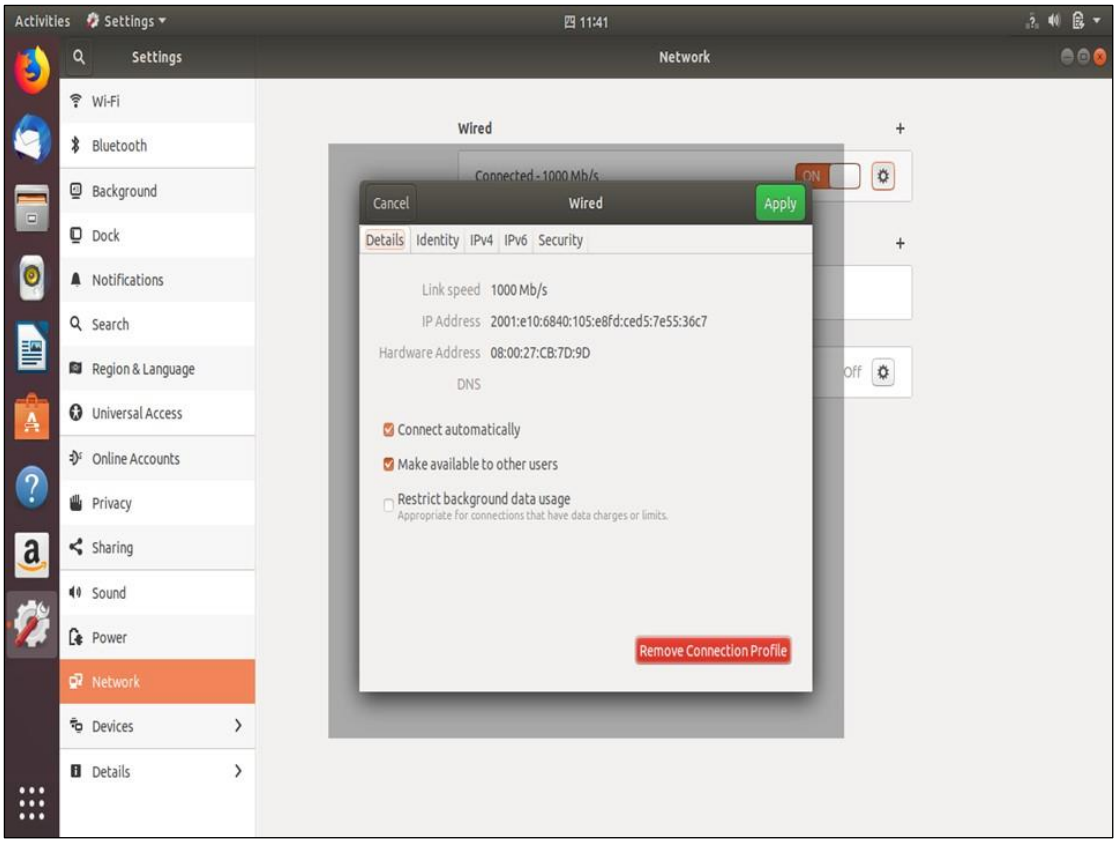
```
root@ipv6:~# nano /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses:
      - 163.18.23.251/24
      - 2001:288:8005:23::251/64
      gateway4: 163.18.23.254
      gateway6: 2001:288:8005:23::254
      nameservers:
        addresses:
        - 163.18.1.7
        - 2001:288:8005:1::7
        search:
        - nkfust.edu.tw
  version: 2
```

125

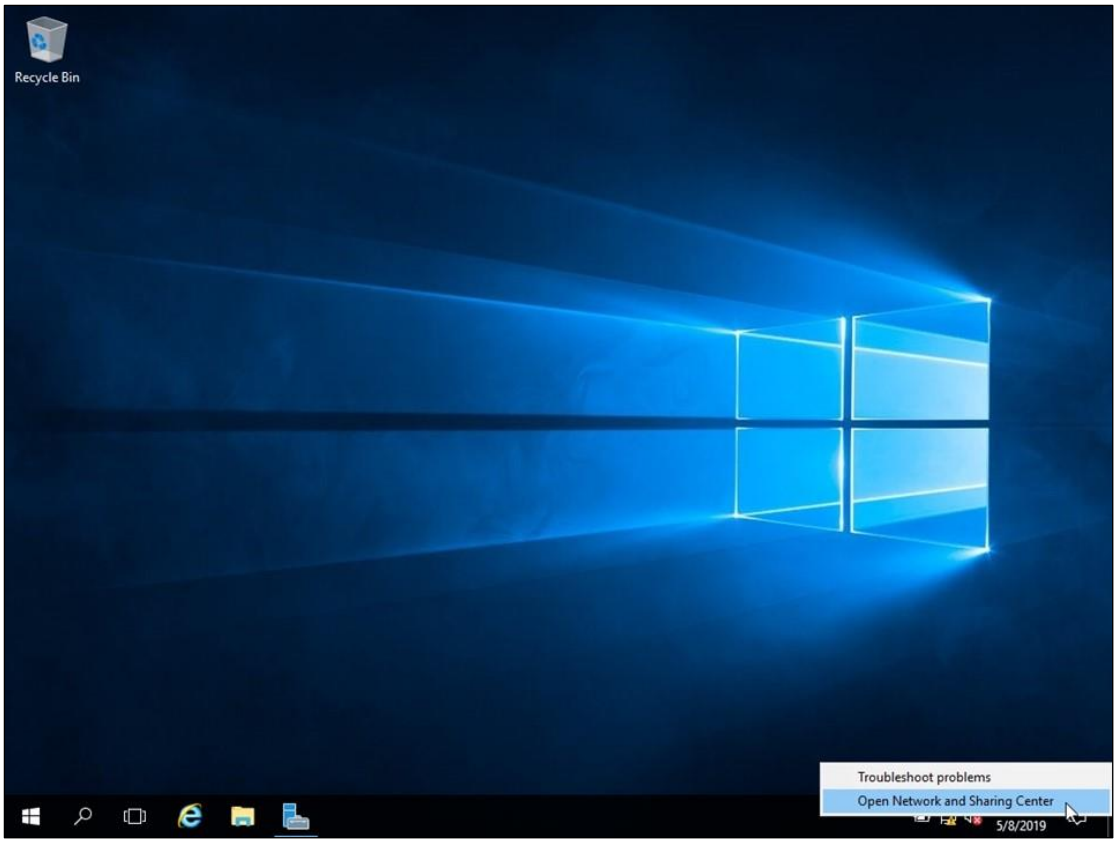


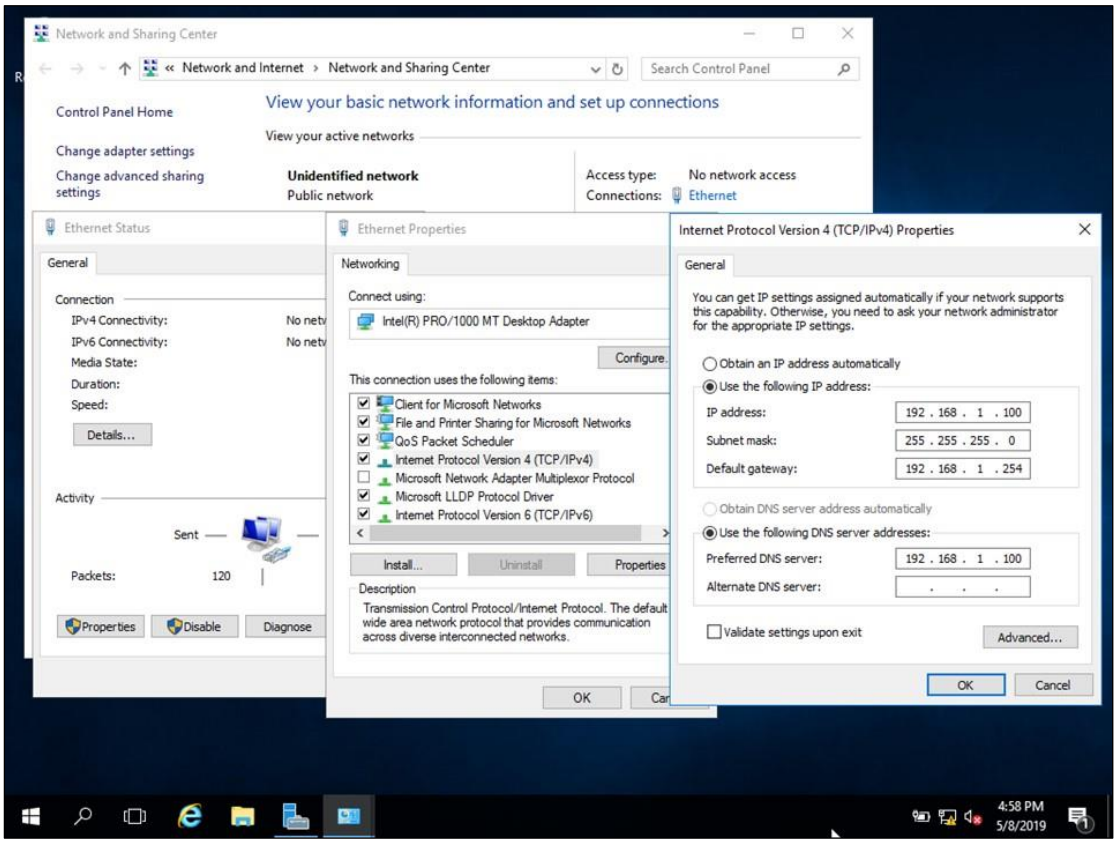

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Off
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile

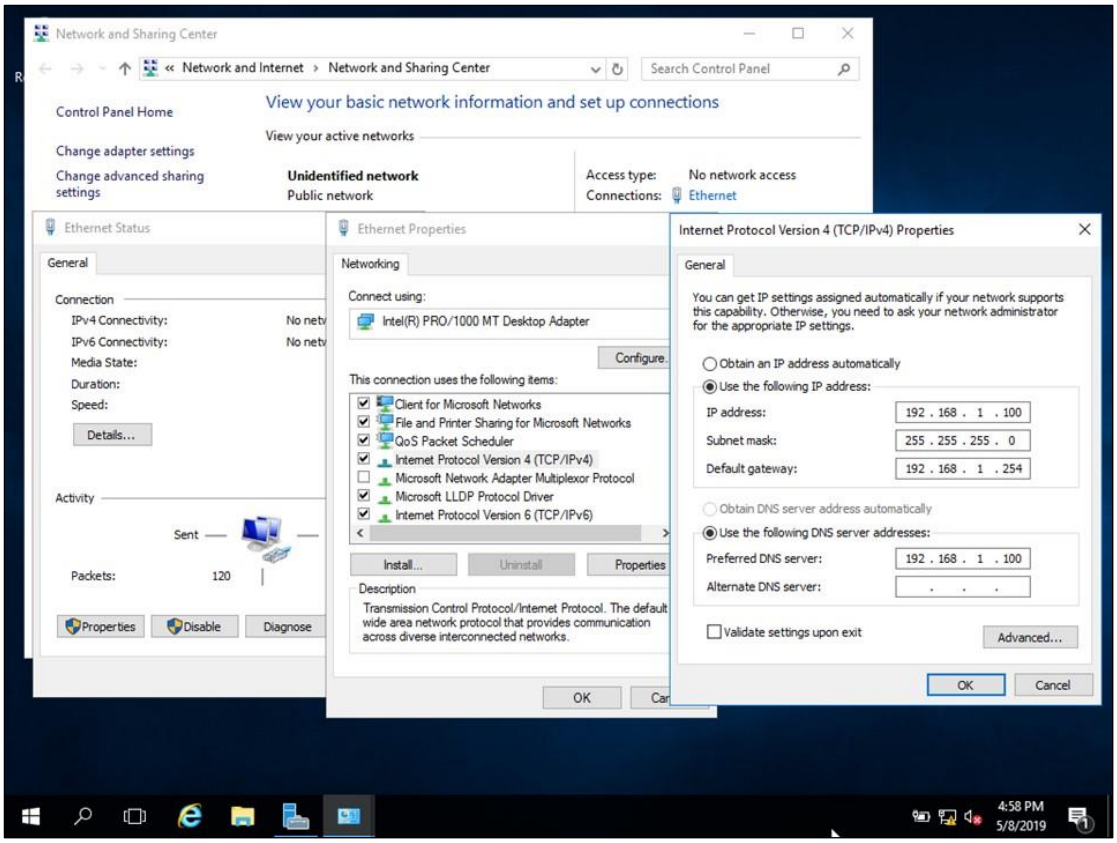

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Off
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile


Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Connected - 1000 Mb/s
ON
Off
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
Hardware Address 08:00:27:CB:7D:9D
DNS
Connect automatically
Make available to other users
Restrict background data usage
Appropriate for connections that have data charges or limits.
Remove Connection Profile

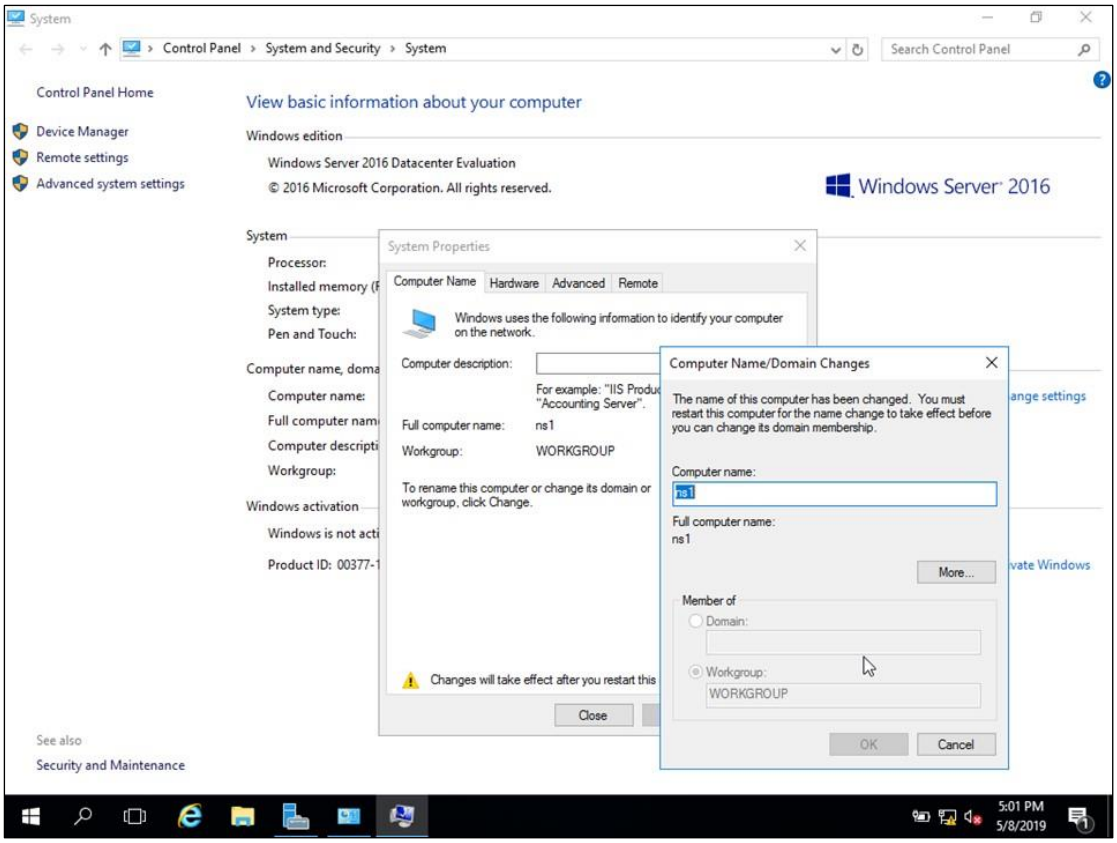

點進網域新視界！
IPv6建置示範
Windows server 2016
作業系統

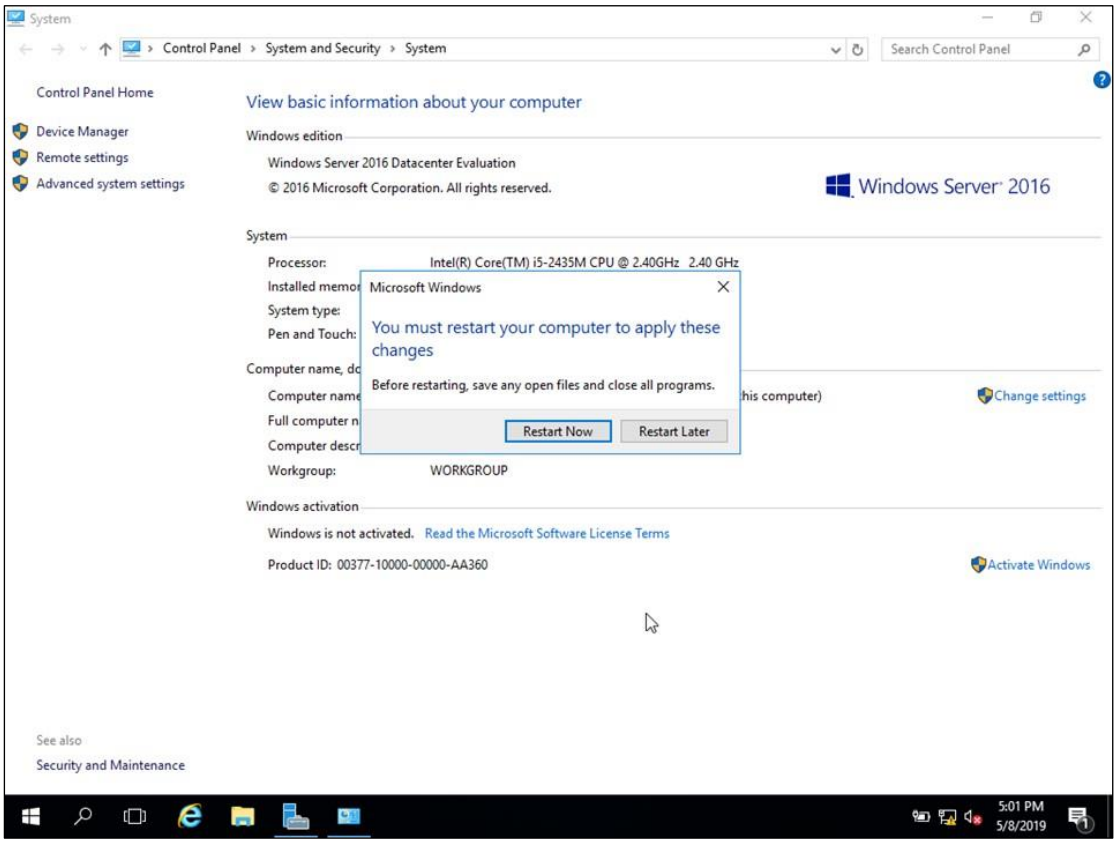

Recycle Bin
Troubleshoot problems
Open Network and Sharing Center
5/8/2019

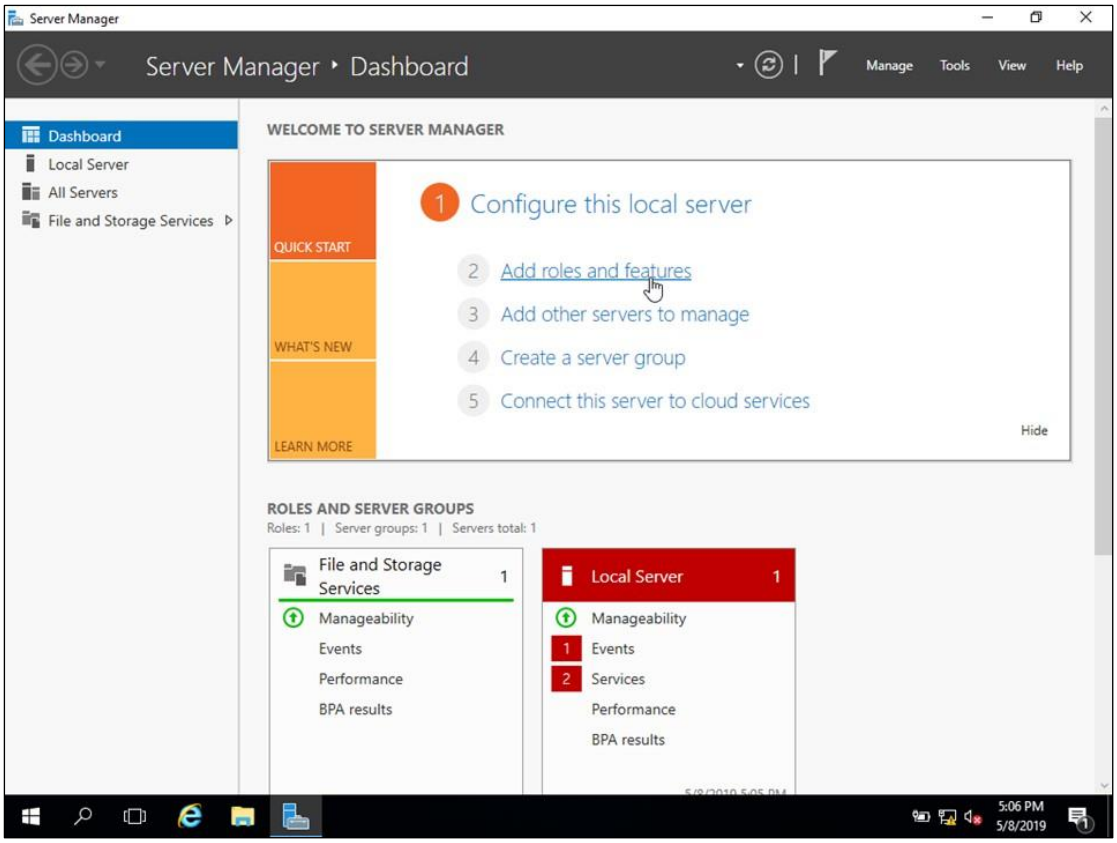

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
4:58 PM
5/8/2019

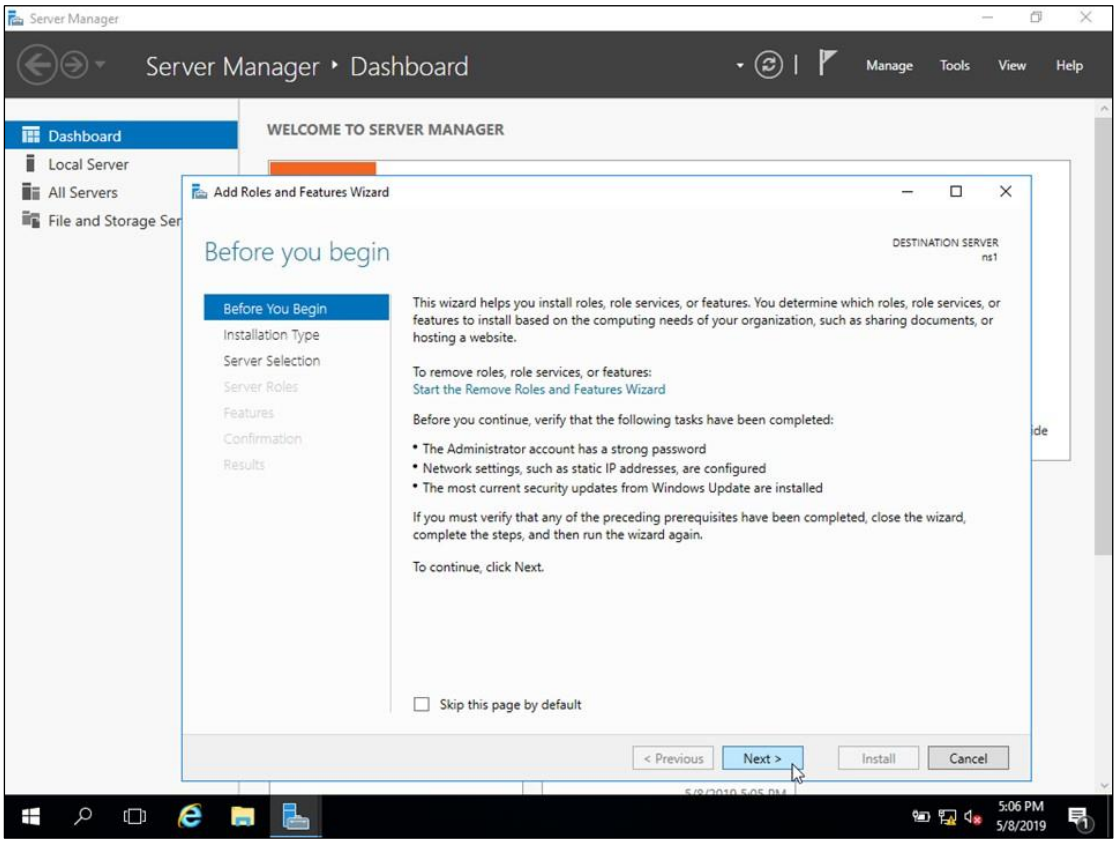

Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
View your active networks
Change adapter settings
Change advanced sharing settings
Unidentified network
Public network
Access type: No network access
Connections: Ethernet
Ethernet Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Packets: 120
Properties
Disable
Diagnose
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 1 . 100
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
4:58 PM
5/8/2019

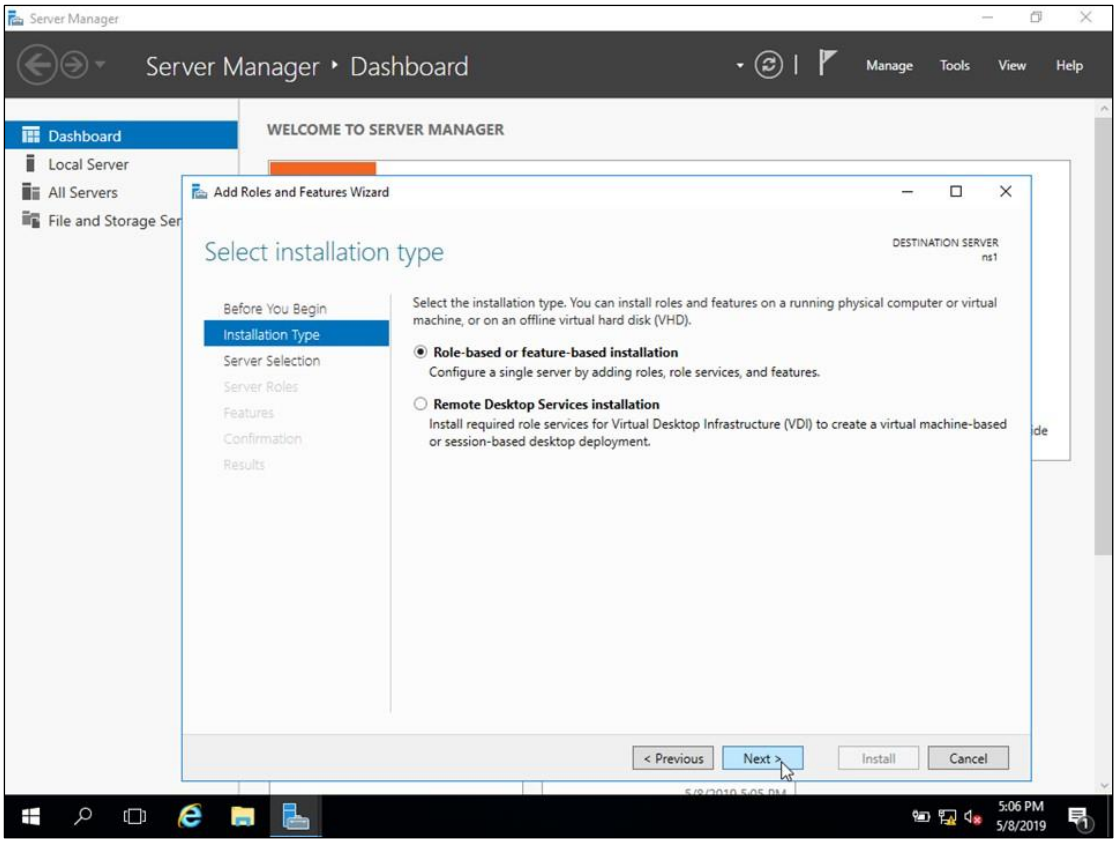

點進網域新視界！
IPv6建置示範
DNS Server

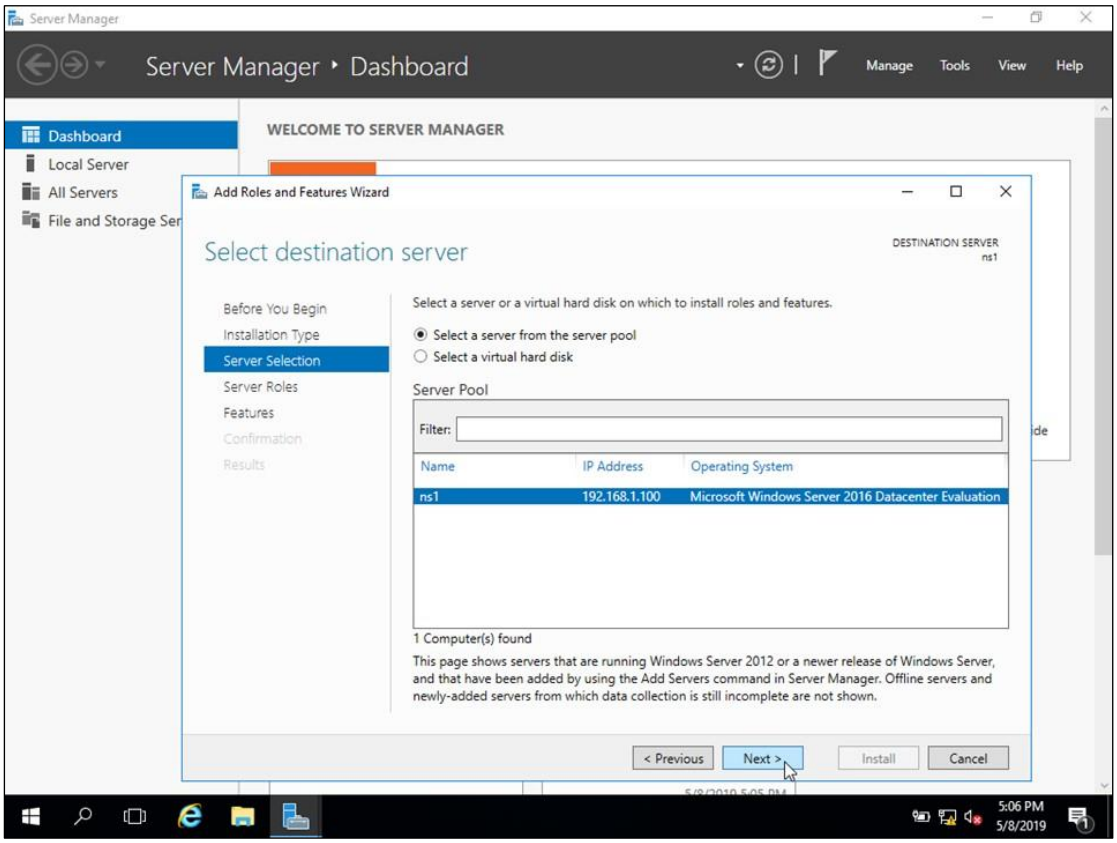

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
View basic information about your computer
Device Manager
Remote settings
Advanced system settings
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor:
Installed memory (
System type:
Pen and Touch:
Computer name, doma
Computer name:
Full computer nam
Computer descripti
Workgroup:
Windows activation
Windows is not acti
Product ID: 00377-1
System Properties
Computer Name
Hardware
Advanced
Remote
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Produc "Accounting Server".
Full computer name: ns1
Workgroup: WORKGROUP
To rename this computer or change its domain or workgroup, click Change.
Changes will take effect after you restart this
Close
Computer Name/Domain Changes
The name of this computer has been changed. You must restart this computer for the name change to take effect before you can change its domain membership.
Computer name:
ns1
Full computer name:
ns1
More...
Member of
Domain:
Workgroup:
WORKGROUP
OK
Cancel
ange settings
vate Windows
See also
Security and Maintenance
5:01 PM
5/8/2019

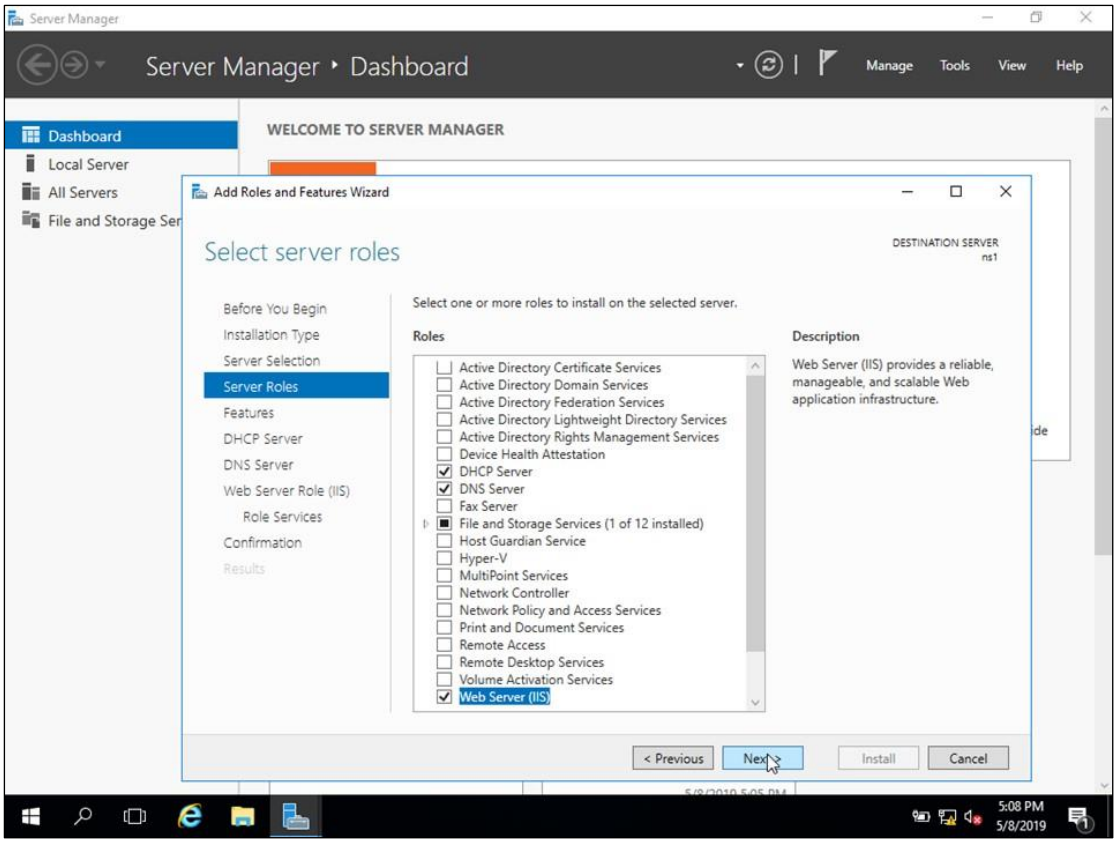

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
View basic information about your computer
Device Manager
Remote settings
Advanced system settings
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows Server 2016
System
Processor: Intel(R) Core(TM) i5-2435M CPU @ 2.40GHz 2.40 GHz
Installed memor
System type:
Pen and Touch:
Computer name, do
Computer name
Full computer n
Computer descr
Workgroup: WORKGROUP
Microsoft Windows
You must restart your computer to apply these changes
Before restarting, save any open files and close all programs.
Restart Now
Restart Later
his computer)
Change settings
Windows activation
Windows is not activated. Read the Microsoft Software License Terms
Product ID: 00377-10000-00000-AA360
Activate Windows
See also
Security and Maintenance
5:01 PM
5/8/2019

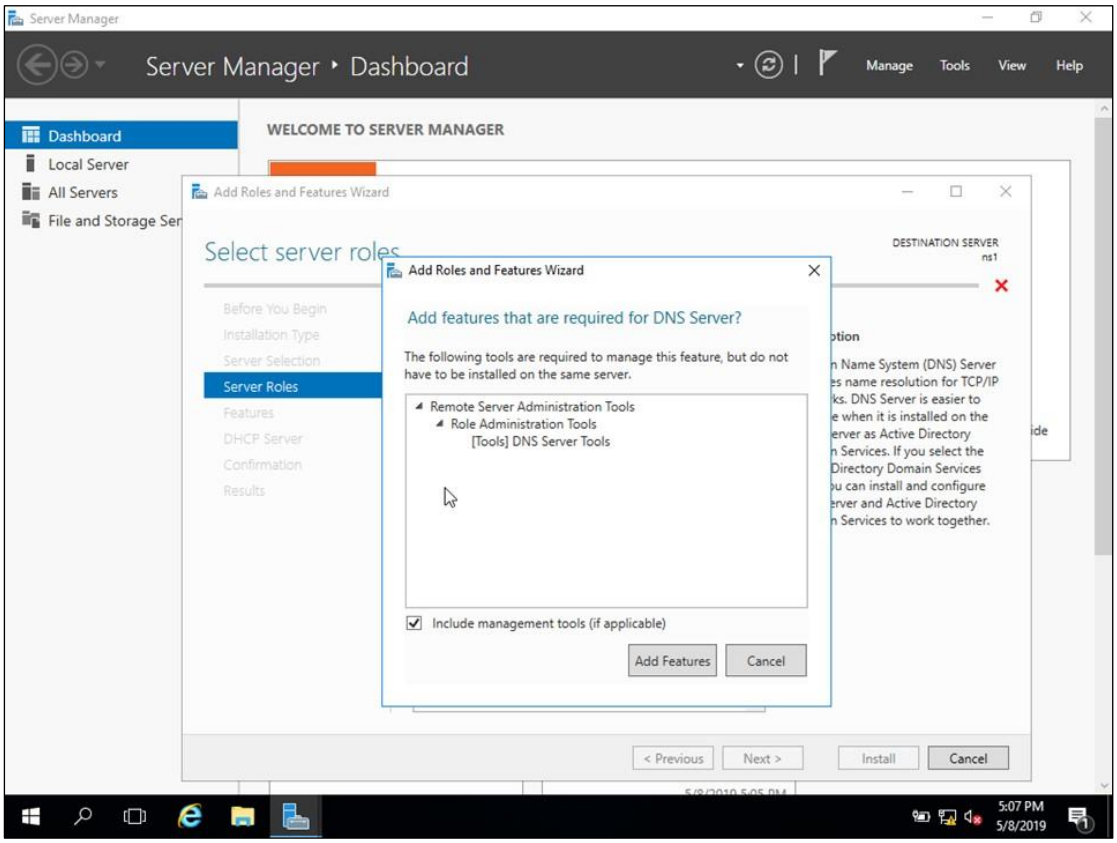

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
1 Events
2 Services
Performance
BPA results
5:06 PM
5/8/2019

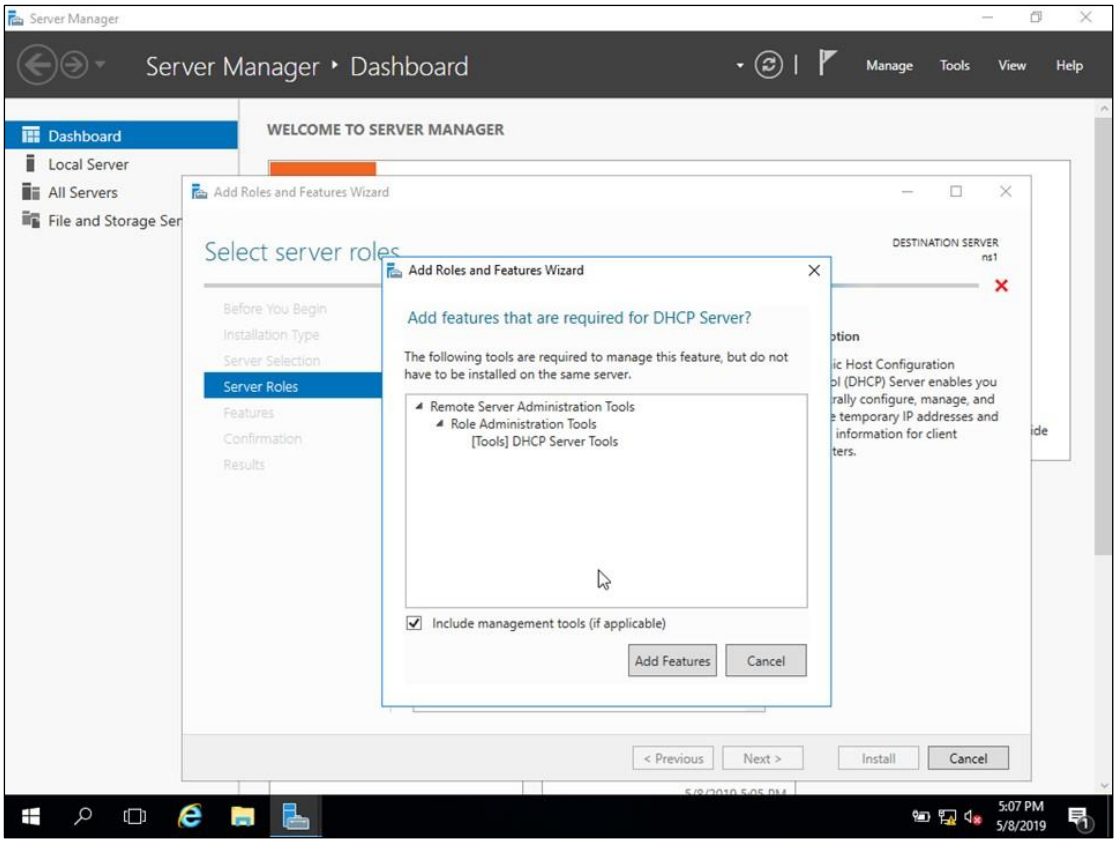

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

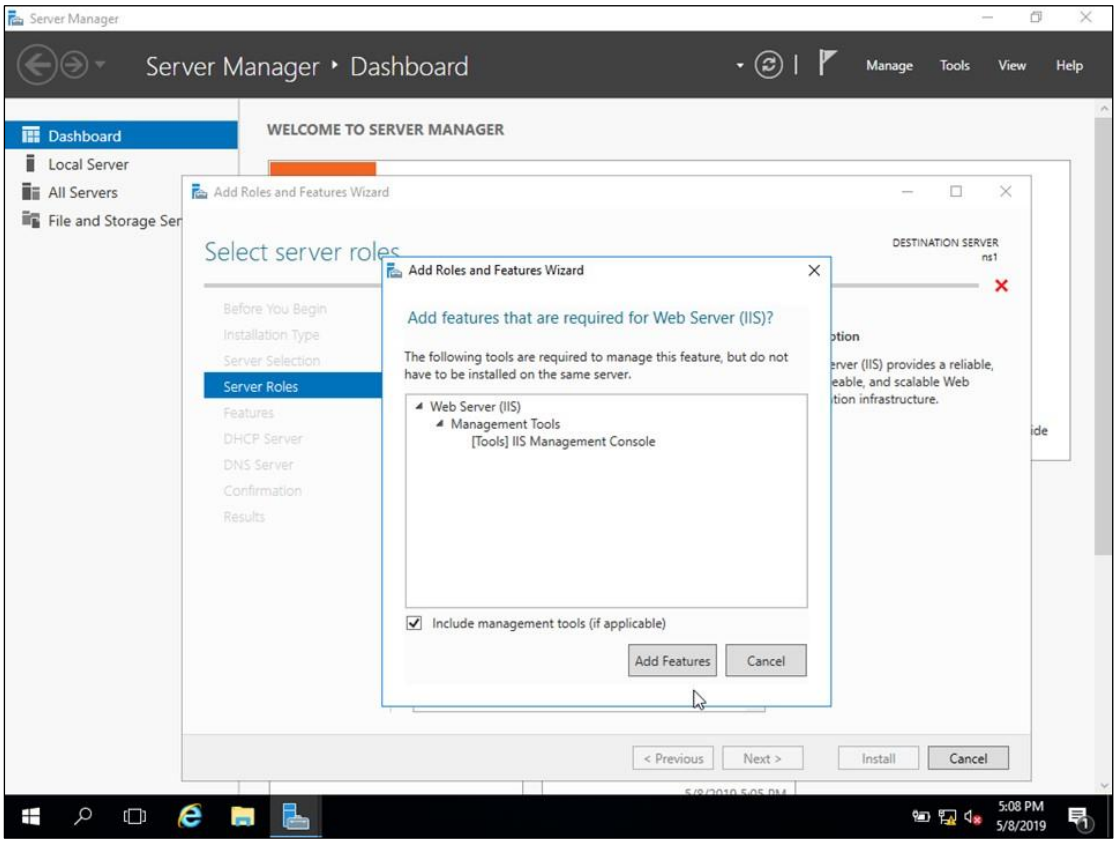

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

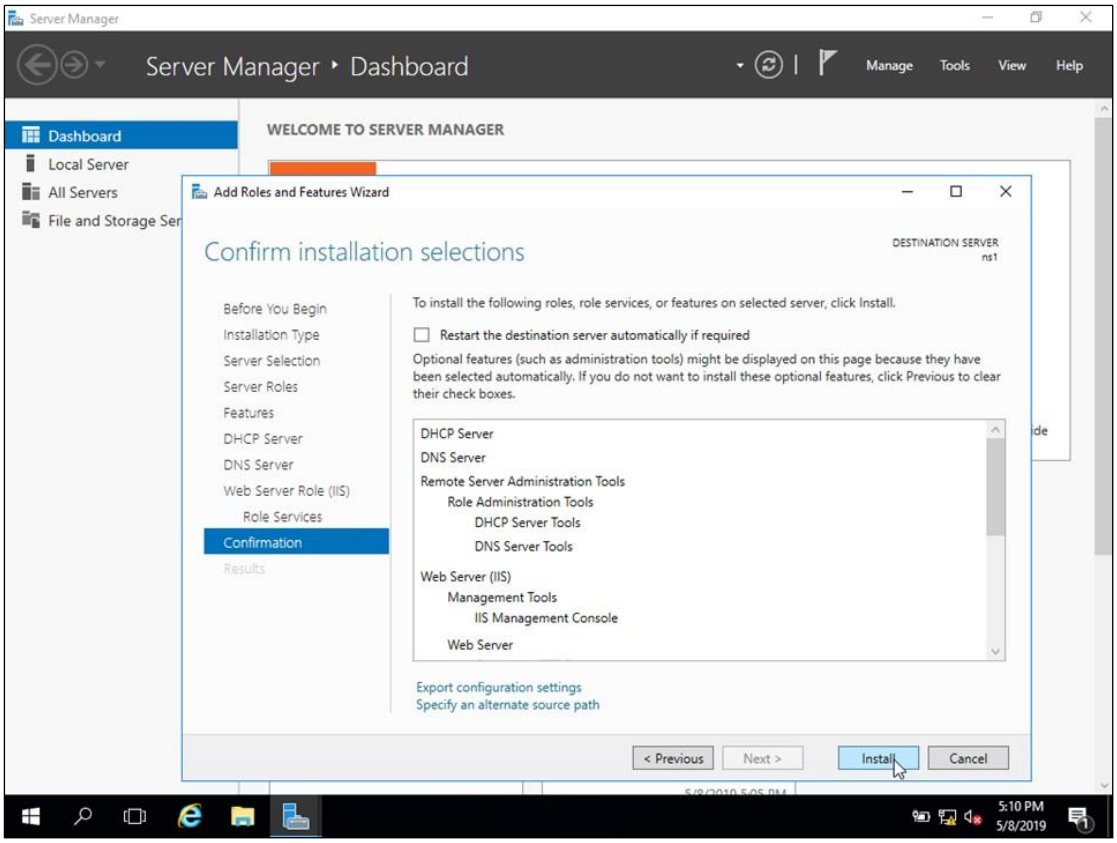

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
ns1
192.168.1.100
Microsoft Windows Server 2016 Datacenter Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
5:06 PM
5/8/2019

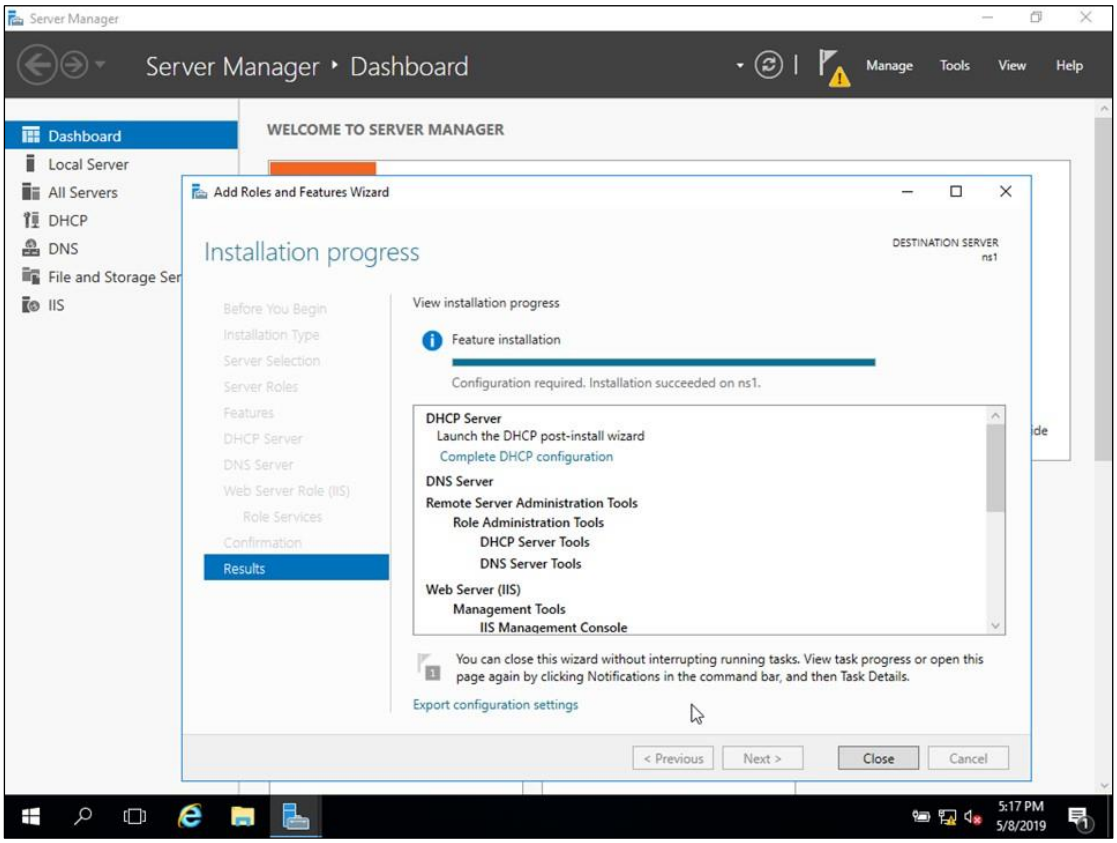

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

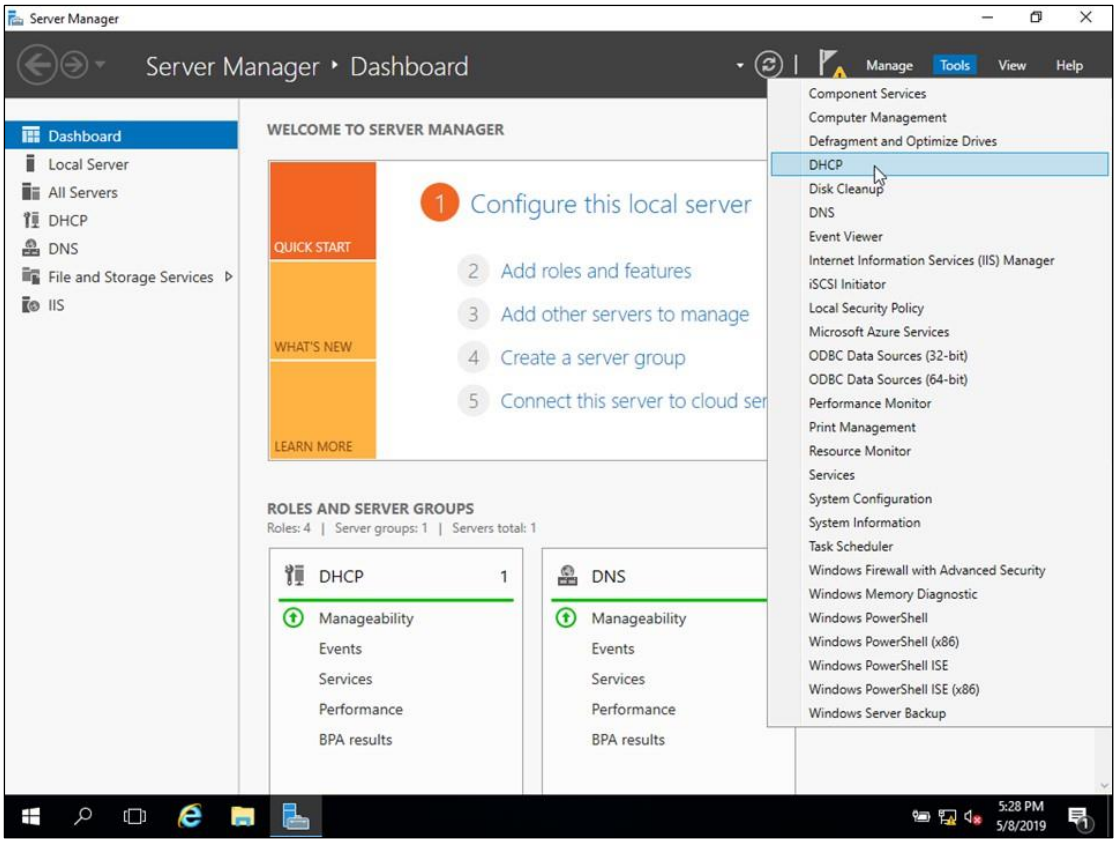

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
Confirmation
Results
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

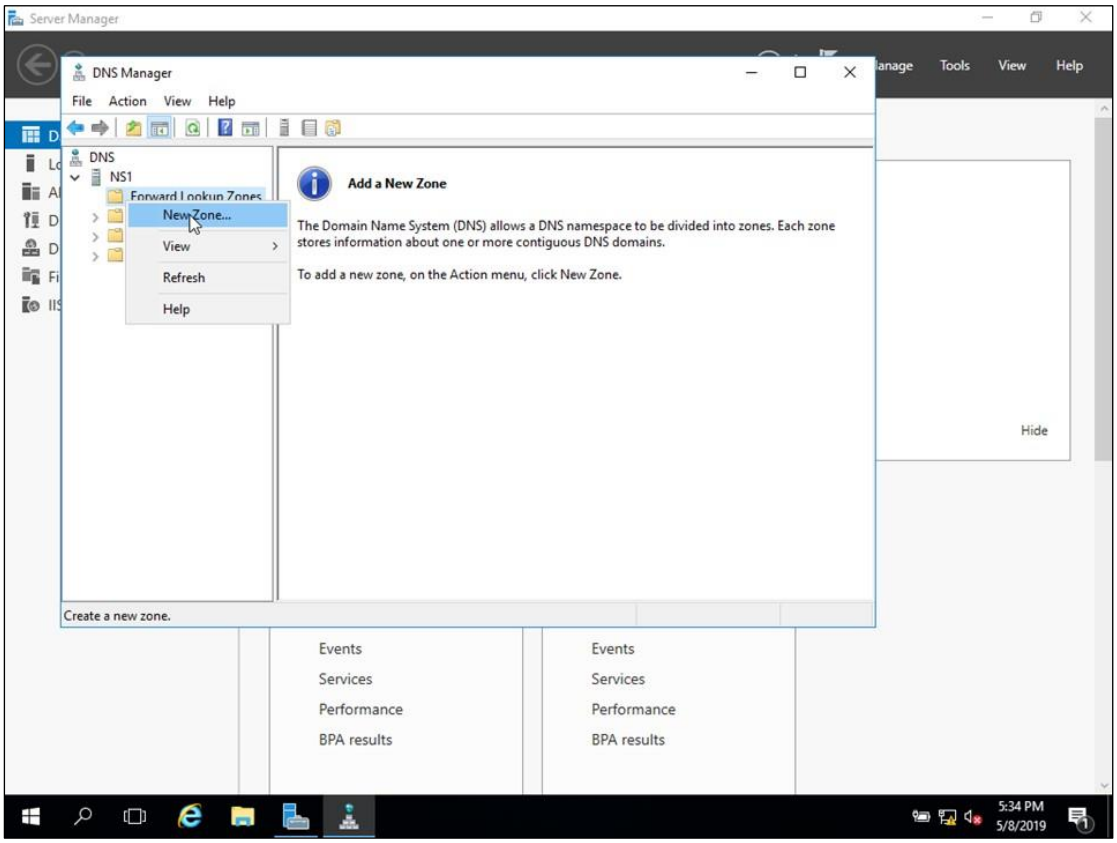

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DHCP Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

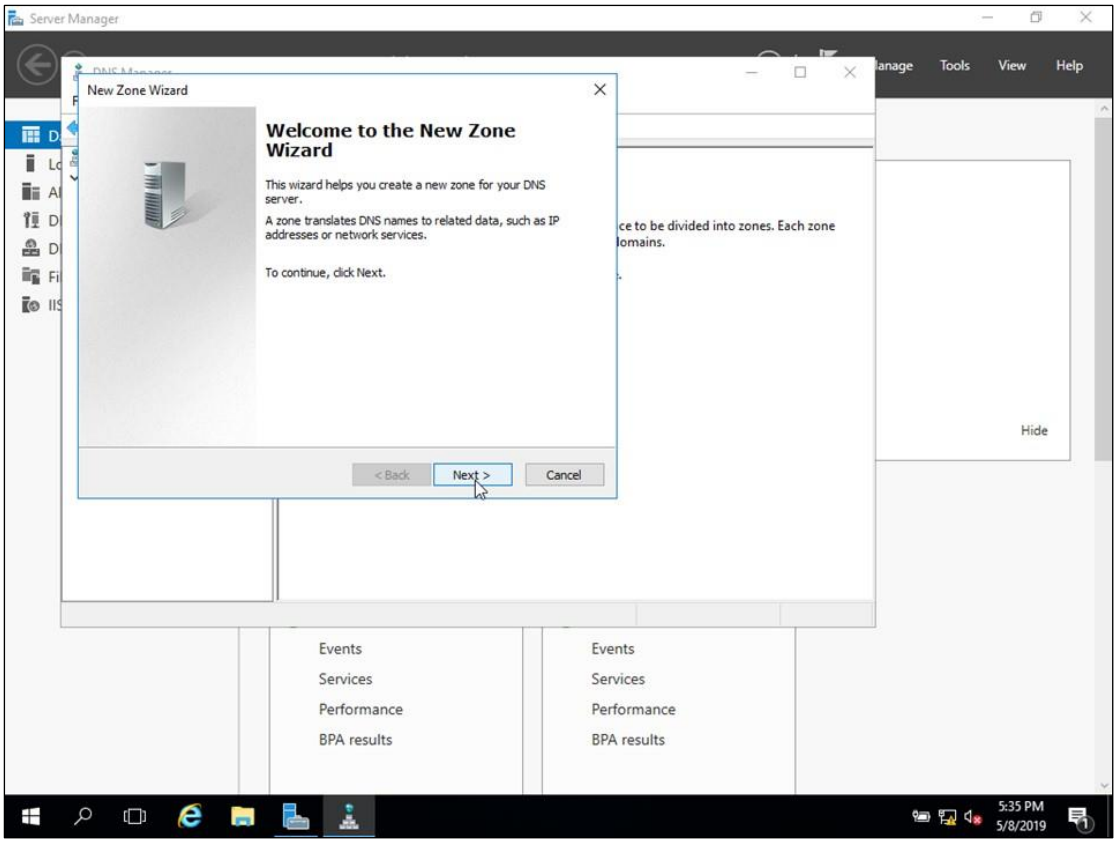

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
5:08 PM
5/8/2019

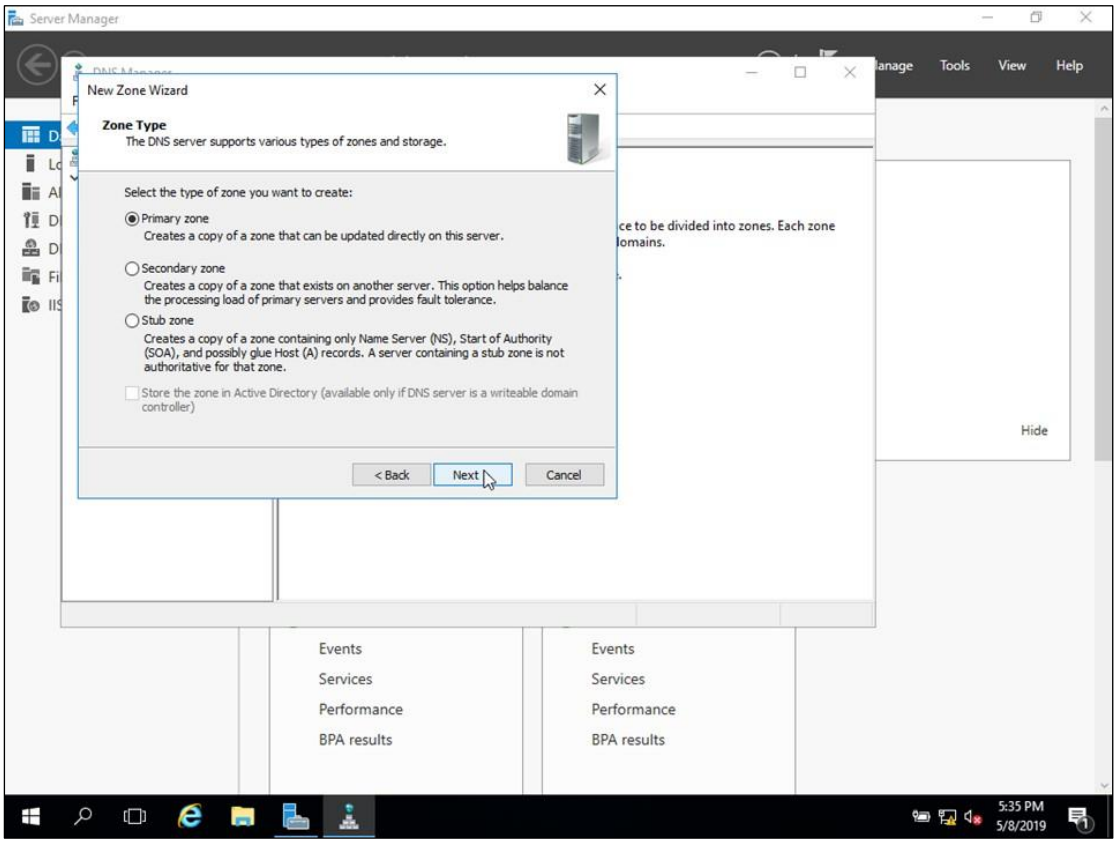

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
DHCP Server
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
5:10 PM
5/8/2019

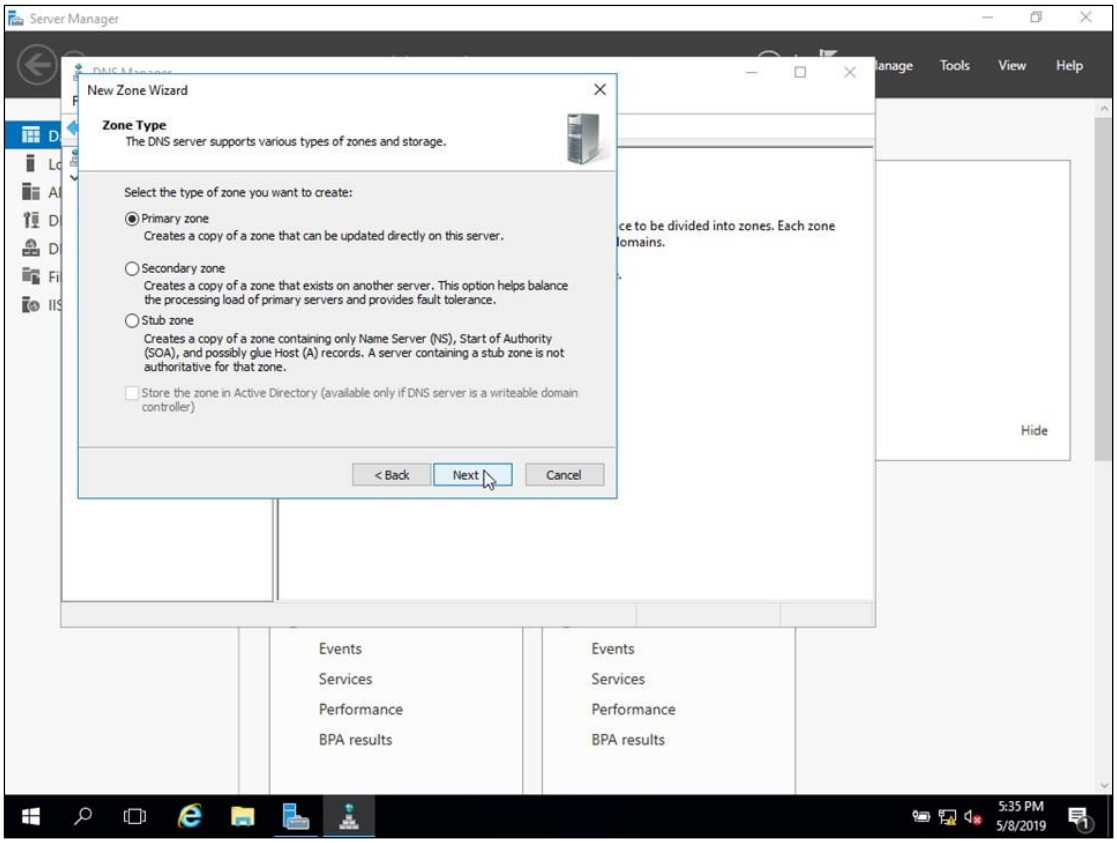

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Ser
IIS
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on ns1.
DHCP Server
Launch the DHCP post-install wizard
Complete DHCP configuration
DNS Server
Remote Server Administration Tools
Role Administration Tools
DHCP Server Tools
DNS Server Tools
Web Server (IIS)
Management Tools
IIS Management Console
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
5:17 PM
5/8/2019

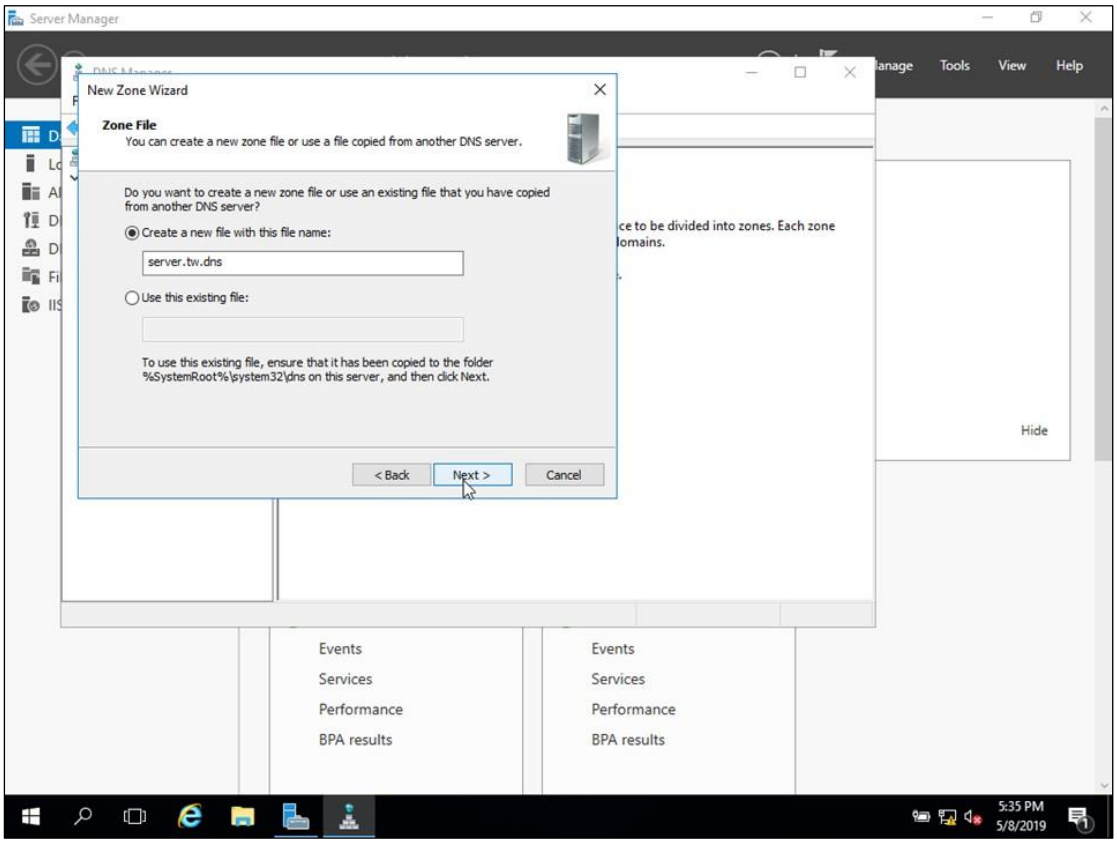

Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud ser
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
DHCP 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
5:28 PM
5/8/2019

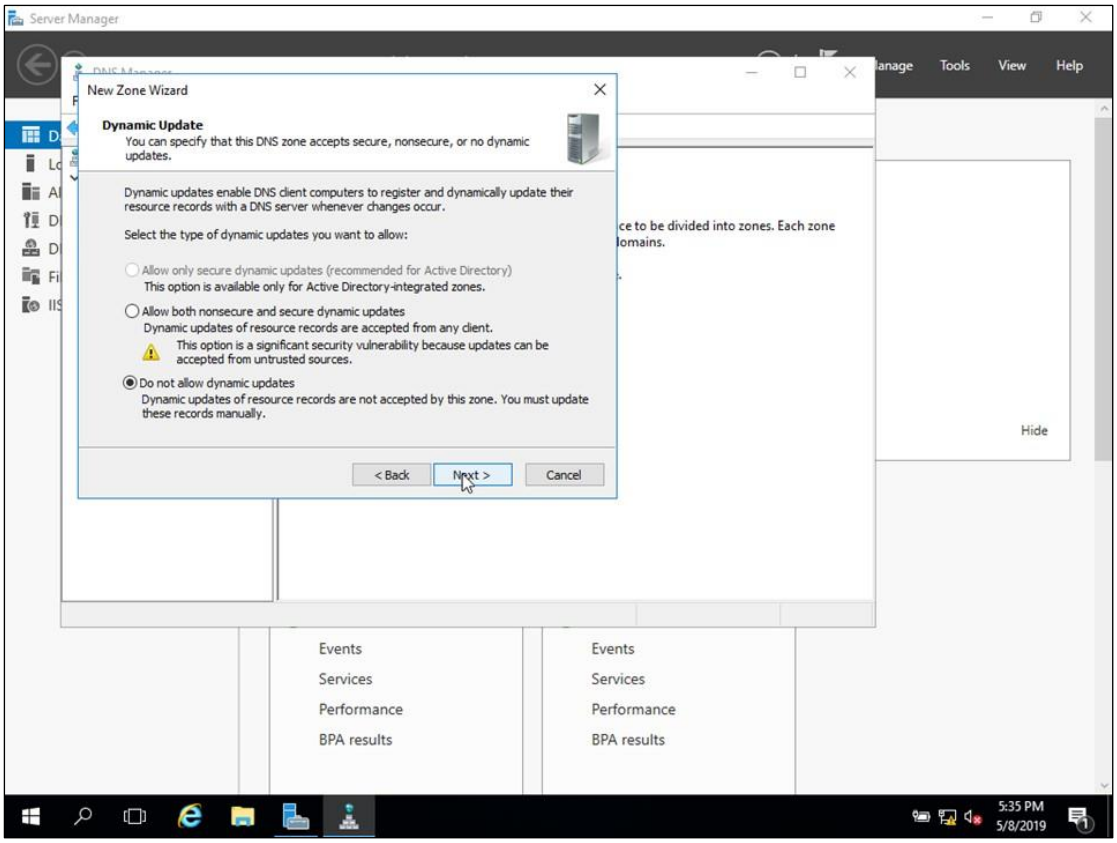

Server Manager
DNS Manager
File
Action
View
Help
DNS
NS1
Forward Lookup Zones
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
To add a new zone, on the Action menu, click New Zone.
Create a new zone.
Tools
View
Help
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:34 PM
5/8/2019

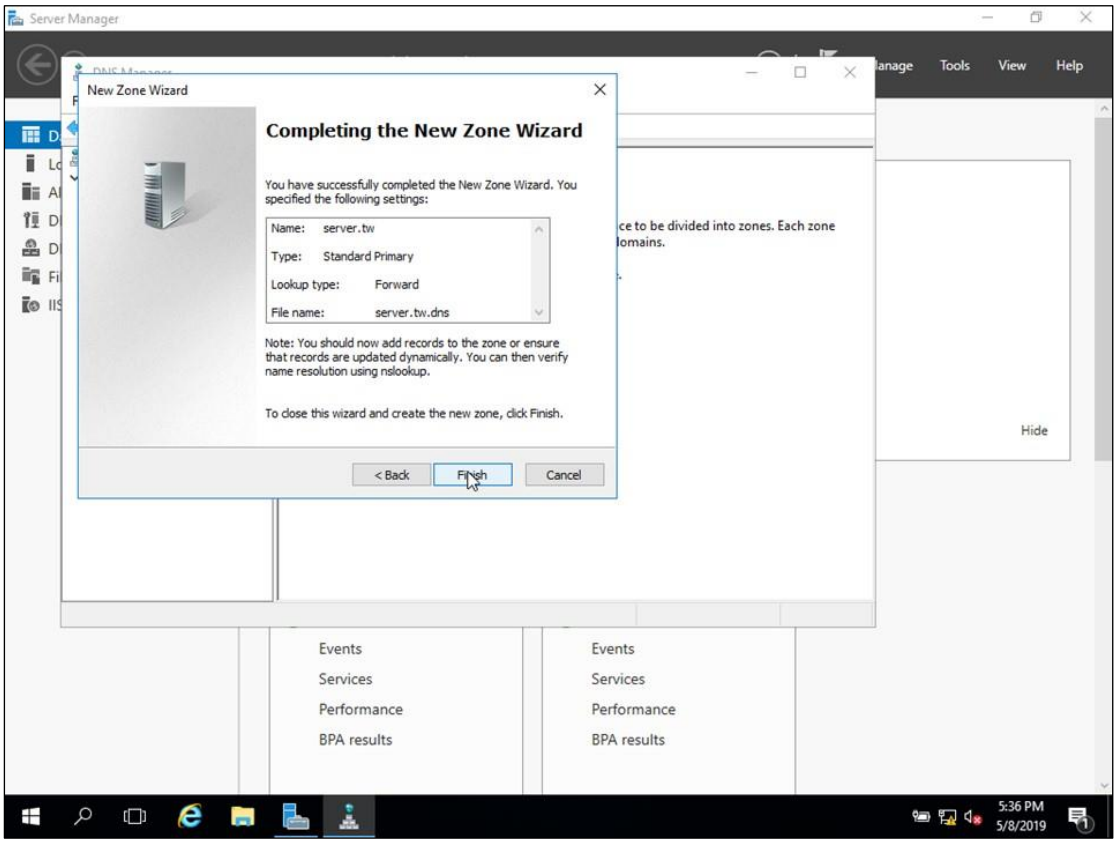

Server Manager
Tools
View
Help
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

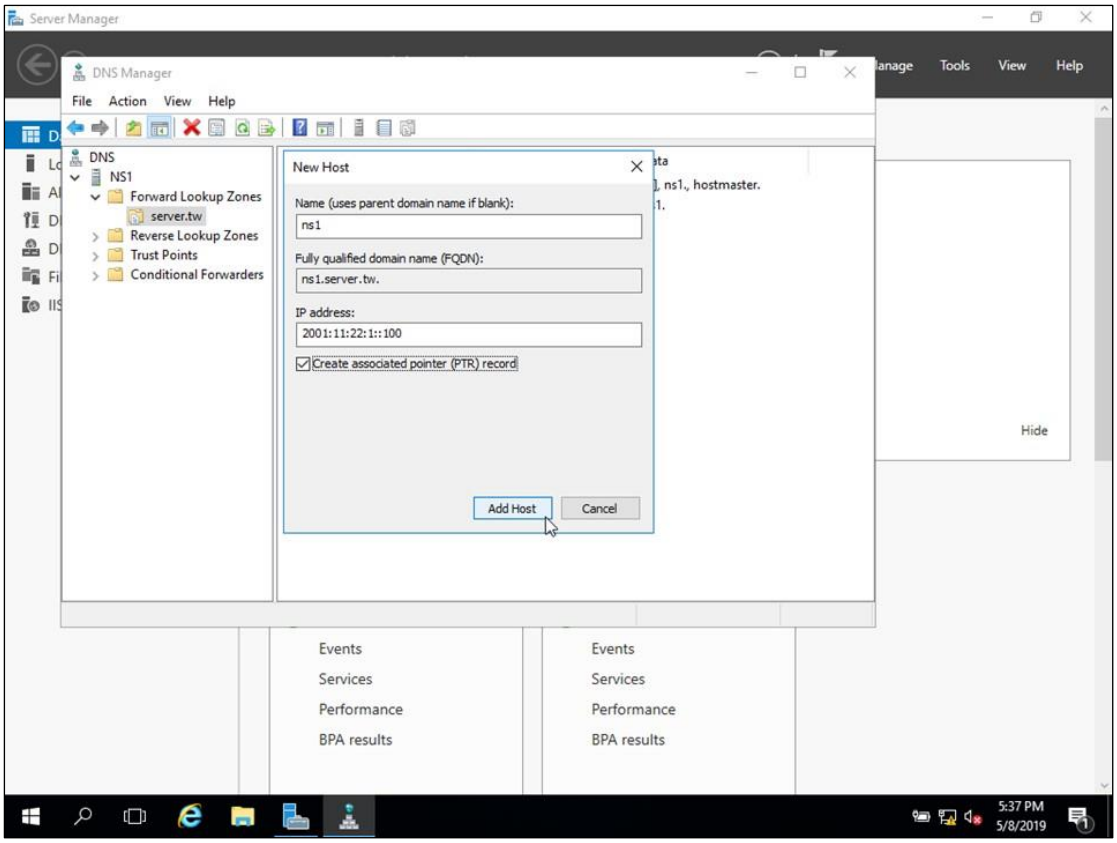

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

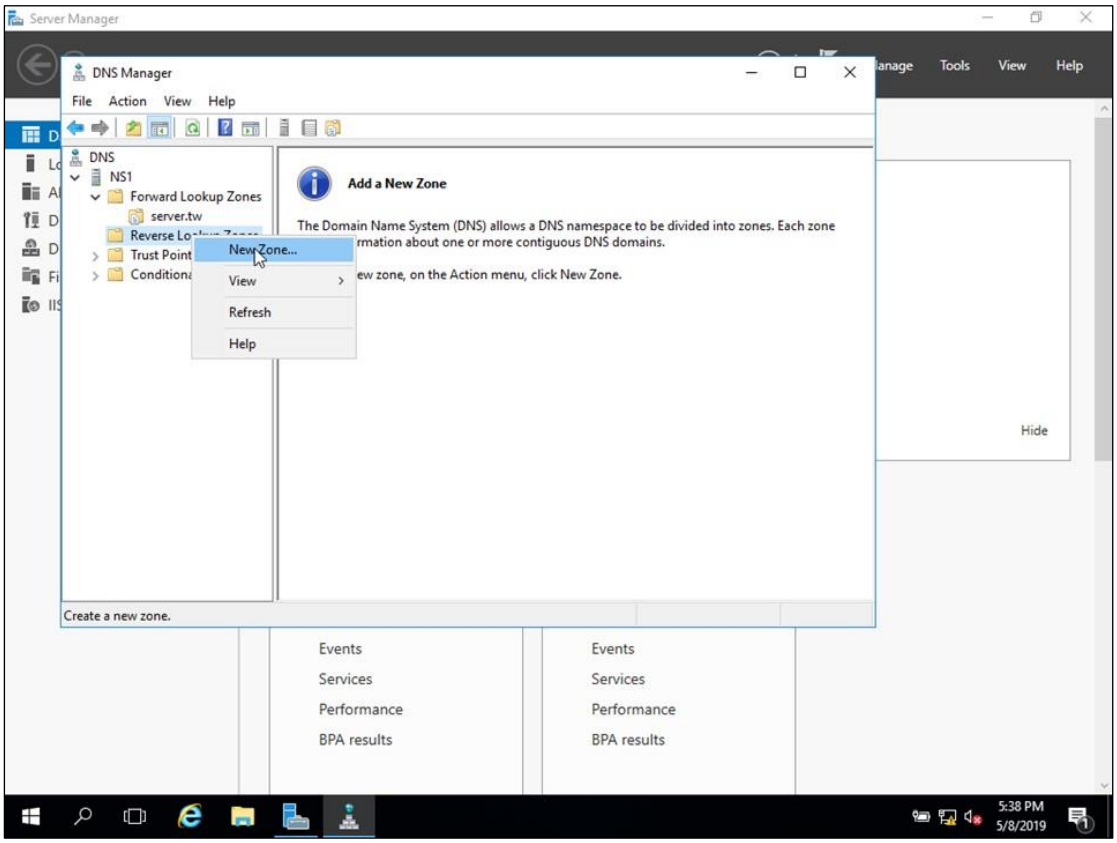

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

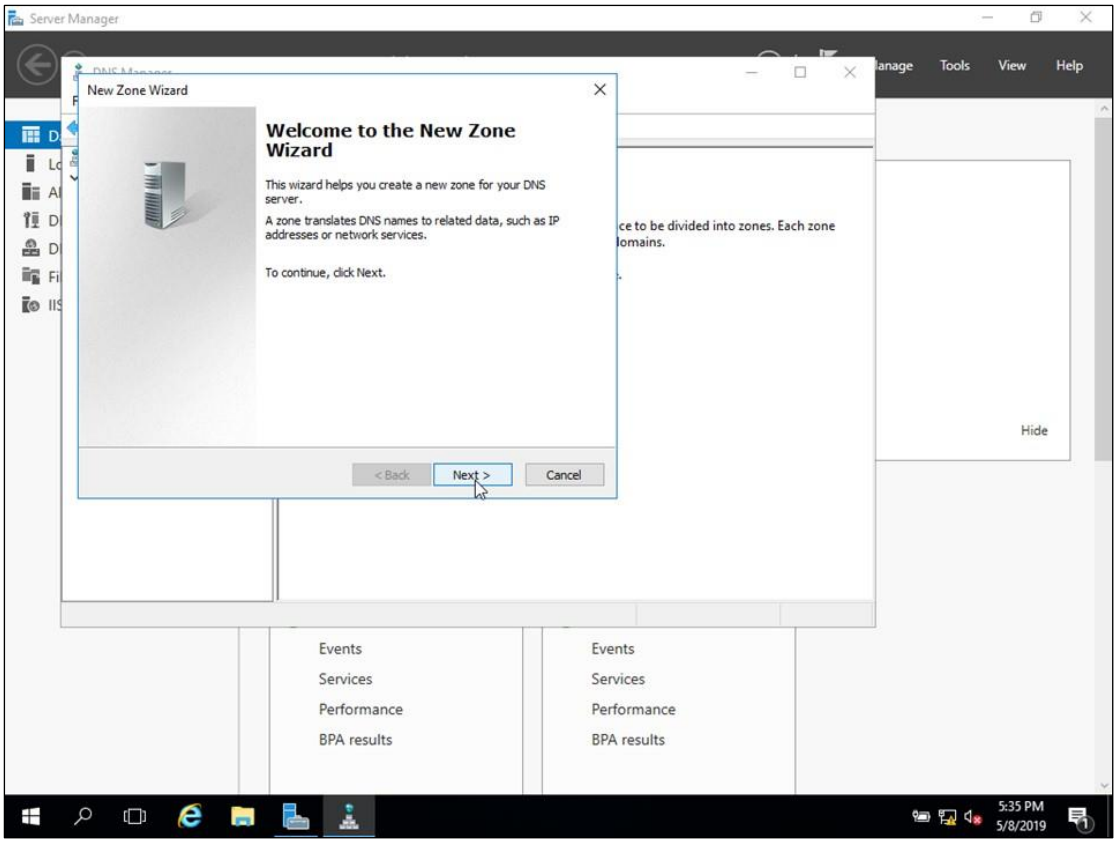

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
server.tw.dns
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

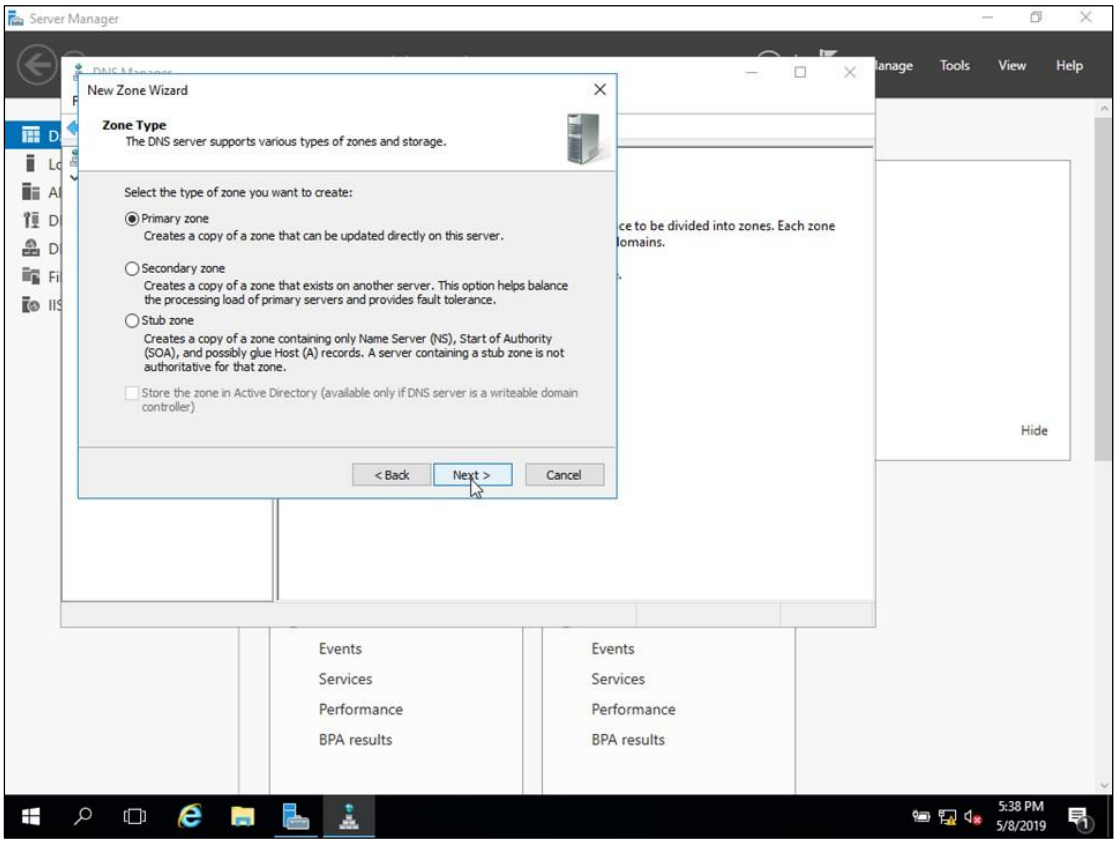

Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

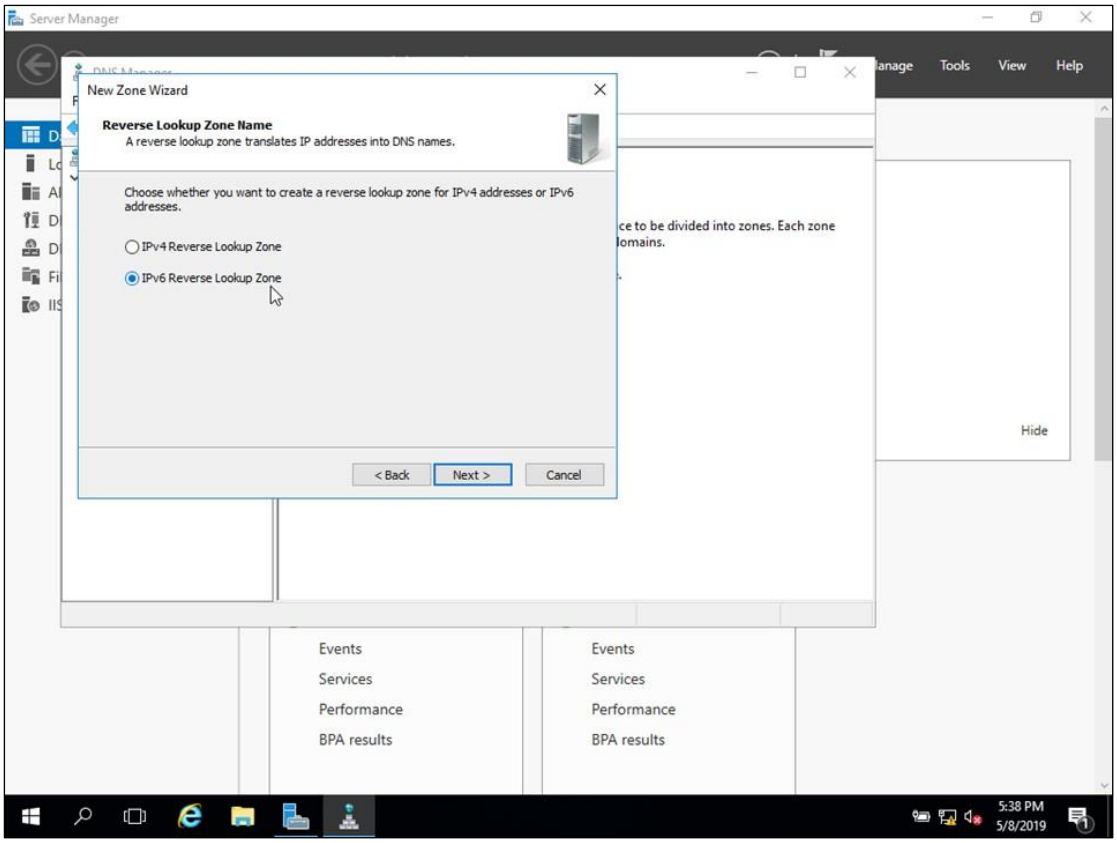

Server Manager
Tools
View
Help
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

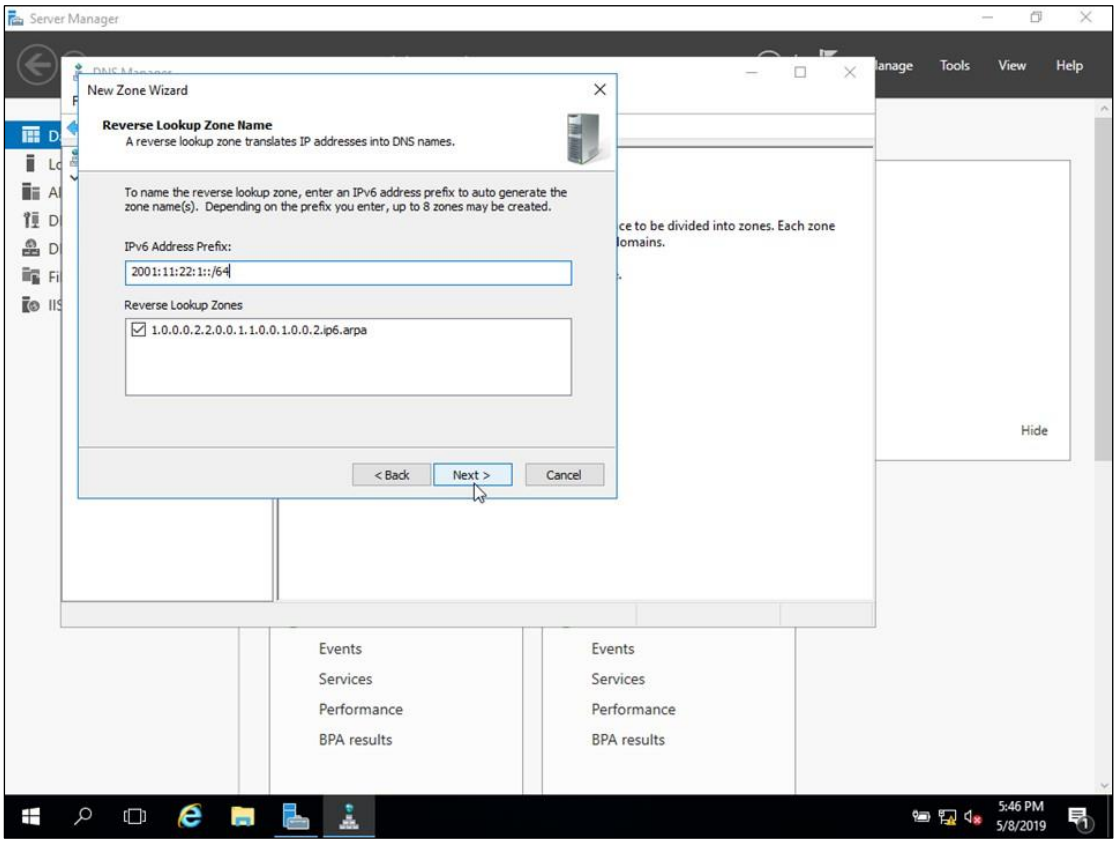

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
Trust Points
Conditional Forwarders
New Host
Name (uses parent domain name if blank):
ns1
Fully qualified domain name (FQDN):
ns1.server.tw.
IP address:
2001:11:22:1::100
Create associated pointer (PTR) record
Add Host
Cancel
Events
Services
Performance
BPA results
5:37 PM
5/8/2019

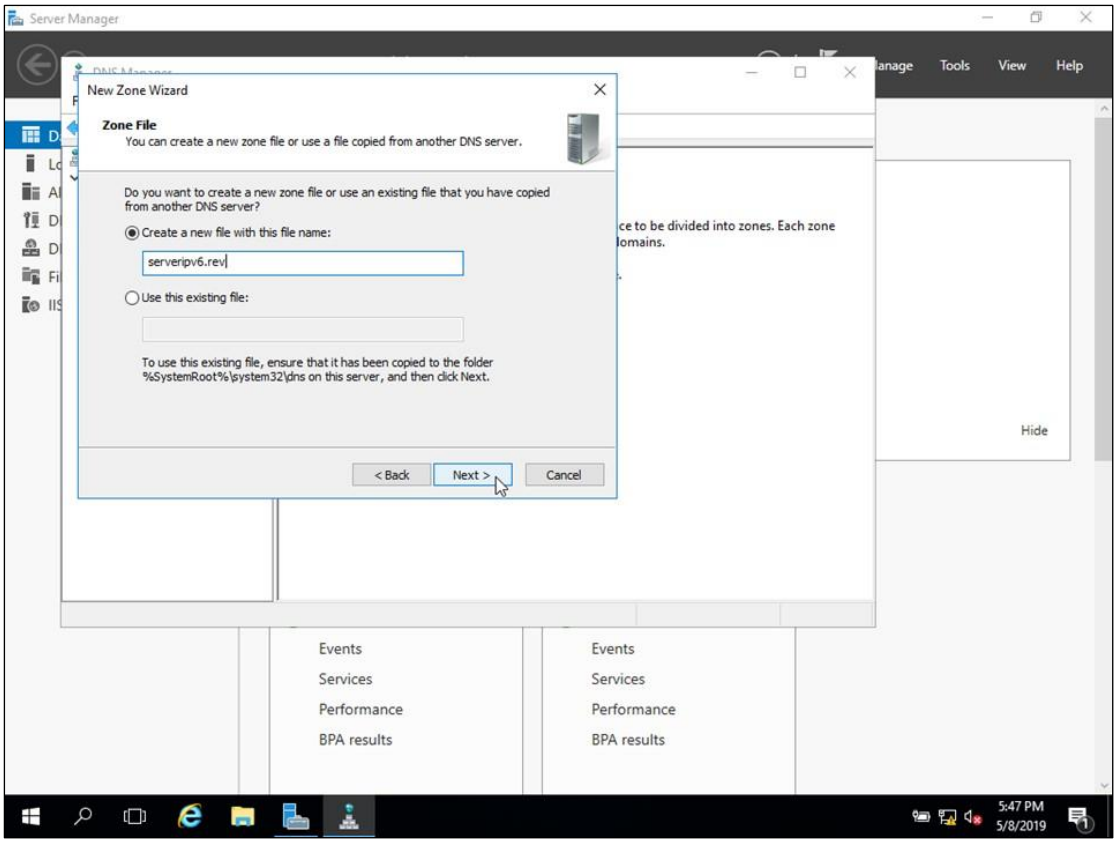

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone
Create a new zone.
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

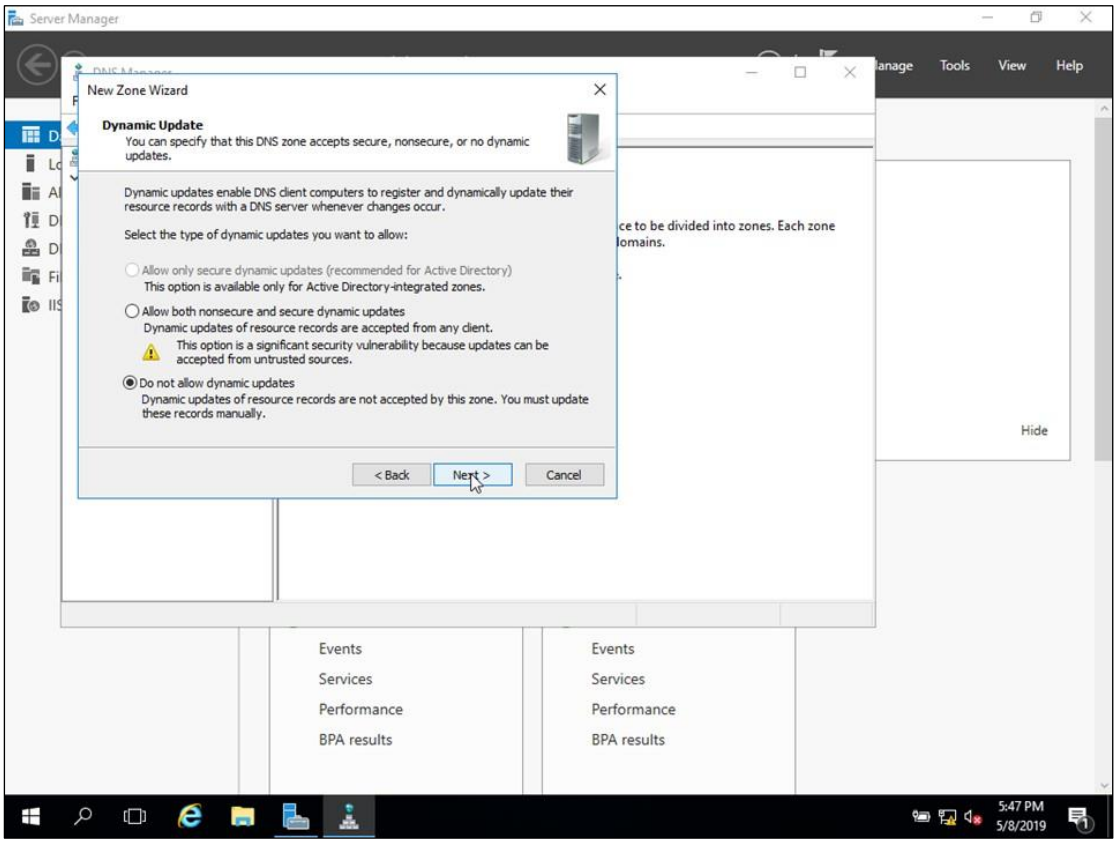

Server Manager
Tools
View
Help
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

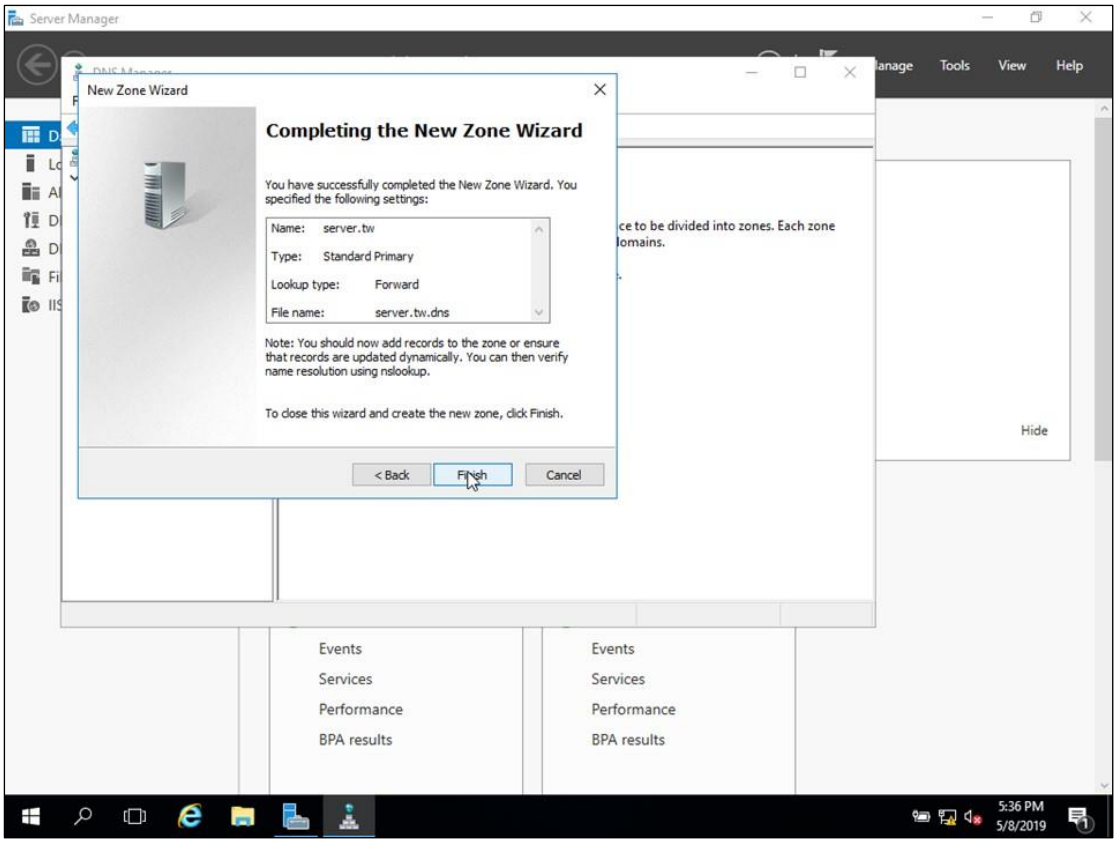

Server Manager
Tools
View
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

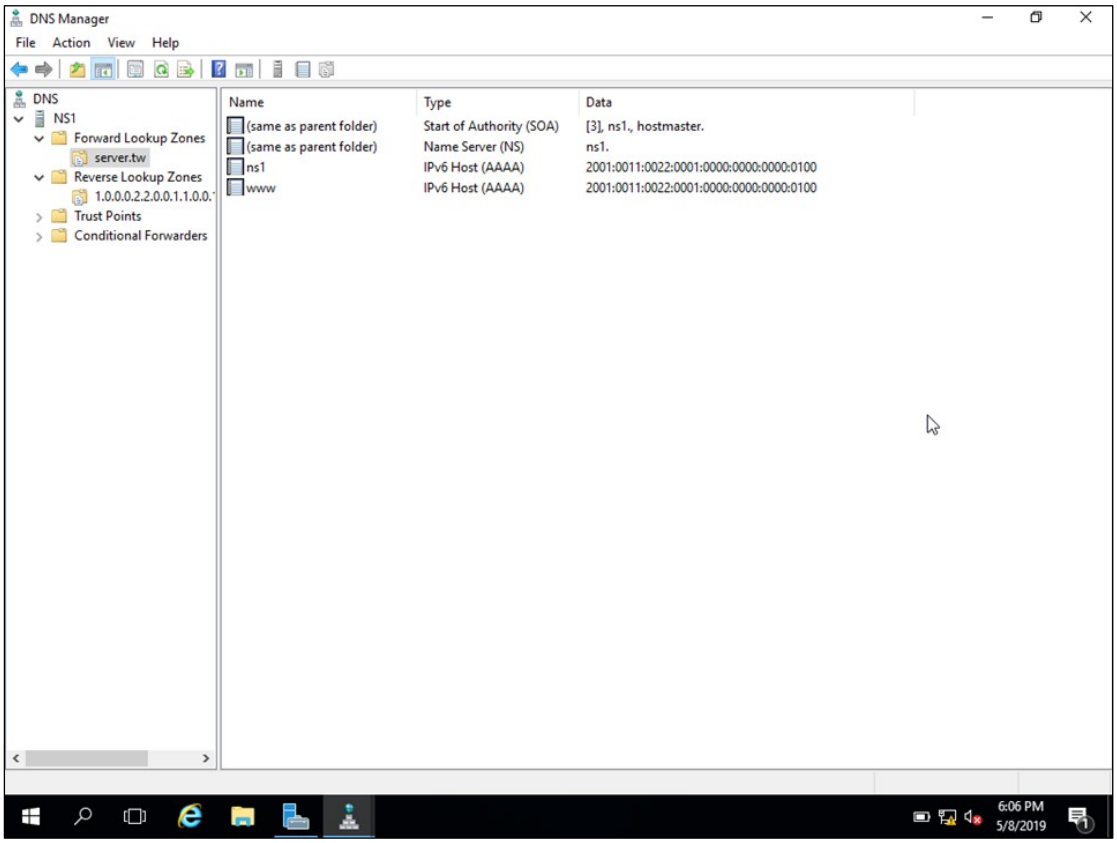

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.
IPv4 Reverse Lookup Zone
IPv6 Reverse Lookup Zone
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

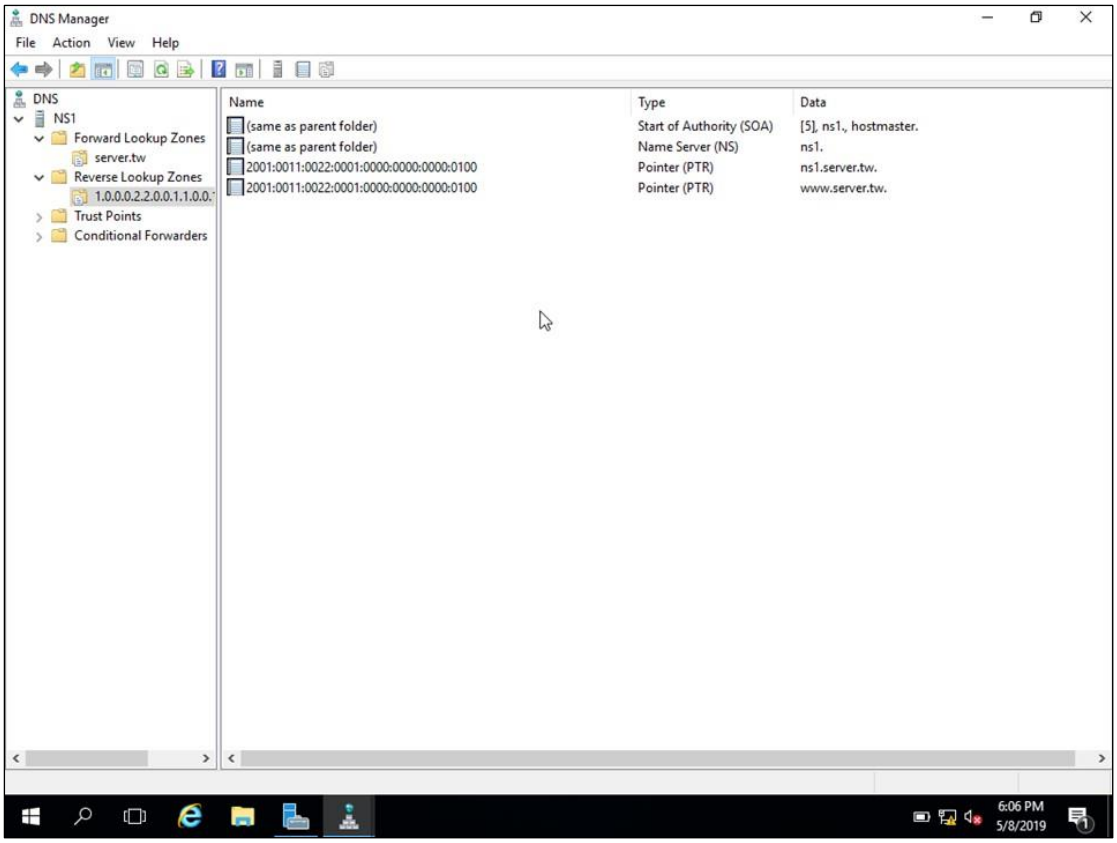

Server Manager
Tools
View
Help
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.
IPv6 Address Prefix:
2001:11:22:1::/64
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.1.0.0.2.ip6.arpa
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:46 PM
5/8/2019

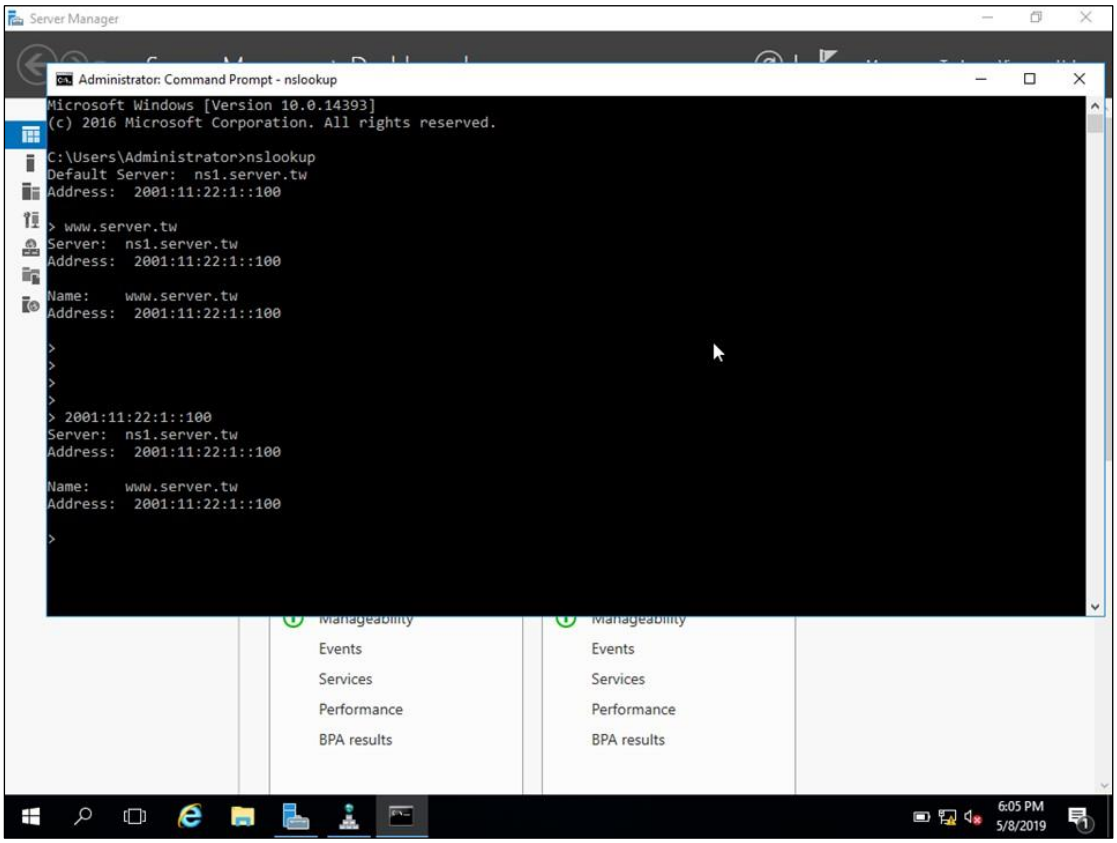

Server Manager
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
serveripv6.rev
Use this existing file:
To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:47 PM
5/8/2019


Server Manager
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:47 PM
5/8/2019


Server Manager
Tools
View
Help
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.
< Back
Finish
Cancel
Hide
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

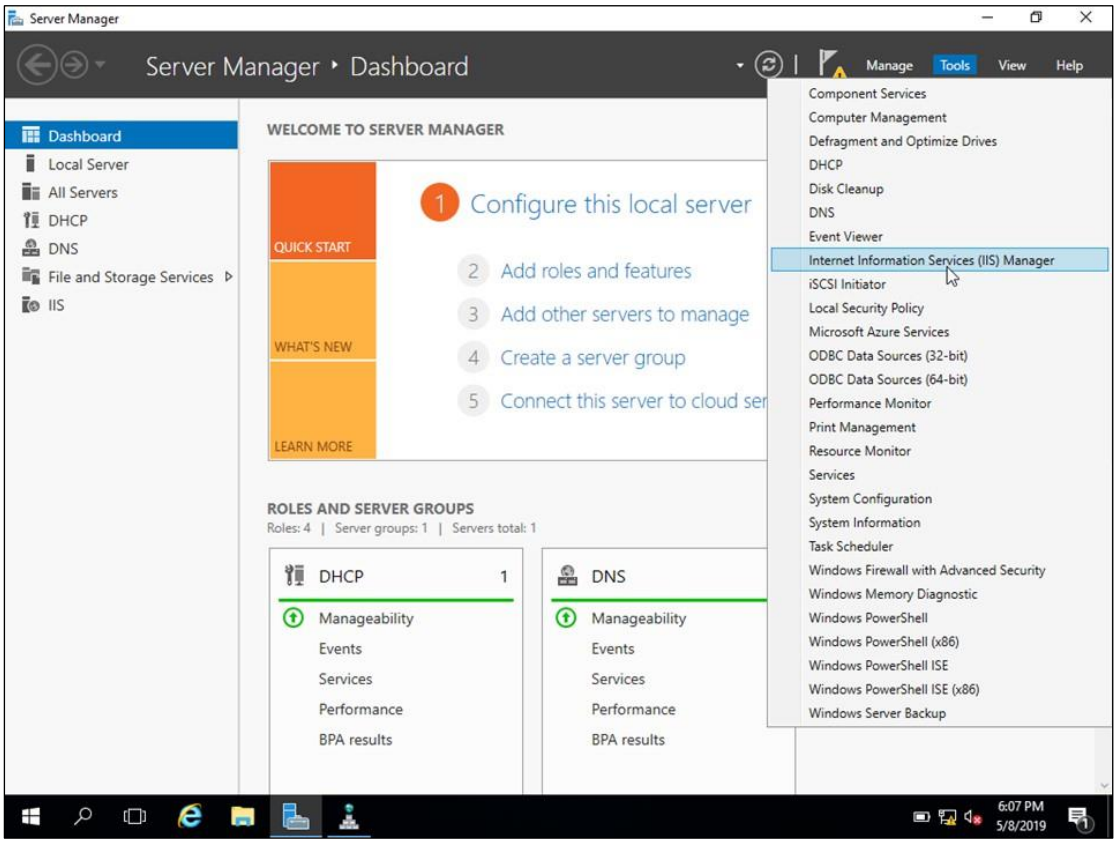

DNS Manager
File
Action
View
Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[3], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
ns1
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
www
IPv6 Host (AAAA)
2001:0011:0022:0001:0000:0000:0000:0100
6:06 PM
5/8/2019

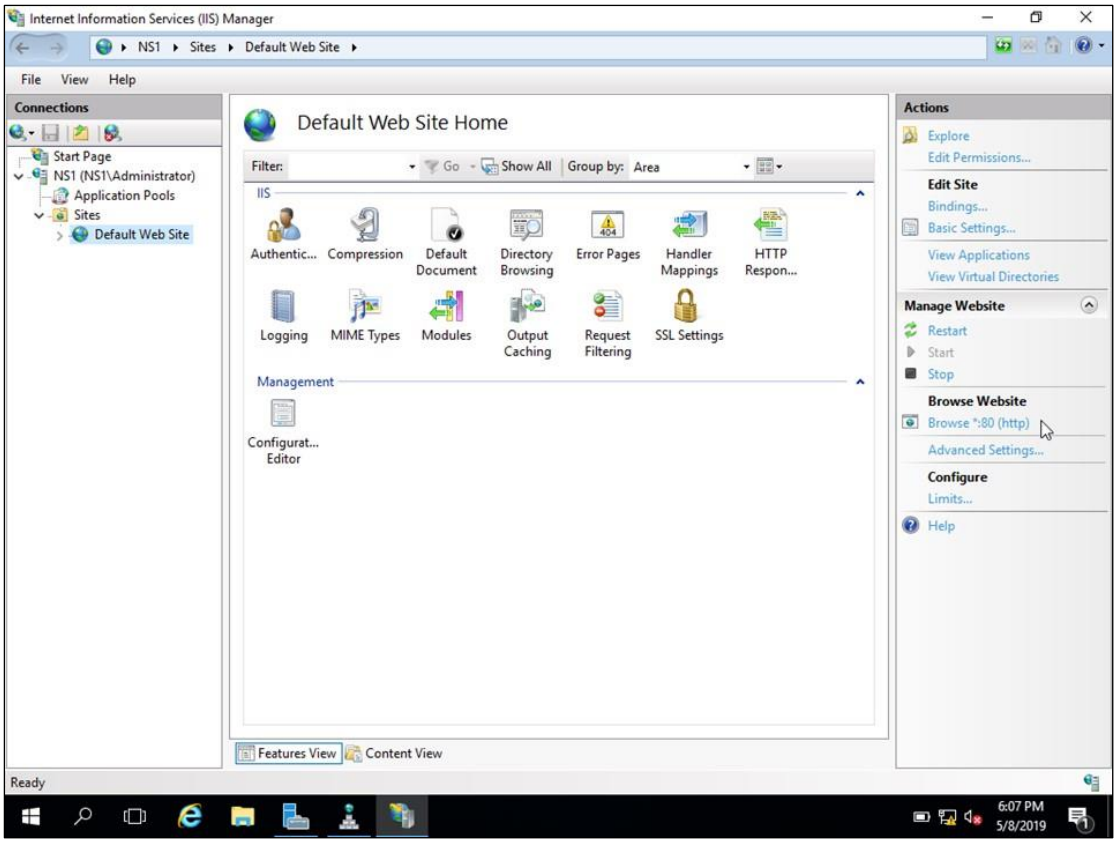

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[5], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
ns1.server.tw.
2001:0011:0022:0001:0000:0000:0000:0100
Pointer (PTR)
www.server.tw.
6:06 PM
5/8/2019

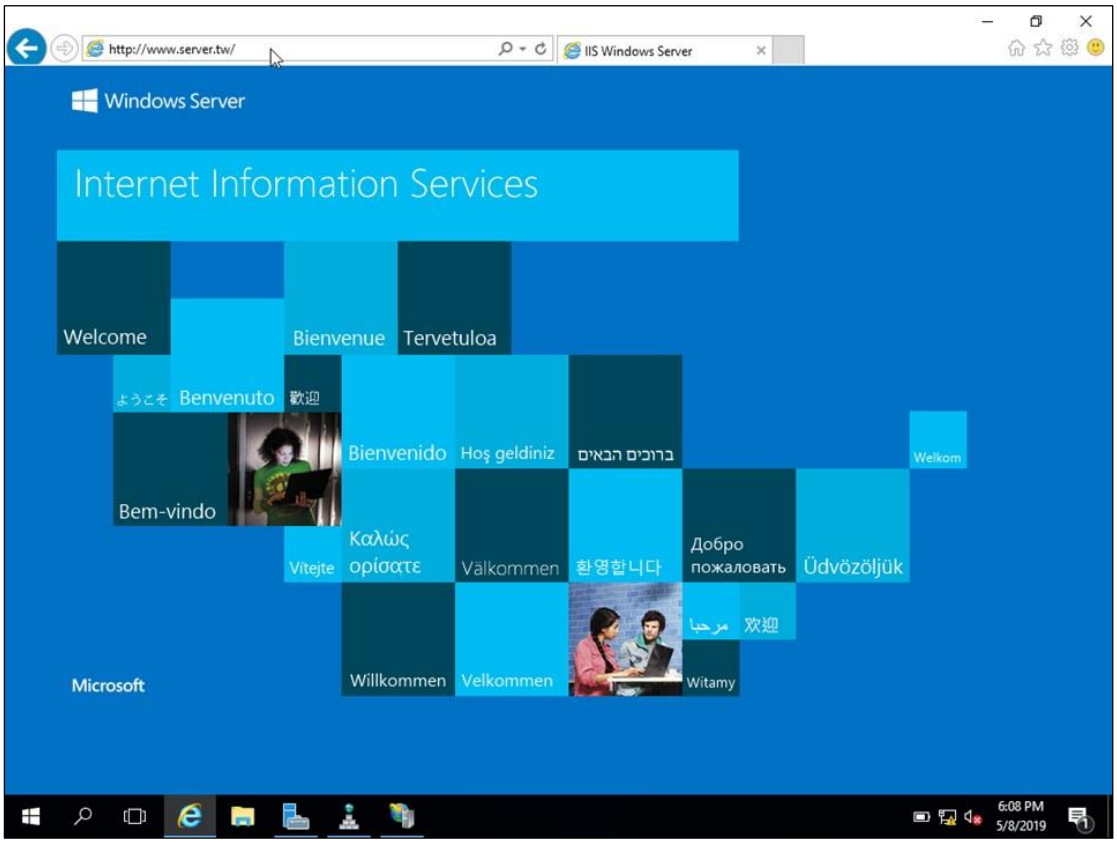

Server Manager
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: ns1.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
>
>
>
> 2001:11:22:1::100
Server: ns1.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
6:05 PM
5/8/2019

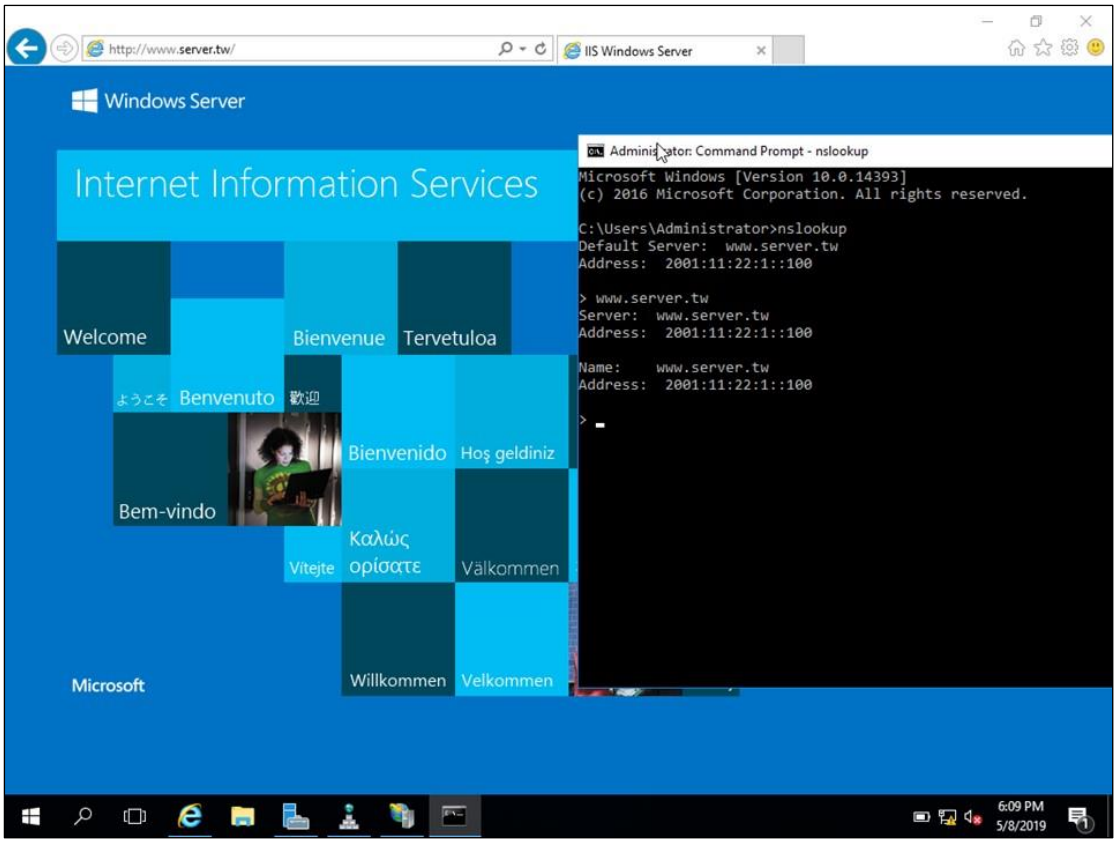
點進網域新視界！

IPv6建置示範
IIS 系統設定

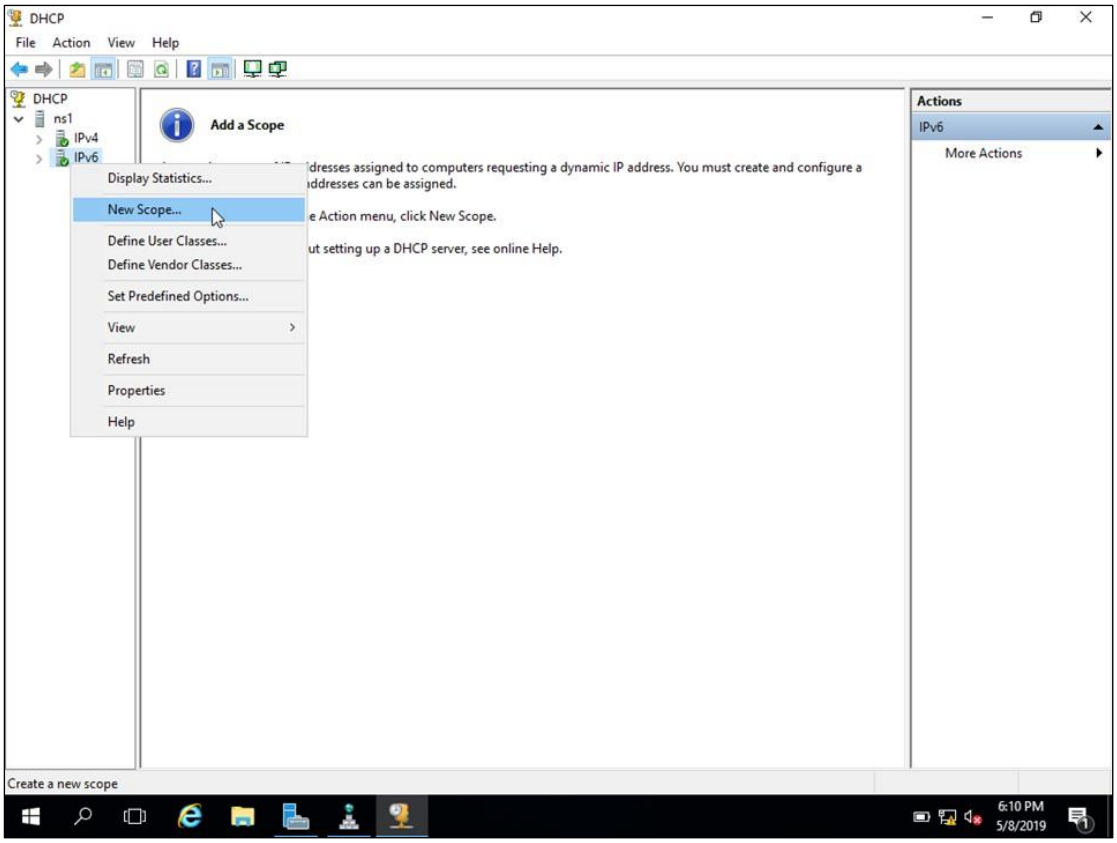


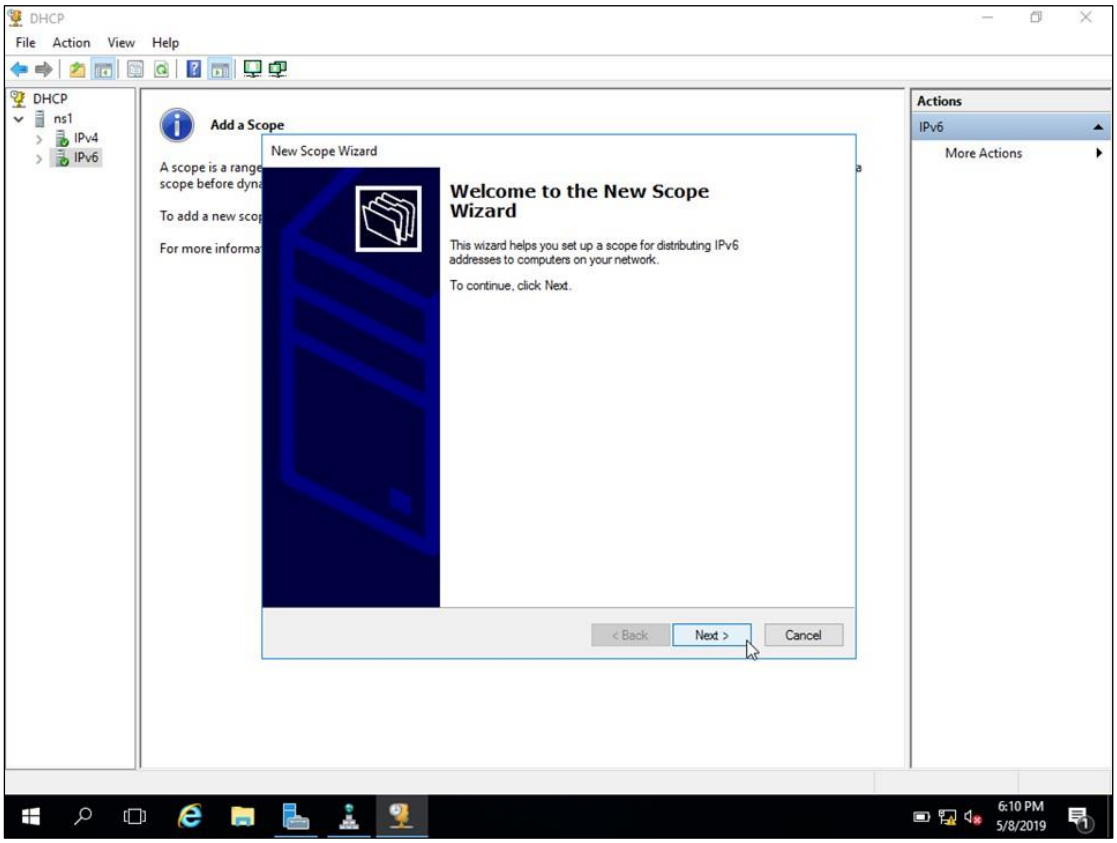

Internet Information Services (IIS) Manager
NS1 ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
NS1 (NS1\Administrator)
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
Help
Ready
6:07 PM
5/8/2019

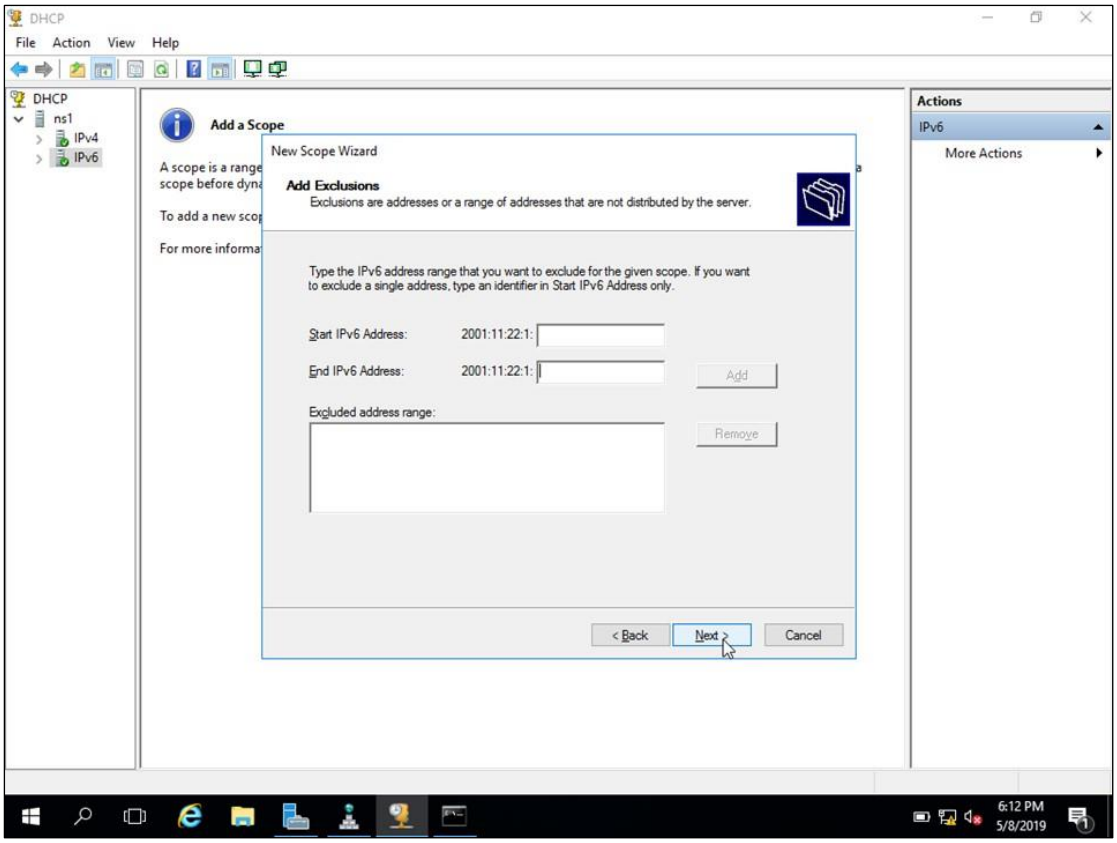

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft
6:08 PM
5/8/2019

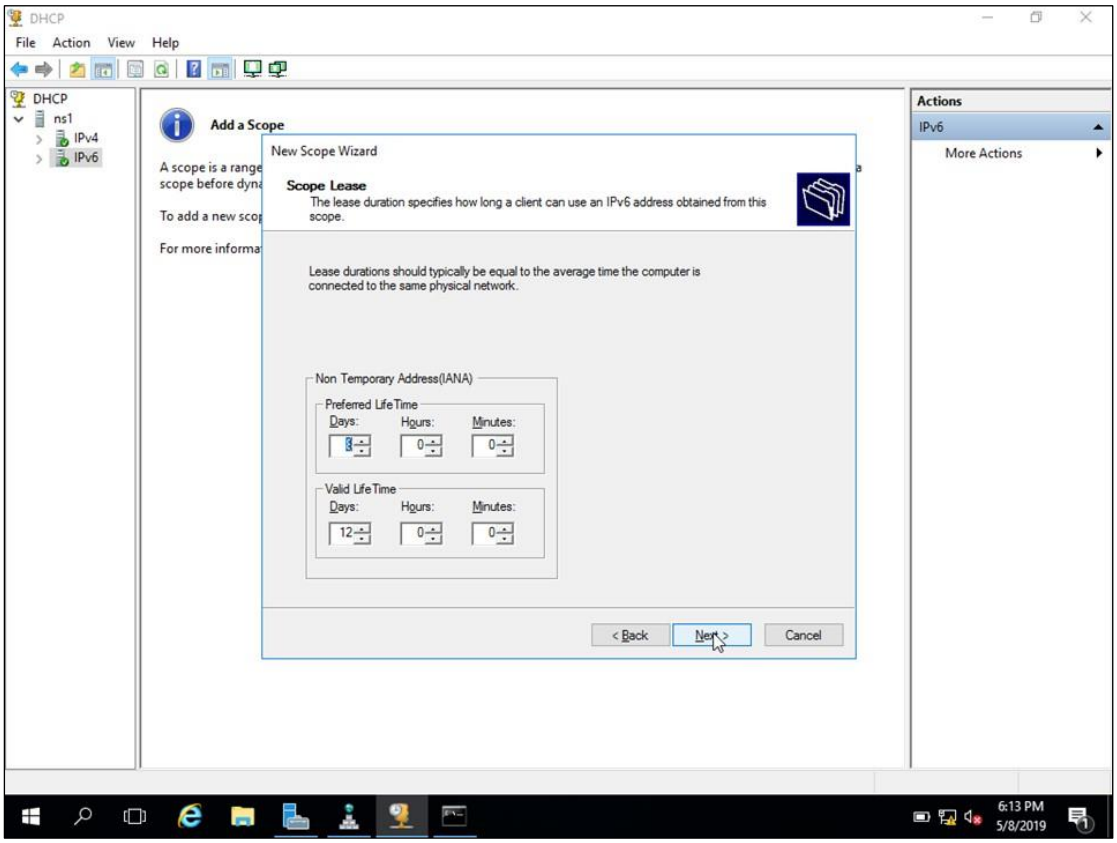

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
Willkommen
Velkommen
Microsoft
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: www.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: www.server.tw
Address: 2001:11:22:1::100
Name: www.server.tw
Address: 2001:11:22:1::100
>
6:09 PM
5/8/2019

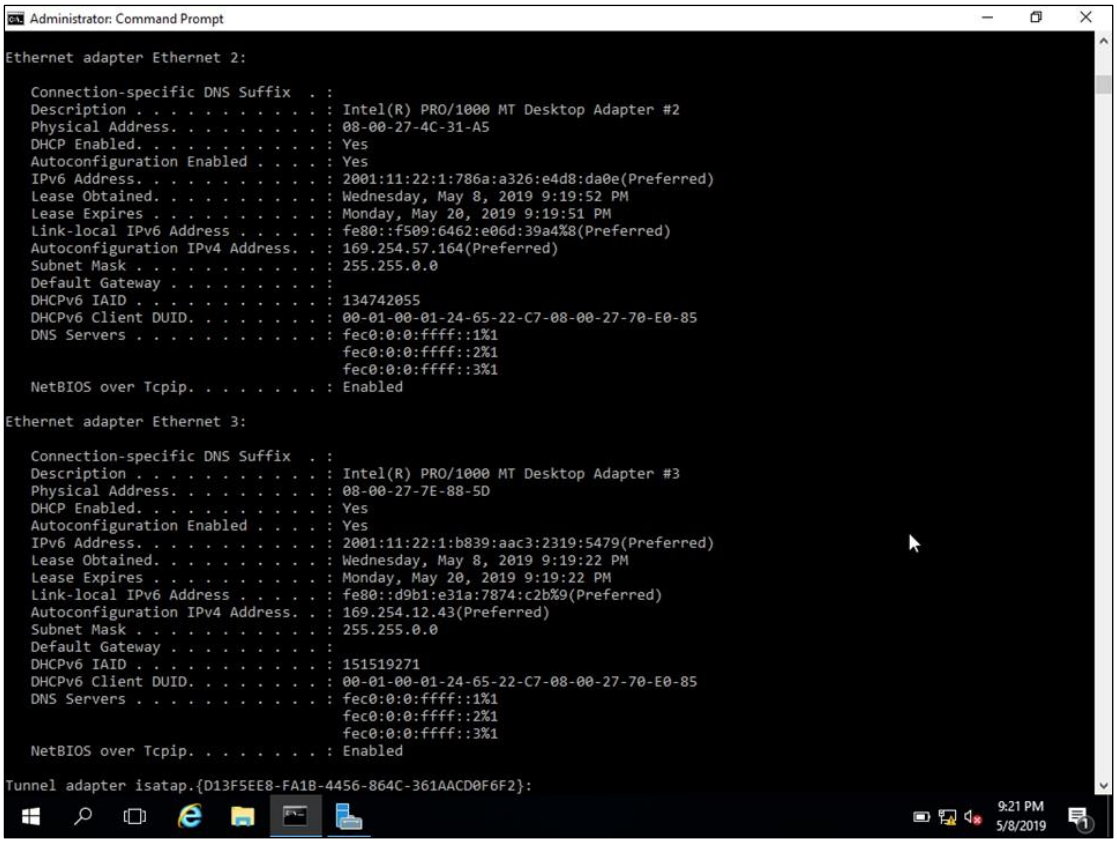

點進網域新視界！
IPv6建置示範
DHCP 系統設定


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
Display Statistics...
New Scope...
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
View
Refresh
Properties
Help
Actions
IPv6
More Actions
Create a new scope
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IPv6 addresses to computers on your network.
To continue, click Next.
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:10 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.
Type the IPv6 address range that you want to exclude for the given scope. If you want to exclude a single address, type an identifier in Start IPv6 Address only.
Start IPv6 Address: 2001:11:22:1:
End IPv6 Address: 2001:11:22:1:
Add
Excluded address range:
Remove
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:12 PM
5/8/2019


DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Scope Lease
The lease duration specifies how long a client can use an IPv6 address obtained from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network.
Non Temporary Address(IANA)
Preferred Life Time
Days: Hours: Minutes:
8 0 0
Valid Life Time
Days: Hours: Minutes:
12 0 0
< Back
Next >
Cancel
Actions
IPv6
More Actions
6:13 PM
5/8/2019


Administrator: Command Prompt
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Physical Address. . . . . : 08-00-27-4C-31-A5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:11:22:1:786a:a326:e4d8:da0e(Preferred)
Lease Obtained. . . . . : Wednesday, May 8, 2019 9:19:52 PM
Lease Expires . . . . . : Monday, May 20, 2019 9:19:51 PM
Link-local IPv6 Address . . . . . : fe80::f509:6462:e06d:39a4%8(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.57.164(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 134742055
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Ethernet 3:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #3
Physical Address. . . . . : 08-00-27-7E-88-5D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:11:22:1:b839:aac3:2319:5479(Preferred)
Lease Obtained. . . . . : Wednesday, May 8, 2019 9:19:22 PM
Lease Expires . . . . . : Monday, May 20, 2019 9:19:22 PM
Link-local IPv6 Address . . . . . : fe80::d9b1:e31a:7874:c2b%9(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.12.43(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 151519271
DHCPv6 Client DUID. . . . . : 00-01-00-01-24-65-22-C7-08-00-27-70-E0-85
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Tunnel adapter isatap.{D13F5EE8-FA1B-4456-864C-361AACD0F6F2}:
9:21 PM
5/8/2019


資料庫IPv6調整示範
點進網域新視界！

在設定MySQL過程中需要設定

--bind-address= [IP/Hostname]

[IP/Hostname] 可以是

IPv4 address

IPv6 address

Hostname

在 my.cnf 設定檔中的[mysqld] 底下

設定 bind-address = ::

只要設定 :: 就可以接收 IPv4 or IPv6 的連接

179

點進網域新視界！

作業系統與網站升級流程步驟和檢查項目清單

網路服務升級 IPv6 檢測作法說明

https://is.gd/UCmheO

IPv6 網際網路通訊協定 升級推動方案

網路服務升級 IPv6 檢測作法說明

網際網路通訊協定升級推動辦公室檢測 DNS、Web、Email、以及 FTP 等各項外部網路服務是否升級至 IPv6 的檢測作法說明如下：

一、檢測 DNS 服務是否升級至 IPv6

(1). 檢測方式說明：

DNS 服務升級 IPv6 之檢測為透過純 IPv6 連線逐層檢查，從最上層的 root DNS 檢測起，再檢測 .tw DNS 以及 .com.tw/.gov.tw/.org.tw DNS 等，再到貴機關的 DNS 主機，一層一層的檢查，

a.檢測各層的 DNS 主機是否有支援 IPv6；

b.檢測各層的 Domain name 是否有設 AAAA 紀錄。

(2). 檢測作法：

逐層檢測時，若有發生檢測不通過的情形，可以在 Linux 環境下用下列 dig 指令的方式了解哪個部份有問題，指令如下：

dig -6 [填入欲檢查的 DNS] AAAA +trace

(例如：dig -6 www.gsnv6.tw AAAA +trace)

(3). 常見問題

181

線上檢測服務升級

IPv6 網際網路通訊協定 升級推動方案

https://www.gsnv6.tw/inventory/checkservicepub.cgi

線上檢測服務升級IPv6

檢測程式作法說明

若是檢測一般Web網站，前面請加 http:// ，例如 http://www.twnic.net.tw
若是檢測 https 網站，前面請加 https:// ，例如 https://www.gsnv6.tw
若是檢測 Email, DNS, FTP，請直接輸入主機名稱(domain name)，例如 dns2.twnic.net.tw
本網站 www.gsnv6.tw 的IPv6位址為：2001:c50:ffff:1::9016

系統分類	服務系統URL(例如：www.gsnv6.tw，請留意上面之說明文字)
Web ▼	

送出檢測

182

點進網域新視界！

IPv4/IPv6雙軌環境下資訊安全規劃概述

ICP IPv4/IPv6升級及網路安全防護差異

- IPv4以ARP表格尋找要傳遞的IP位址，IPv6則以ICMPv6將通訊資訊包在封包內
- IPv4對於Domain的定義放在A record內，IPv6則以AAAA record對應
- IPv4使用DHCP動態配置IP，IPv6 則以DHCPv6達成相同功能
- MTU(最大傳輸單位)在IPv4是576個位元組，IPv6則是1280個位元組

- IPv6 Ready Logo是由國際IPv6論壇組成的標章委員會設計及制定的規範
- IPv6 Ready Logo認證分成Phase-1 Logo、Phase-2 Logo及功能性Logo
- Phase-1 Logo 表明設備包括強制性的核心機制基本上能夠與其他設備進行通訊
- Phase-2 Logo表明設備全部符合IPv6基本協議相關RFC
- 擴展功能性Logo有包括DHCPv6、IPSEC、SIP Logo等

- 新創公司建議使用Amazon的AWS及Google的Google Cloud Platform及Microsoft的Azure等的大型且完備的雲端主機
- 或者使用Linode、Digital Ocean等雲端主機
- 若使用台灣的雲端主機，須先詢問是否有支援IPv6，有些台灣雲端業者不支援

- 網站伺服器建議使用Apache、Nginx或IIS，因為普及率高，支援IPv6
- 如果考慮多平台支援，以Apache跟Nginx為優先考量

- 防火牆分硬體防火牆跟軟體防火牆，考慮到效能，採購建議以硬體防火牆優先。
- IPv4跟IPv6對不同網路攻擊的風險不同，建議導入IPv6之後，以IPv6的安全策略為版本，規劃一個IPv6的風險評估表。

- 針對IPv6的網路設備的採購，建議購買有IPv6 Ready Logo的設備。
- 雲端主機如Amazon AWS、Google Cloud Platform及Microsoft Azure都有提供完整的服務，且支援IPv6，適合新創公司使用。
- 網站伺服器依據公司未來發展需求而定，不論是使用Apache、Nginx或者Microsoft IIS，都可以支援IPv6 。
- 網站作業系統不論是使用Unix based如CentOS、Ubuntu或者Microsoft Windows，目前都已經有支援IPv6 。
- 硬體防火牆在市場上大品牌眾多，如果是使用於機房，建議優先考慮使用硬體式防火牆 。

- ICP安全策略的制定從內部到外部，建議可以先參考現有IPv4的安全策略，並製作IPv6的安全管理規範，之後再針對差異部分，進行修正。

ICP IPv4/IPv6升級雙雙協定網路安全防護檢查項目清單

- 機房設備盡量挑選具有IPv6 Ready Logo的設備或者使用已經完整實現IPv6的雲端主機服務商(例如Amazon AWS、Google Cloud Platform、Microsoft Azure)。
- 路由器須開啟IPv6。
- 防火牆須設定IPv6過濾規則(防火牆分為硬體防火牆跟軟體防火牆)。
- 網站伺服器(包括Apache、Nginx及Microsoft IIS等)須開啟IPv6 listening並設定好安全規則。
- 作業系統也須開啟IPv6設定。

- 需要設定DNS使得IPv6訪客可以透過IPv6位址查到該domain name對應的IPv6位址並進行連線。
- 須設定MX records確保Email的收送可以正常運作。
- 如果網站程式碼是 CMS，則須檢查程式碼內是否有針對IPv4進行特別的設定。

- 應利用公司現有的安全漏洞掃描工具對修改的網站進行安全漏洞掃描，確保無安全問題。
- 利用壓力測試工具，對修改後的網站近行壓力測試，確保在同時支援IPv4跟IPv6的情況下，網站可以運作正常。
- 確定現在使用的安全漏洞/程式碼掃描工具都支援IPv6。

- 對於所有進出的IPv6封包都需要進行過濾。
- 針對ICMPv6封包進行過濾，可慮哪些可以放行，哪些需要阻擋，可以參考RFC4890。
- IPv6 extension header要進行過濾，並只能開放有需要的。
- 盡量維持IPv4跟IPv6規則的同步。

- 要求你的合作廠商一起升級IPv6。
- 從外部測試網站，利用一些IPv6 驗證網站或者申請一個外部的主機，進行外部測試。
- DNS記得要設定IPv6的AAAA record 。
- 連帶的服務也記得一併升級IPv6。

- 要求你的合作廠商一起升級IPv6。
- 從外部測試網站，利用一些IPv6 驗證網站或者申請一個外部的主機，進行外部測試。
- DNS記得要設定IPv6的AAAA record 。
- 連帶的服務也記得一併升級IPv6。

- Apache的設定檔為 httpd.conf
- Listen 80
- Listen 443
- Listen [::]:80
- Listen [::]:443
-
- <VirtualHost *:80 [::]:80>
- ...
- </VirtualHost>

- <VirtualHost [2607:f:1:11::4]>
- </VirtualHost>

- nginx設定檔為 nginx.conf
- 如果是443 SSL要啟用 ipv6
- server {
- listen 80 default_server;
- listen [::]:80;
- listen 443 ssl http2;
- listen [::]:443 ssl http2;
- }

- 新版的作業系統Kernel都有支援IPv6，但有些預設關閉、有些預設開啟。
- 作業系統許多都會內建防火牆機制，防火牆也需要一併將IPv6 的規則設定後啟用，以免造成IPv6封包可以讓網卡接送跟傳送 ，但是在軟體防火牆那一層卻被過濾掉，造成無法連線。

- 範例：僅允許特定IPv6 位址可以連線
- ip6tables -I INPUT -p tcp -m tcp --dport <port> -s 2b00:x:x:x::/64 -j ACCEPT

- 範例：禁止特定IPv6 位址不能連線
- ip6tables -I INPUT -p tcp -m tcp --dport <port> -s 2b00:x:x:x::/64 -j DROP

常見網路安全管理機制簡介

- 封包過濾防火牆
- NetFlow 流量監測
- DPI 資安防禦設備

201

,

(一) 防火牆

防火牆以提供網路封包篩選過濾為主要功能，其做法是依據預設好的規 則，對流入或流出的 IP 封包是否放行進行管制，以決定是否允許或阻止網路連線存取的行為。

202

(一) 防火牆

封包過濾通常只檢查封包的表頭(Header)，不會檢查資料段的內容，可以 檢查的項目包括來源 IP 位址、目的 IP 位址、協定種類(TCP、UDP 等)、 TCP 或 UDP 的來源埠、TCP 或 UDP 的目的埠、以及 ICMP 的訊息代碼等。

203

(一) 防火牆

封包過濾型防火牆建置簡單、價格便宜、效率佳，但不易定義出有效又能 長期使用的規則，也無法進行應用層協定的防護。

目前相當熱門的次世代防火牆

Layer 7 Applications Firewall

204

(二) NetFlow 流量監測

Netflow (Network Flow)是一套網路流量監測方式

一個 Flow 代表一個來源 IP 位址和目的 IP 位址之間傳輸的單向流量

且所有封包具有相同傳輸層的來源及目的端口號

205

,

(二) NetFlow 流量監測

Netflow 以網路介面為單位呈現分析的結果

包含各服務流量的資訊、各 IP 位址的流量資訊，甚至各種傳輸協議之流量高低排序...等等

並可以列出疑似受病毒感染或被植入惡意程式的電腦所使用的 IP 列表

206

(二) NetFlow 流量監測

網管人員可以透過Netflow 快速有效的掌握所管轄網路的狀態，包含效能、壅塞程度等資訊。

第一可從網路層的角度分析，例如有些攻擊行為可能針對某個特 定埠進行攻擊，或是出現不合理的 IP 位址。

第二則是從傳輸層角度分析，例如透過Netflow 資料揭連線(Session)數目最多的主機，或者不正常的封 包控制旗標(TCP Flag)。

207

,

(三) DPI 資安防禦系統

DPI 為深層封包檢測的簡稱

其做法為經由接收路由器介面端口複製的鏡像(Port Mirror)封包

經由封包的內容的特徵比對

進行第三層到第七層的資安風險分析

208

(三) DPI 資安防禦系統

DPI 資安防禦系統可以判斷封包所屬的服務類型例如是否屬於 YouTube 等常見的服務流量

也可以偵測出典型的殭屍病毒，例如網路聊天感染(Internet Relay Chat Bot, IRC Bot)等安全相關的病毒程式，並可以將相關資訊儲存於資料庫中，再藉由網頁介面呈現統計資料

209

,

(三) DPI 資安防禦系統

許多具有安全疑慮的封包特徵值並無法從表頭欄位進行判別，DPI 系統則可以深入觀察封包內容，並檢驗出可疑封包及流量。

對於難以掌握的殭屍網路，都必須藉由 DPI 系統才比較容易檢驗出可疑的感染封包。

210

(三) DPI 資安防禦系統

但由於深度封包檢測需要較複雜的比對和檢測，若以通透模式 (Transparent Mode) 接在既有網路骨幹時，若流量超過設備的負荷，可能會導致進出口壅塞，甚至有可能出現封包遺失 (Packet Loss) 的狀況。

故大多數 DPI 設備都是採取旁聽模式 (Sniffer Mode) 去監測鏡像 (Mirror) 的流量。

211

,

雙協定網路安全管理機制差異性

以下整理比較 IPv4/IPv6 雙協定網路可能面臨的安全性議題

- IPv4 網路常見攻擊行為
- IPv6 網路在安全機制的強化

212

IPv4 網路常見攻擊行為

IPv4 的設計主要考慮點對點傳輸模型，在網路安全的考量較少，因此導致 幾種下列常見的攻擊行為：

- 服務阻斷式攻擊(Denial of Service Attack, DoS)：此種攻擊為對服務提供者進行大量非法要求，使得目標系統未處理這些非法要求而癱瘓正常服務提供
- 惡意程式散播(Malicious code distribution)：病毒或蠕蟲會藉由 IPv4 小位址空間裝載惡意程式散播危及主機甚至遠端系統的安全性

213

,

- 分片攻擊(Fragmentation Attacks)：利用作業系統需大量重組 IPv4 封包 的特性，傳送不完全且不連續的片段封包導致主機當機
- 埠口掃描攻擊(Port Scanning)：利用端口掃描技術找出潛在的漏洞，由於 IPv4 的位址空間很小，整個 ClassC 網路僅需四分鐘就可全部掃描
- ARP 欺騙及 ICMP 重導攻擊(ARP poisoning and ICMP redirect)：偽造的 ARP 回應通知網域中主機不正確的對應資訊可能導致封包傳送錯誤

214

IPv6 網路在安全機制的強化

大部分 IPv4 常見的攻擊已可藉由成熟的防禦機制過濾出可疑封包，或是經由一些網路技術而避免。

IPv6 則從網路的設計上，提供比 IPv4 更完整的網路安全機制，說明如下：

215

,

IPv6 網路在安全機制的強化

- 預設啟動 IP 安全性協定(Internet Protocol Security, IPSec)：雖然 IPv4 也支援 IPsec，但為選擇性使用，而在 IPv6 由 RFC4301 指定所有網路節點都必須使用 IPsec 。
- IPsec包含Authentication Header(AH) 和 Encapsulating Security Payload (ESP)，以及 Internet Key Exchange (IKE) 等技術。這些技術在 IPv6 都提供更好的設計，可以防止封包欺騙、偽造、修改、重播等攻擊。

216

IPv6 網路在安全機制的強化

- 使用鄰居探索(Neighbor Discovery, ND)進行位址自動設定：不同於 IPv4 於資料鏈結(Link-Layer)層以 ARP-RARP 找出主機位址，ND 於網路層(network-layer)操作減少欺騙主機的可能

- 更多的位址空間(Large address space)：不同於 IPv4 掃描一個 Class C 僅需四分鐘，由於 IPv6 一個子網是由 64bits 組成整個掃描則需耗時 584,942,417,35 年。

217

IPv4/IPv6 雙協定共存的安全議題

雖然 IPv6 增強了大部分的安全性，但也並非萬能藥，仍然有許多安全性的挑戰。

導入 IPv4/IPv6 雙協定後的安全性議題可以分成下列幾個主題探討，網路管理者可根據這些建議，對內部網域進行管控，觀察 IPv6 相關 flow，若有異常流量情形，例如要求不存在之服務則可設定規則過濾之。

218

IPv4/IPv6 雙協定共存的安全議題

- 雙堆疊相關安全性問題：例如不適當的防火牆攔截、不穩定的 DNS 區域記錄等，因此在網路建立前就須審慎規劃
- ICMPv6 安全性問題：IPv6 網路存在封包被攔截的可能，由於採用開放式路由廣播訊息(Router Advertisement, RA)，以協調網域中主機自動獲取位址，可能發生節點假扮為路由設備並發出錯誤的 RA 廣播訊息。

219

IPv4/IPv6 雙協定共存的安全議題

- 標頭操作相關議題：由延伸性標頭(Extension header)及 IPSec 的使用可以抵擋掉大部分攻擊種類，然而，由於 EH 須被整個網路堆疊進行處理，很長的延伸性表頭及大封包可能被利用來癱瘓某些特定節點(例如 防火牆)，或是假扮為攻擊，因此，最好的方式是過濾掉不支援的服務流量
- Spoofing 議題：欺騙技術仍然可能發生在 IPv6 網路中，但由於 Neighbor Discovery，Spoofing 欺騙的位址範圍僅侷限在內部網域。

220

IPv4/IPv6 雙協定共存的安全議題

- Flooding 議題：IPv6 位址不使用廣播位址已大幅減少攻擊的可能性，但多點位址傳送的位址仍然是問題，最主要的防範方式仍為過濾不存在服務之流量。

- 移動性 Mobility：移動性為 IPv6 的新特色，該協定是一複雜方程式，利用兩種類別的位址—真實位址(real address)和移動位址(mobile address)，由於此種網路的特性加上暫時性的移動位址可能暴露而成為欺騙攻擊，這需要特別安全性量測，並且網路管理者須全面了解設定。

221

點進網域新視界！

IPv4/IPv6雙軌環境之資訊安全軟體與硬體設定

IPv6 網路安全防護的建議

網路安全防護是矛與盾的戰爭，越厲害的矛會驅使發明更厲害的盾。

由於IPv6 網路尚未成為主流，相關的網路攻擊事件也幾乎還未聽聞，所以先就建議 IPv4 網路安全防護的做法為基礎，配合 IPv6 在通訊協定設計上的差異，進行規劃設置即可，同時也需要注意 IPv6 網路安全相關的研究報告，參酌安全設備廠商的建議，隨時進行安全強化的工作

223

1. 防火牆

清查既有防火牆是否支援 IPv6，如尚未支援，應經由韌體升級或重新採 購，取得支援 IPv6 的能力。以韌體升級方式支援 IPv6 的防火牆，必須注 意檢查 CPU Loading 及記憶體的消耗狀況，確定不會造成效能不足。

防 火牆支援 IPv6 後可參考 IPv4 既有規則設定 IPv6 的過濾方式，再依據監 控蒐集的 IPv6 流量資訊進行觀察，逐步補足 IPv6 的防禦規則。

224

1. 防火牆

ICMPv6 在 IPv6 網路扮演很重要的角色

在 IPv4 網路裡大部分的 ICMP 都會被關掉

再選擇適當的項目開放。

225

1. 防火牆

- 必須開放的 ICMP：Types 1, 2, 3, 4, 128, 129, 130, 131, 132, 143, 148, 149, 151, 152, 153, 133, 134, 135, 136, 141, 142
- 通常開放的 ICMP：Types 3 - Code 1, Type 4 - Code 0
- 必須過濾丟棄的 ICMP：Types 138,144,145,146,147
- 視需要制定是否過濾丟棄的 ICMP：Types 137,139,140,5-99,102,126

226

NetFlow

升級路由器的 IOS 至支援 NetFlow version 9，以提供 IPv6 的流量統計資 料，Netflow 分析軟體(如 Netflow Analyzer)也要升級到支援 IPv6

建議以不同時間排程將 IPv6 與 IPv4 流量資訊的抓取與分析時間錯開，以降低設備負載度

1:1 的 NetFlow 是目前正夯的研究資料收集目標

227

(1) 依服務類別統計流量：

每天依據服務類別統計流量資訊，例如依據 Inbound、Outbound、SSH 連線、FTP 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計。

統計的項目包括連線流量、封包數目、封包大小等，並在位居排名前面(如前 20 名)的服務類別中，觀察送出該流量的 IP 位址、總流量數、總封包數、總封包大小。

228

個人 IPv6 流量資訊查詢：

每天依據使用者 IPv6 位址統計網路流量資訊

統計的項目包含上述提到的各種服務

並以圖表呈現各類別流量一週的使用資訊

229

DPI System

DPI 主要目的為觀察封包 Payload 並比對出可疑流量，IPv6 流量 Payload的比對方式與 IPv4 並無不同，目前持續累積足夠的 IPv6 可疑流量特徵(Signature)，建議可配合 Netflow 的統計，針對異常流量進行 Payload 的觀察，以蒐集建立異常流量的特徵值數據庫

230

異常位址追蹤與控管

IPv6 用戶端位址的自動核發機制主要為 SLAAC (包含 SLAAC RDNSS 及 SLAAC + Stateless DHCPv6) 以及 Stateful DHCPv6，建議優先選用 Stateful DHCPv6 的位址核發機制，可以如同 IPv4 DHCP 的管理方式，記錄 IPv6 位址的核發記錄，並控管位址的核發原則，例如依據 MAC 位址綁定 IPv6 位址，或依據 MAC 位址管制是否核發 IPv6 位址。

231

異常位址追蹤與控管

如果選用 SLAAC 機制，則只能依據 Prefix 追蹤到相關的區域網路，雖然藉由 EUI-64 運算法可從 IPv6 位址反算出 MAC 位址，但用戶端可設定不使用 EUI-64，MAC 位址也可以手動變造，並不能保證能找出特定 IPv6 位址的使用者

所以在 SLAAC 的機制下，要責成每個區域網路的連線單位自行負擔/64 網段的資安管理責任

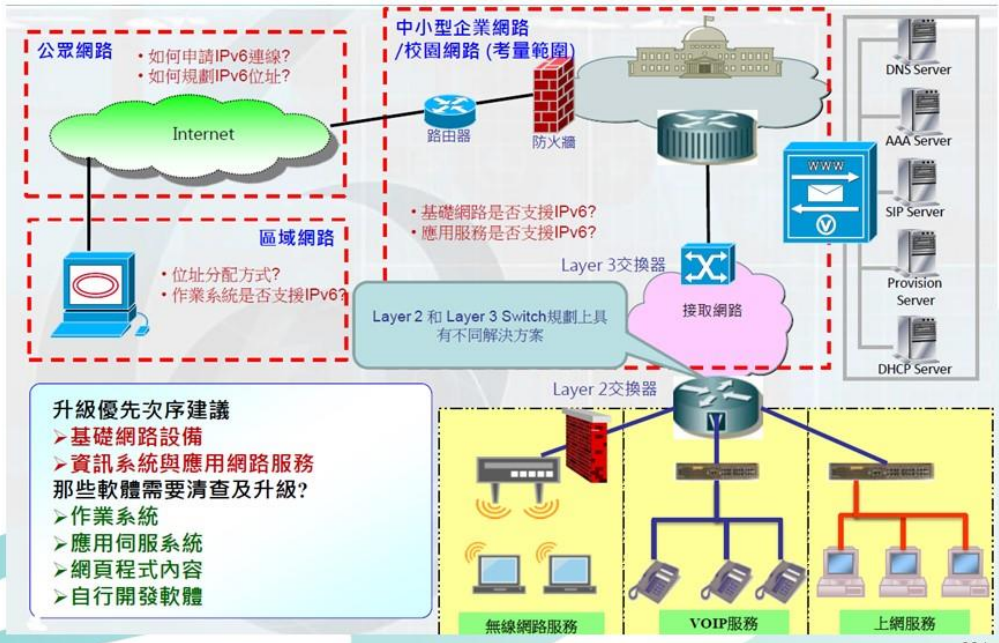
232

點進網域新視界！

IPv4/IPv6雙軌環境下資訊安全檢查項目清單(網路環境、作業系統、網站、資安設備)

233

IPv6網路升級考量



升級優先次序建議
- 基礎網路設備
- 資訊系統與應用網路服務

那些軟體需要清查及升級?
- 作業系統
- 應用伺服系統
- 網頁程式內容
- 自行開發軟體

234

升級作業考量 升級經費與人力評估

- 升級目標：
  - –IPv6升級非一蹴可幾
  - –降低導入成本為優先選擇
  - –達到採取無縫隙升級目標
- 評估重點項目：
  - –上級單位或上級主管願意提供多少預算進行升級？
  - –網路管理人員是否有足夠人力支援IPv6升級？
- 成立升級團隊
  - –網路管理人員是否有相關IPv6技術背景？
- 委外訓練：如：搭配購案採買新型網路系統…
- 自辦訓練：如：聘請講師…等

235

升級作業考量 網路架構升級評估

- 升級目標：
  - –以雙協定為升級終極導向
- 評估重點項目：
  - –外部接取網路調查：
- 網路服務供應商(ISP)是否提供IPv6接取方案？
- 上級單位是否提供IPv6接取方案？
  - –內部網路架構調查：
- 釐清現有IPv4網路拓樸圖
- 規劃未來雙堆疊(Dual Stack)網路拓樸圖

236

升級作業考量 網路架構升級評估

- 網路設備IP位址規劃以及如何配置？
- 基礎網路設備調查：
  - 內部傳輸設備：路由器、L3交換器、L2交換器…等是否支援雙協定？
  - 資安防護設備：IDS、IPS、防火牆…等是否支援雙協定？
  - 網路管理設備：流量監控設備及流量報表程式是否支援雙協定？
  - 加值服務設備：VPN Server、Network Storage …等是否支援雙協定？

237

升級作業考量 終端設備升級評估

- 升級目標：
  –從終端使用者之角度來思考
- 評估重點項目：
  - 使用者較常使用那些Internet & Intranet服務？
    EX：DNS, Web Services (eForm)、E-Mail Services…等
  - 清查終端資訊設備是否支援雙協定?
    使用者設備之作業系統支援現況，EX：Windows, Linux…
    資訊系統設備之應用程式，EX：DHCP, FTP, DNS…
  - –是否以採購方式進行IPv6升級方案？
  - 添購新型終端資訊設備以支援雙協定？
  - 添購新版作業系統授權碼以支援雙協定？

238

升級作業考量 維運人員與使用者心態

- 評估重點項目：
  - 網路維運人員心態：
    - 因已熟系IPv4運作與設定拒絕配合
    - 須花費額外時間重新了解新的技術
    - 須花費時間熟悉新設備及設定，如：IPv6配發機制、DNS設定
  - 使用者面對升級心態：
    - 因使用習慣排斥配合升級及修改設定
    - 因額外費用拒絕更換現有軟硬體
    - 因網路順暢度對升級的誤解
  - 宣導政策減緩對未知的恐懼：

239

升級作業考量 維運人員與使用者心態

- 評估重點項目：
  - 網路維運人員心態：
    - 因已熟系IPv4運作與設定拒絕配合
    - 須花費額外時間重新了解新的技術
    - 須花費時間熟悉新設備及設定，如：IPv6配發機制、DNS設定
  - 使用者面對升級心態：
    - 因使用習慣排斥配合升級及修改設定
    - 因額外費用拒絕更換現有軟硬體
    - 因網路順暢度對升級的誤解
  - 宣導政策減緩對未知的恐懼：
    - 教育訓練與講座
    - 提供簡易的升級設定降低技術門檻
    - 誘因式的導入，如：差別化服務..

240

調查升級網路架構

建議升級順序

1. 核心層(Core Layer)：
2. 分配層(Distribution layer)：
3. 接取層(Access Layer)：

241

基礎網路架構分類

核心層(Core Layer)

- 環境：骨幹網路 (Core Network, Backbone)
- 用途：負責運輸大量的網路訊務，並且達到快速與可靠的服務
- 設備：對外ISP連接之路由器，如：ATM Switch, MPLS Switch, Core Router…

242

基礎網路架構分類

分配層(Distribution layer)

- 環境：接取網路(Edge Network)
- 用途：負責做額外判斷網路訊務封包，提供Routing, Network Policy (如：Security, Filter, QoS…等)服務
- 設備：Layer 3 Switch, Firewall…

243

基礎網路架構分類

接取層(Access Layer)

- 環境：DMZ(外部WWW/DNS/E-mail 伺服器)，Server Farm (內部使用伺服器)，辦公室區域網路
- 功能：負責提供可靠的網路接取給終端設備或重要的Content和網路應用服務，提供Switching, Access Control (VLAN Tagging…)
- 設備：Layer 3 Switch(VLAN), Layer 2 Switch(VLAN), Wireless Router, PCs, Servers, Printers…

244

網路設備IPv6升級概念

設備汰換時，必須支援 Dual Stack IPv4/IPv6

- 處理Layer 3以上資訊相關的設備
  - 提供Routing技術，處理IP層封包的設備，如：路由器、第三層交換機(Layer 3 Switch)、防火牆、負載平衡器…等
- 處理Layer 2相關的設備
  - 提供Switching技術，第二層交換機，如：第二層交換機(Layer 2 Switch)
  - 確保可透通IPv6訊務 (包含Multicast與Unicast)

245

調查網路設備現況 (1)

- 網路傳輸設備
  - Switch Hub, Layer 2 Switch、Layer 3 Switch、Router…等
- 網路安全防護設備
  - 防火牆(Firewall, FW)、入侵偵測系統(IDS)、入侵防護系統(IPS) 、新一代防火牆(Network Generation Firewall, NGFW)…

246

調查網路設備現況 (1)

- 應用伺服器
  - DNS、Web、FTP、Proxy、Media、Database…
- 網路管理設備
  - SNMP Manager, Multi Router Traffic Grapher (MRTG)
- 終端設備
  - 個人電腦、筆記型電腦、平板電腦、行動電話…等

247

調查網路設備現況 (2)

清查網路設備IPv6支援程度

- 網路設備廠牌與供應商
- 網路設備廠軟體版本
- 網路設備授權年限
- 網路設備目前CPU乘載量

請注意，若是CPU 已接近滿載設備
建議重新添購新設備支援IPv6

248

調查網路設備現況 (3)

網路設備支援IPv6現況

- 原有網路設備已內建支援IPv6功能，網路管理員僅需執行基本IPv6指令，如：設定、啟動與測試...等步驟，即可升級支援IPv6。
- 原有網路設備未支援IPv6，透過官方所釋放的新版本韌體，進行官方標準更新動作，即可升級支援IPv6。
- 上述情況無法導入IPv6，則建議列入汰換清單，重新採購新型網路設備。
- 網路設備升級負責人

249

https://www.gsnv6.tw/download.html

IPv6內部網路完成升級報告書

IPv6內部網路升級作業規劃書

250

資料來源

- TWNIC 財團法人台灣網路資訊中心
- 行政院 NICI 小組網際網路通訊協定升級推動辦公室

251

Thank You

252