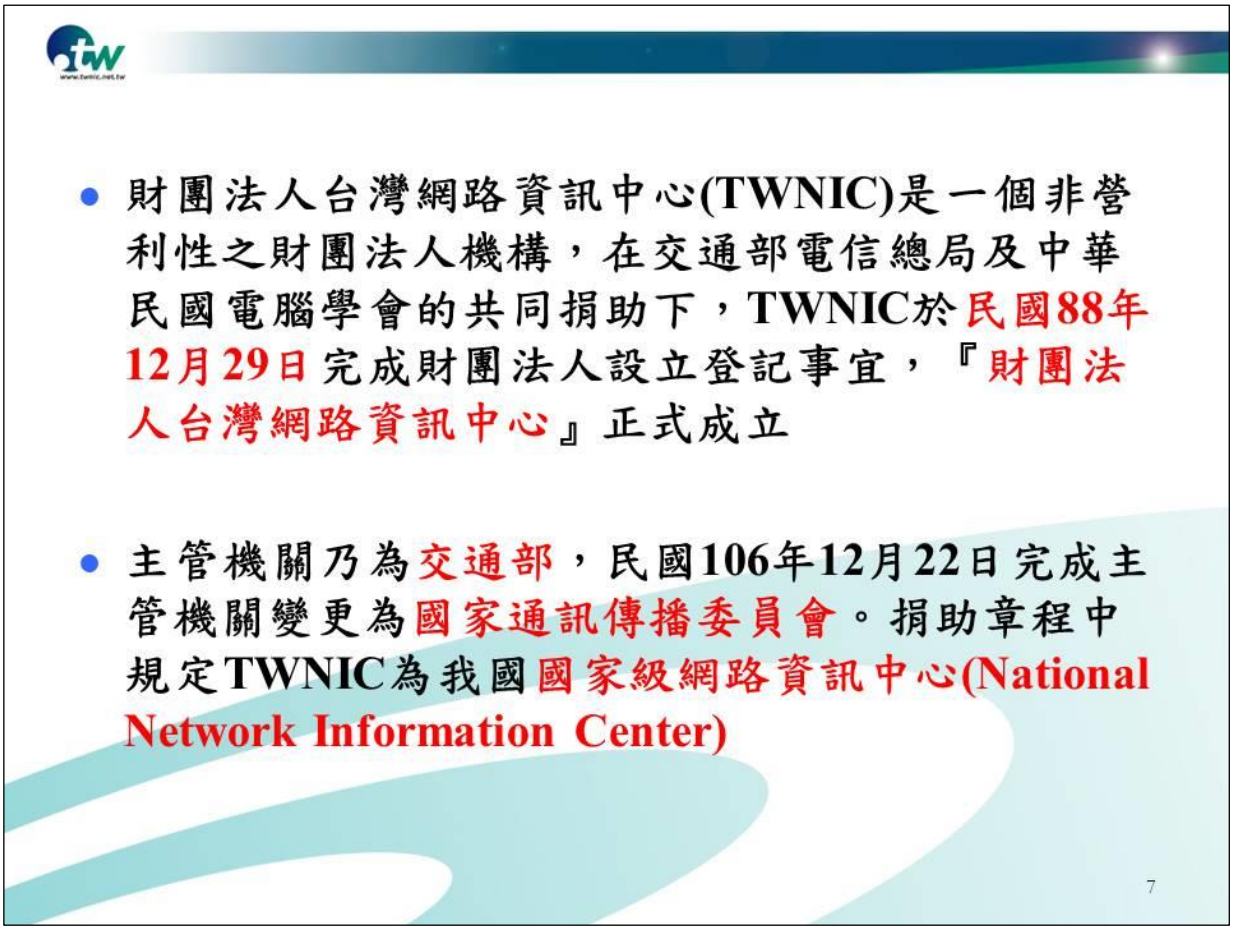
『推動 IPv4/IPv6 雙軌普行方案』

附錄三
『ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練』
課程教材

目錄

一、 TWNIC 財團法人網路資訊中心簡介



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。

8

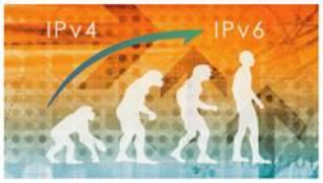
- TWNIC是目前國內唯一統籌網域名稱註冊及IP位址發放之超然中立之非營利性組織，除提供國內完整之網路服務外，更積極參與各項國際相關網路會議。

- 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。

9

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。

「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

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

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」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

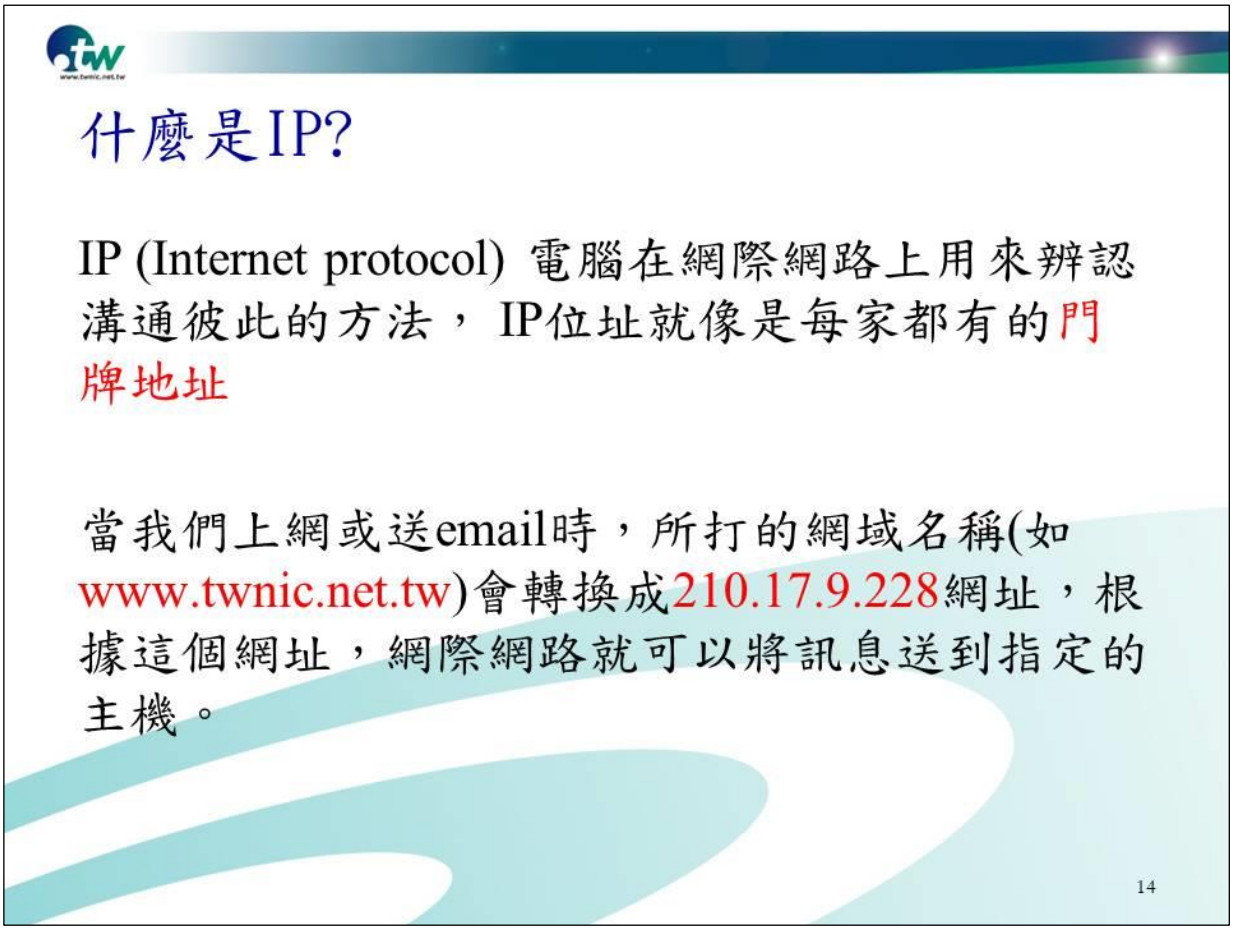
2019-05-06 | 活動訊息

ICANN與TWNIC共同在台北舉辦網路論壇

2019-04-18 | 活動訊息


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
12

二、 IPv4/IPv6 雙軌運作概念介紹



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。

15

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?

16

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)

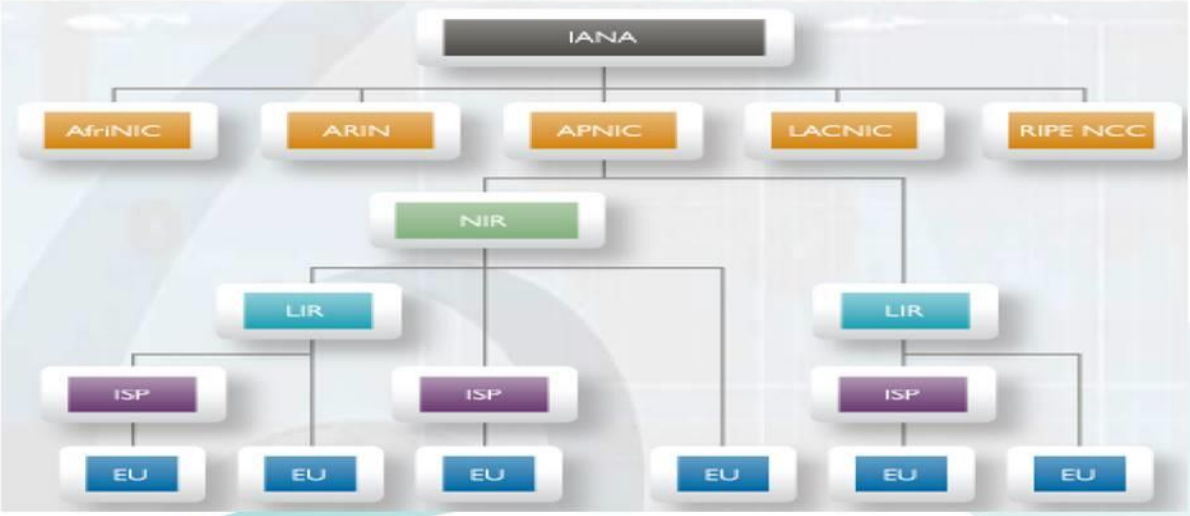
–歐洲地區：RIPE NCC
Réseaux IP Européens Network Coordination Centre
–北美地區：ARIN
American Registry for Internet Numbers
–亞太地區：APNIC
Asia Pacific Network Information Centre
–拉丁美洲：LACNIC
Latin American and Caribbean Internet Addresses Registry
–非洲: AfriNIC
Africa Network Information Centre

17

全球網際網路號碼管理架構

18

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

19

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

20

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

21

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

22

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

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

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

25

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

26

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。

27

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

28

IPv4技術本身的缺陷

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

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

29

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

30

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

31

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

32

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)

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」

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

35

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

36

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)

37

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

38

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

39

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

2003000000000B30000000000001234

(太長容易記錯)

40

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)

41

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

42

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

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。

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

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)

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。

47

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

48

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

49

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

IPv6 IP address 全部都是IPv4 Public IP address

50

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

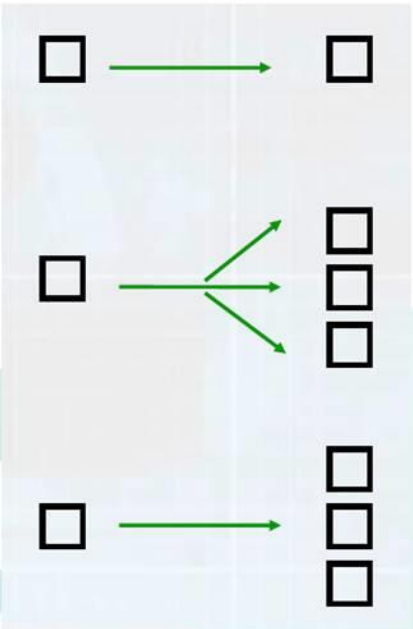
讓IPSec直接可以鑲嵌在IPv6的封包中

Basic Address Types

•Unicast (點對點傳輸)

•Multicast (群播傳輸)

•Anycast (多點備援傳輸)



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

53

Unicast Address Structure

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

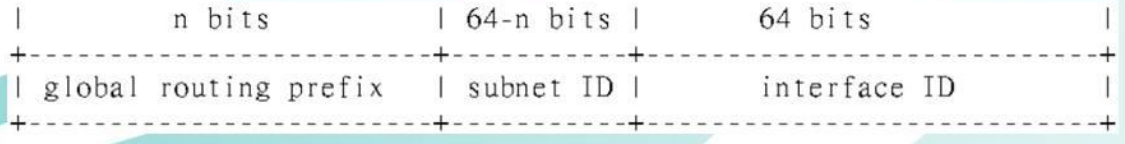
網路位址部份 2003:0:0:B3

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



54

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)

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

Interface ID 產生方式

1.採用modified EUI-64 演算法，經由MAC Address計算出Interface 位址

2.作業系統自動產生隨機位址

3.手動設定

4.Tunnel Server系統自動產生或指定

5.經由加密機制產生之虛擬位址(IPv6 IPSec)

6.DHCPv6伺服器指定(Stateful)

由MAC Address 產生Interface ID

1.First three octets of MAC is Company-ID

2.Last three octets of MAC is Node-ID

3.將 FFFE置入Company ID與Node-ID間

4.Company ID 2進位表示法之第7碼為Univeral/Local-Bit，設為1表示Global Scope

如: MAC Address為 00-C0-3F-BB-93-91，則

1.Company ID 為00-C0-3F， Node ID為BB-93-91

2.00-C0-3F-FF-FE-BB-93-91

3.Company ID 2進位表示法為00000000 11000000 00111111

4.將第7bit改為1，為00000010 11000000 001111111

5.重組為02-C0-3F

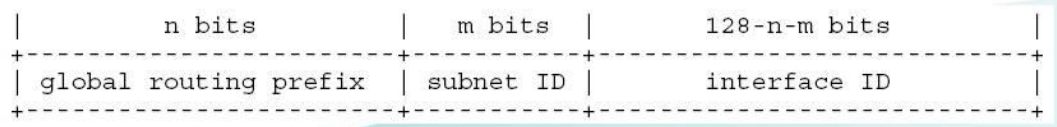
6.Interface ID為 02C0:3FFF:FEBB:9391

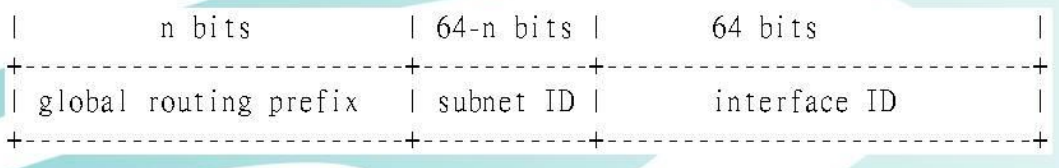
Global Unicast Address

•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.





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

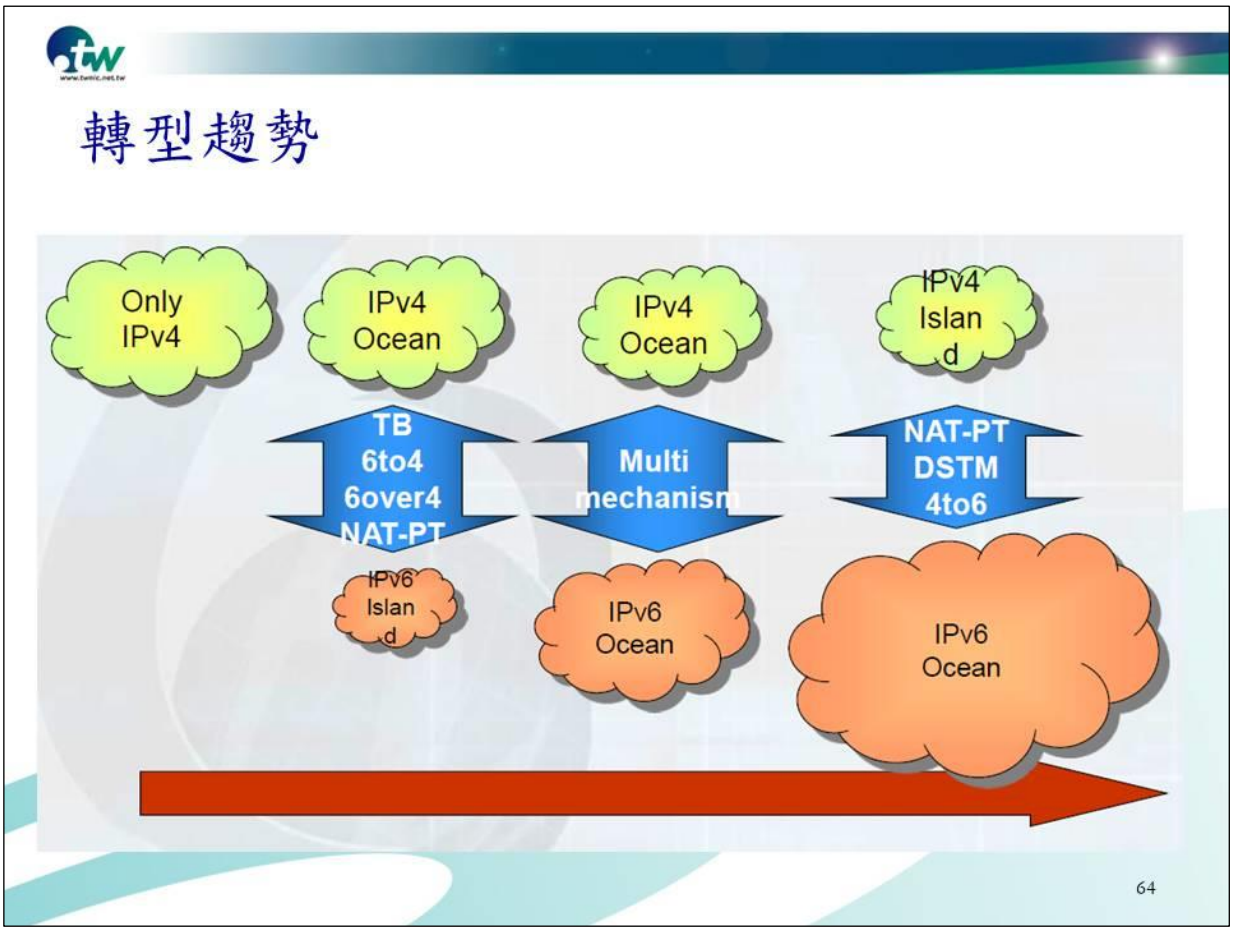
Link-Local Address

- 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

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

三、 IPv4/IPv6 雙軌環境建置概述



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

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。

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。

67

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。

68

三大類過渡技術

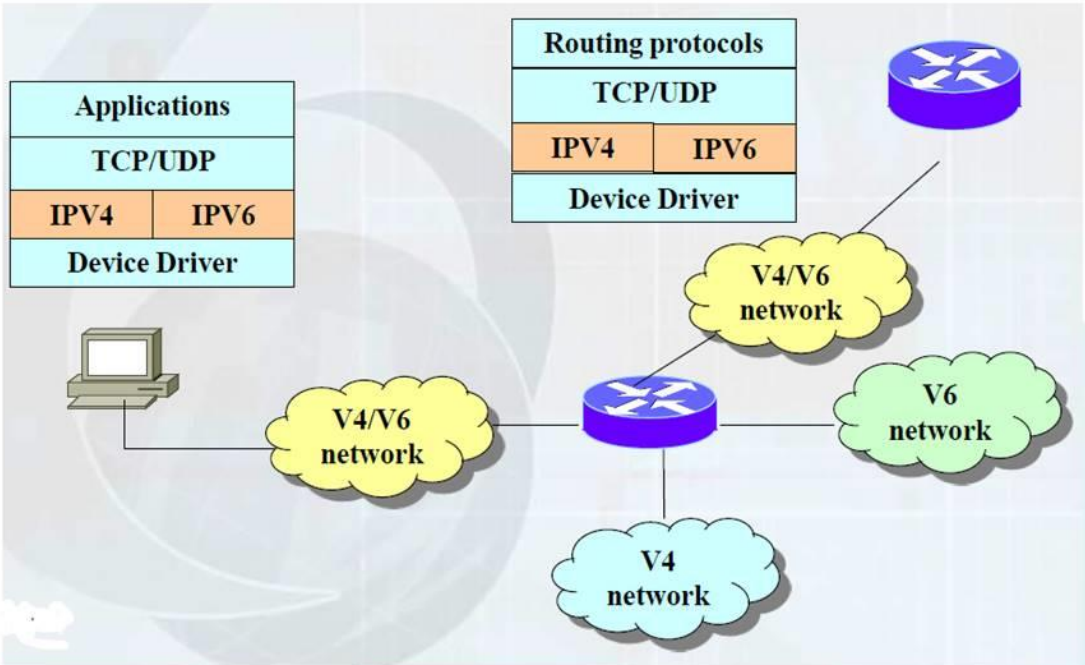
1. IPv6/IPv4 Dual Stack

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

Dual Stack Mode 示意圖



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

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

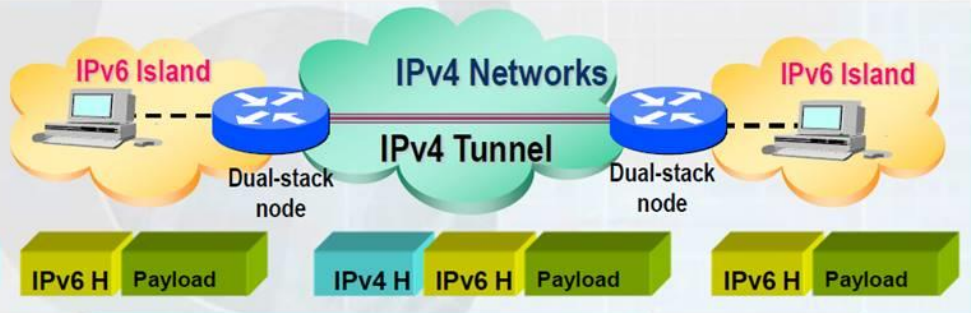
Tunnel 的種類(一)

• 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

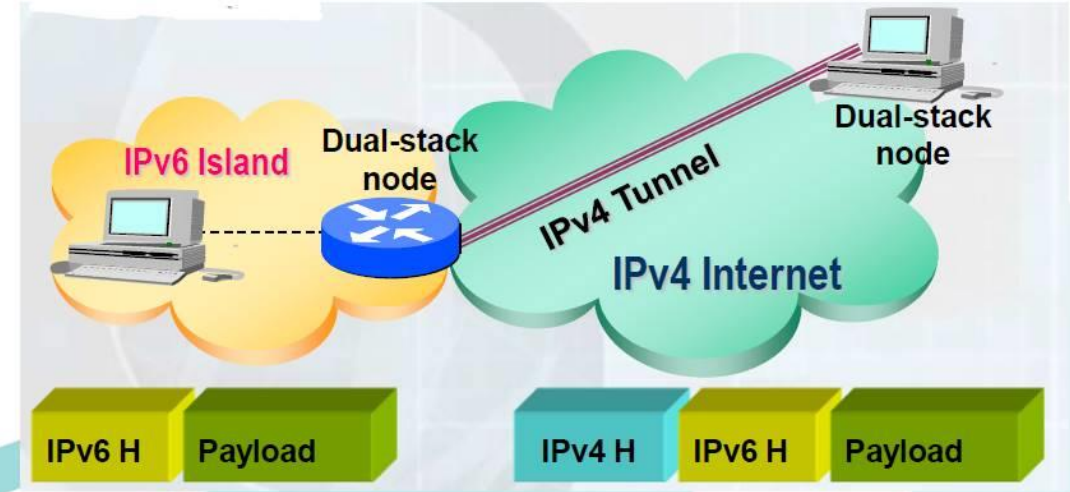
缺點:設定之工作負擔很重



73

Tunnel 的種類(二)

• Automatic Tunnel



74

Automatic Tunnel

ISATAP:
優點: 使用者完全不用進行設定，適用於企業內部網路之步署。可為Private IPv4使用者提供Public IPv6 之位址, Cisco路由器支援
缺點: 安全性不足,會造成Bottle Neck。但如配合Firewall使用，即為安全性最佳之解決方案。
6to4:
優點: 適用於WAN端連結，Cisco路由器支援
缺點: 安全性不足，網際網路連線能力不足，沒有Business Model
Teredo:
優點:可以讓在IP分享器後之虛擬IP Tunnel Client 與使用Public IP之Teredo Tunnel Server 建立IPv6 Tunnel
缺點: 使用者需進行設定、安全性不足、難以控管、會造成Bottle Neck、 Cisco路由器不支援。

75

Tunnel Broker System

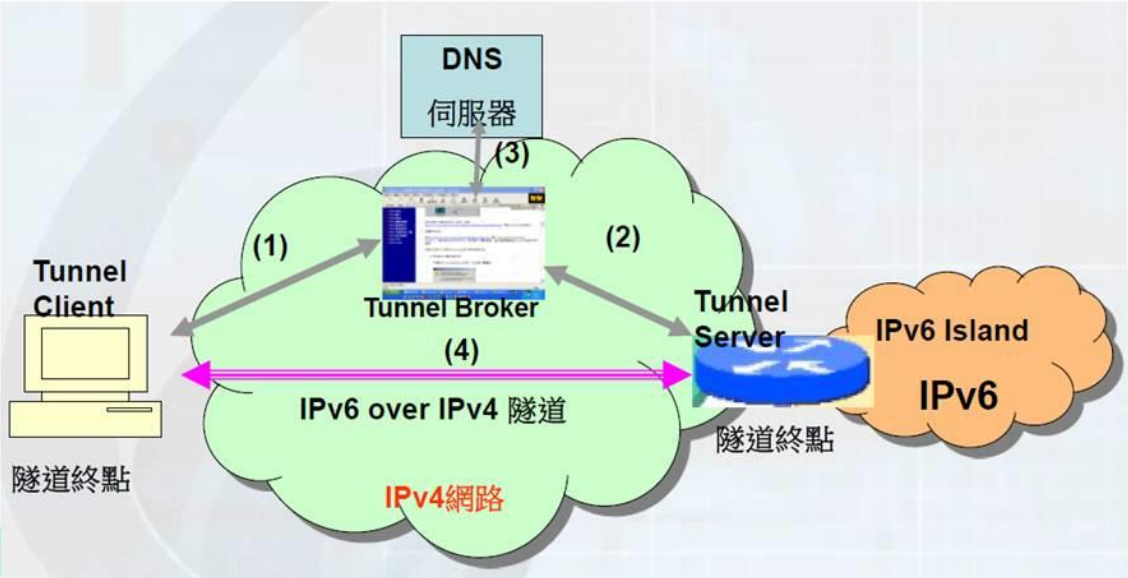
由於Automatic Tunnel 無法有效進行安全管控，而Configured Tunnel 需要太多的手動設定。

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

76

Tunnel Broker 系統示意圖



77

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

78

Translator的功用

1. IPv6在根本上改進了IPv4原有的缺點，並移除了原來IPv4最仰賴的Broadcast機制。因此原有在IPv4上的應用必須重寫才能支援IPv6

2. 為了讓原IPv4的應用可以用到IPv6網路上，必須要經過Translator的轉換，將IPv4的模式及IPv6的模式相互轉換，才有機會讓應用程式能夠互通

3. 很多應用程式在IPv6時的編寫標準與IPv4不時是有差異的，必須要靠依據個別程式的特性，打造其專屬的轉換機制

Translator 技術之限制

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

四、 IPv4/IPv6 雙軌網路環境建置

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)。

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

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。

85

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

86

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

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

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

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。

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。

91

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。

92

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。

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

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。

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

97

(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

98

(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

99

(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

100

(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

101

(三) 防火牆的限制

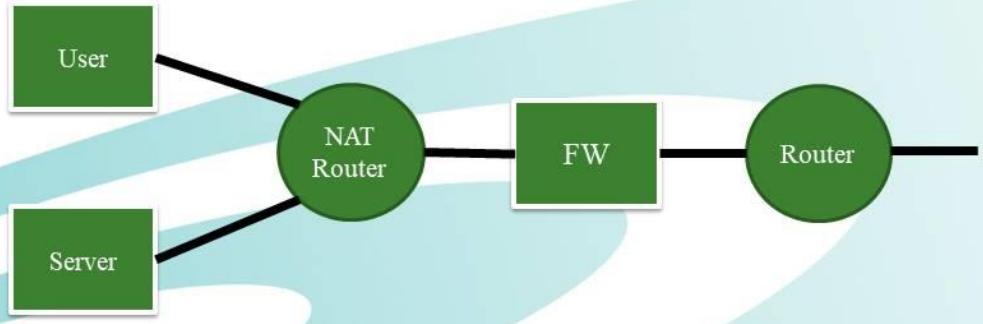
防火牆無法抵擋所有型態的訪問與攻擊，尤其傳統的防火牆運作在網路的第三層與第四層為主，對於應用層的攻擊或是session layer的攻擊往往需要搭配其它資安設備與策略進行防堵

新型態防火牆 Layer 7 Application Firewall

102

(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



(一) 透通模式Transparent Mode

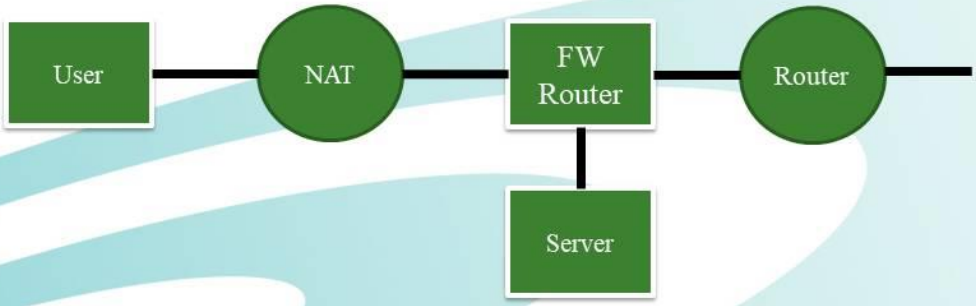
採用本架構可以限制外來的訪客對於內部網路的存取，並且在不改變內部原有的設備設定，以提供內部使用者安全的IPv4/IPv6對外存取服務。

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。

(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



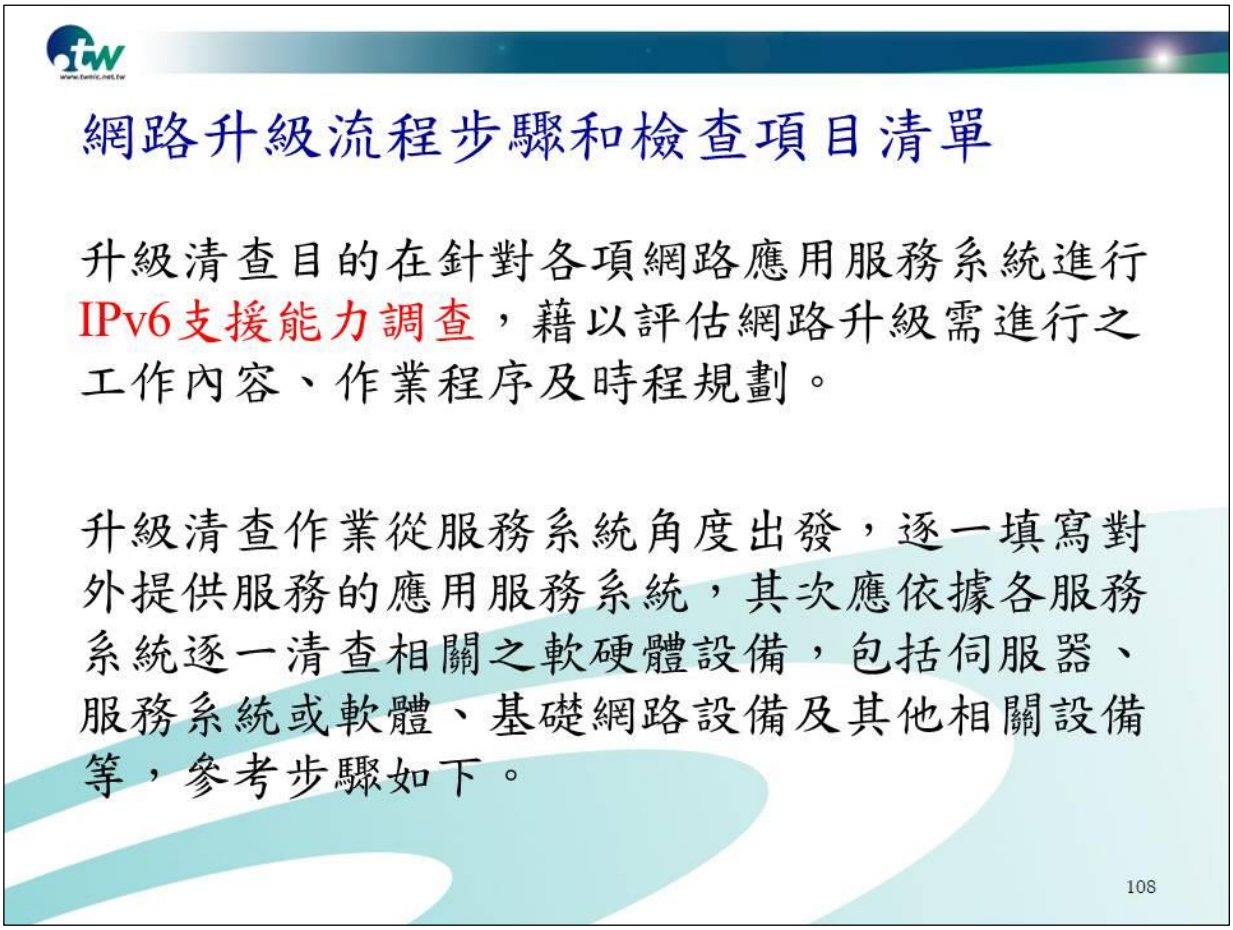
(二) 路由模式Route Mode

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。

五、 網路升級流程步驟和檢查項目清單



(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

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

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

111

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。

112

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

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)

(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

(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

(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。

(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。

(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。

119

(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

120

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。

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

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

網路升級檢測

網路除錯通常使用 ping6 與 tracert6

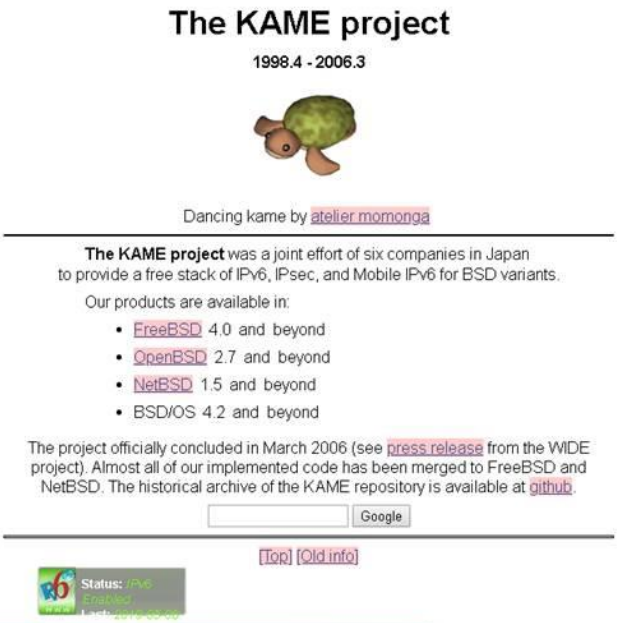
如要進行此類測試，應事先檢查網路上相關設備是否已開放此類封包訊息傳送，如路由器、防火牆、伺服器、終端電腦等

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

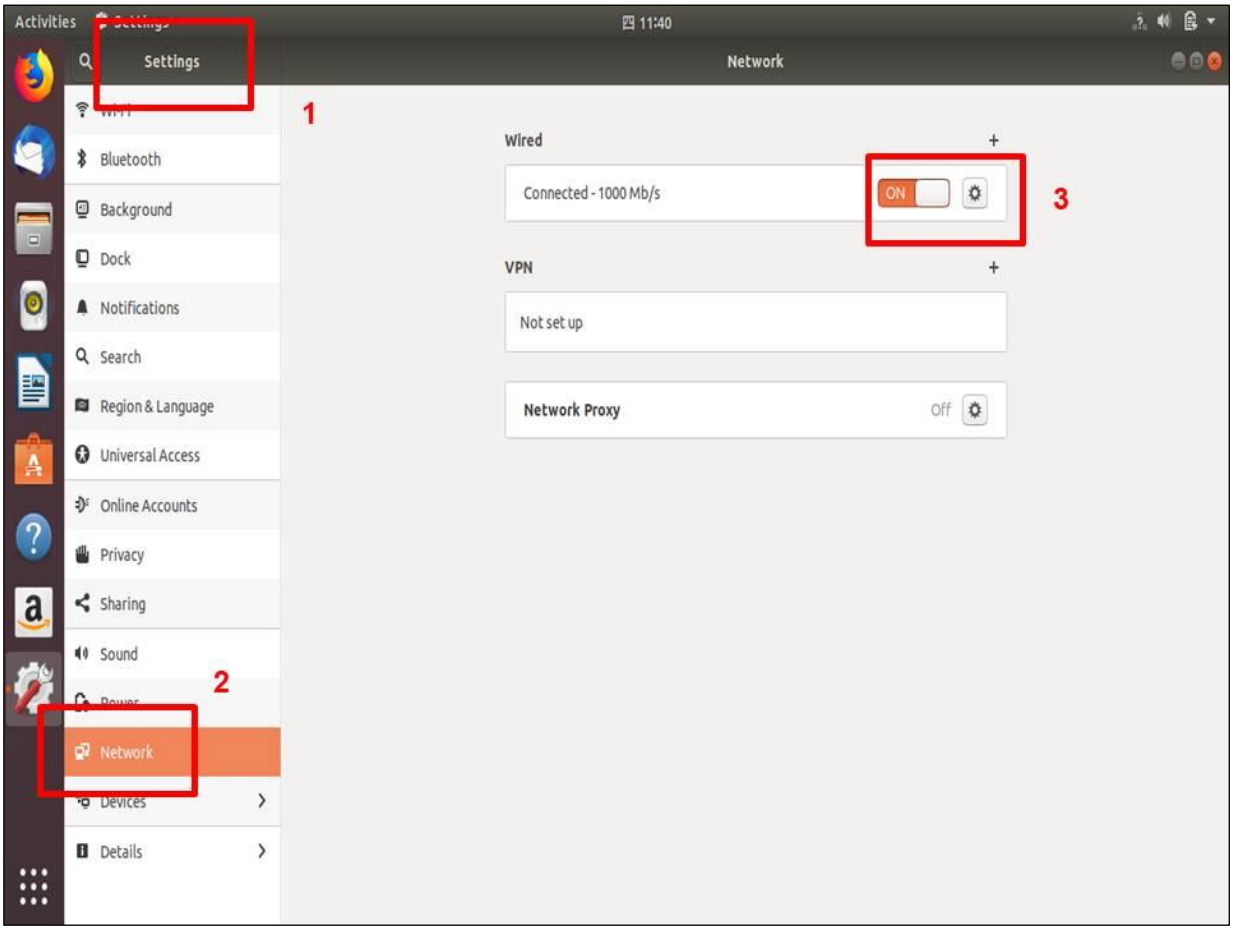
以下提供檢測IPv6能力的測試網站：

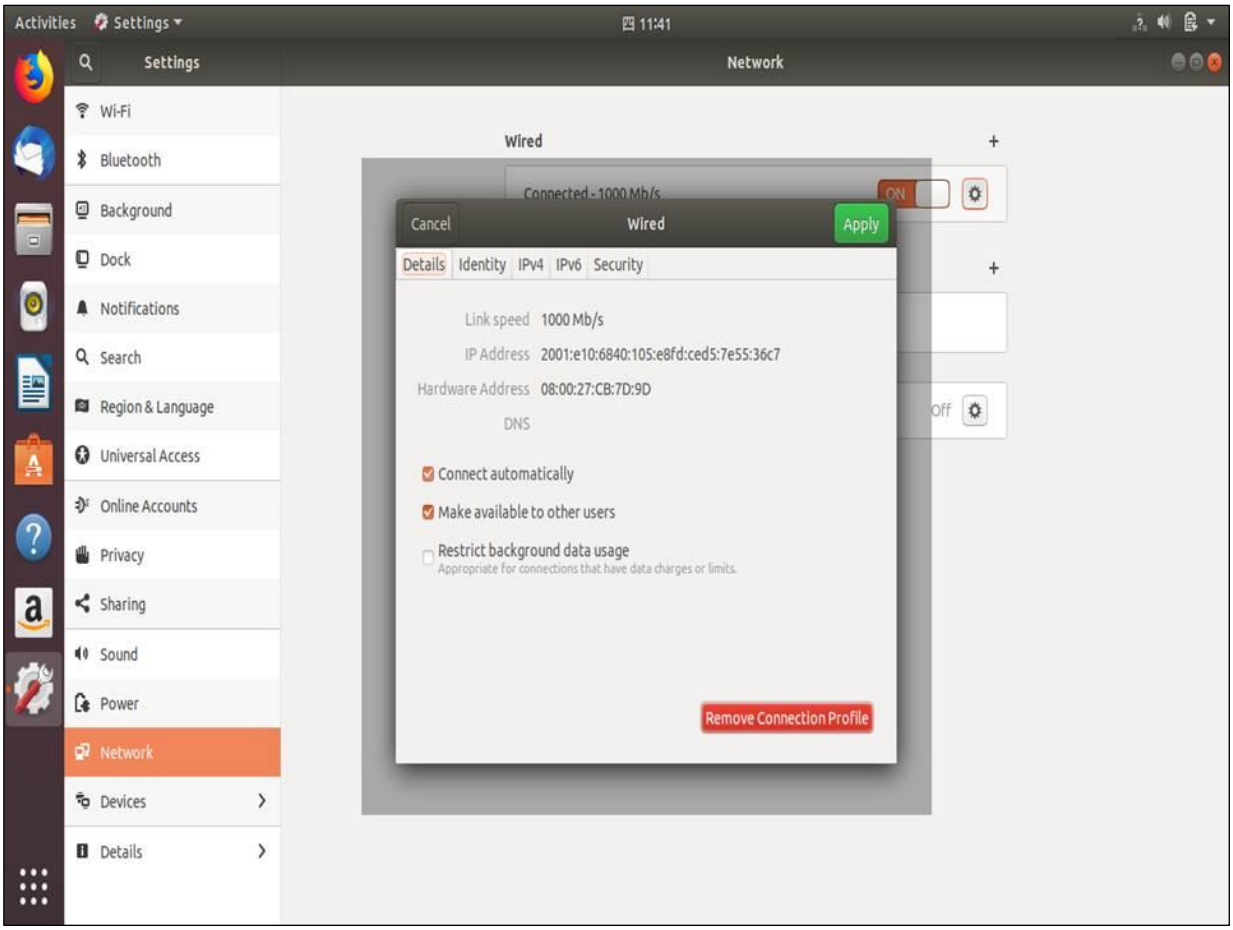
http://test-ipv6.com/

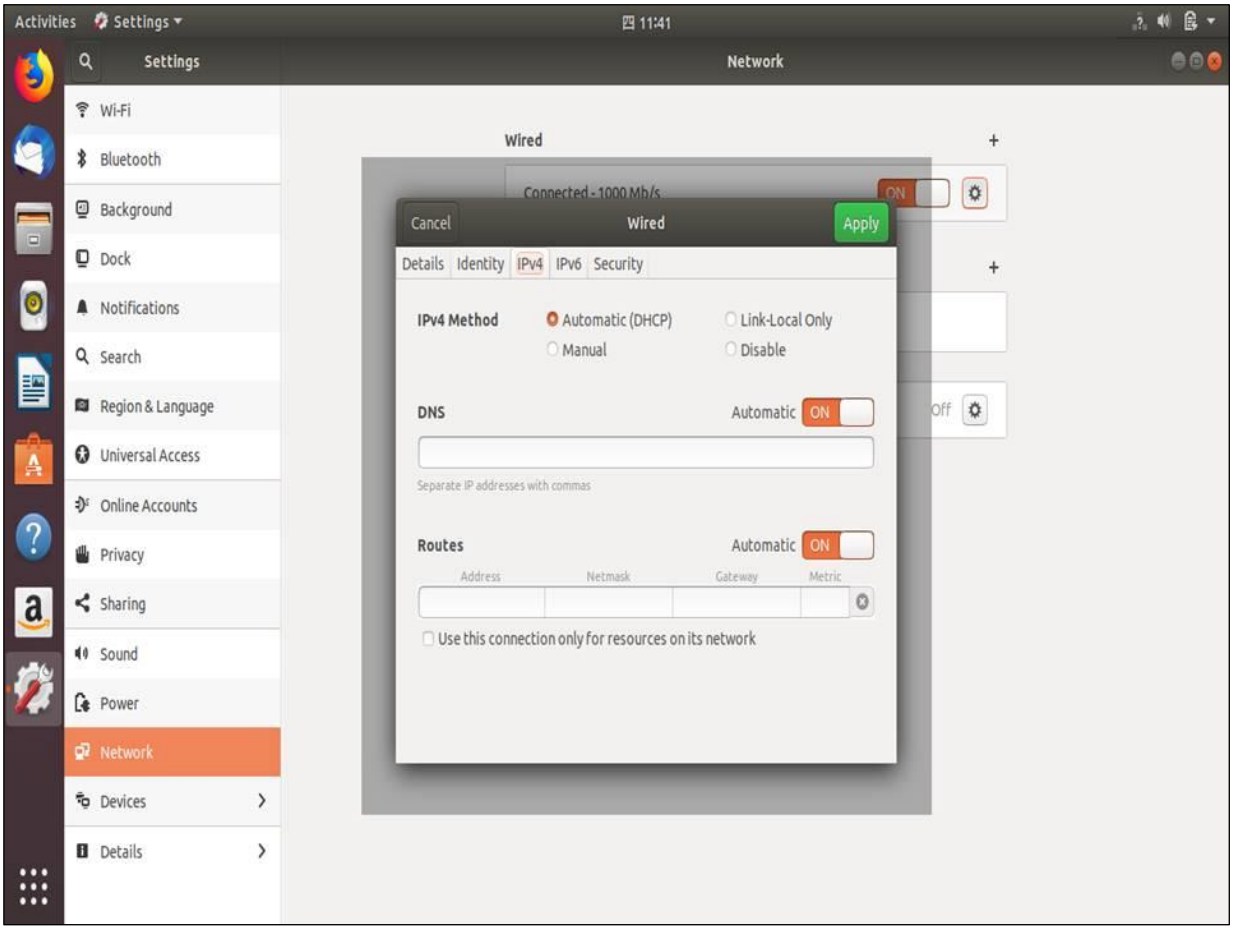
http://www.kame.net/

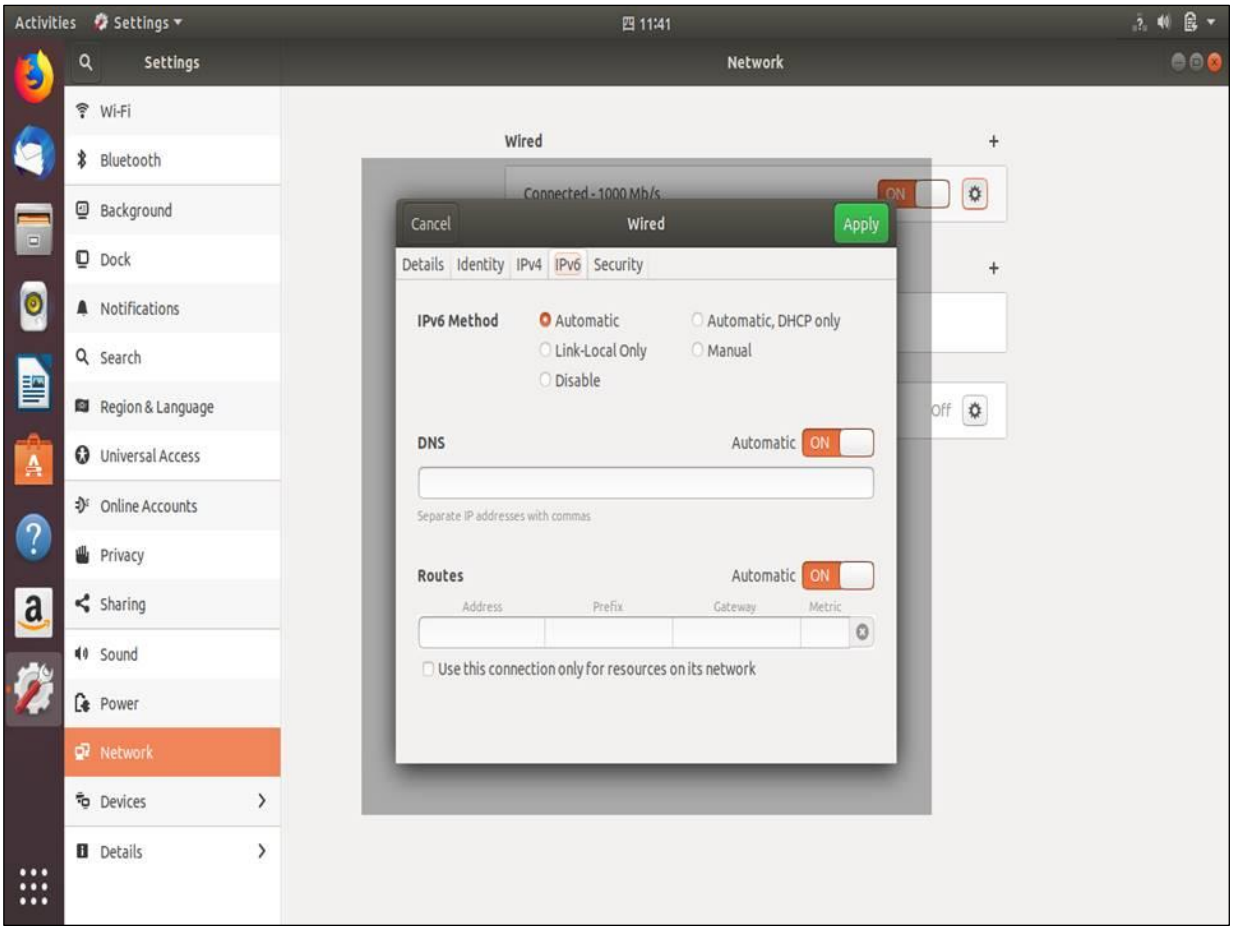


六、 IPv6 建置示範 Ubuntu 作業系統

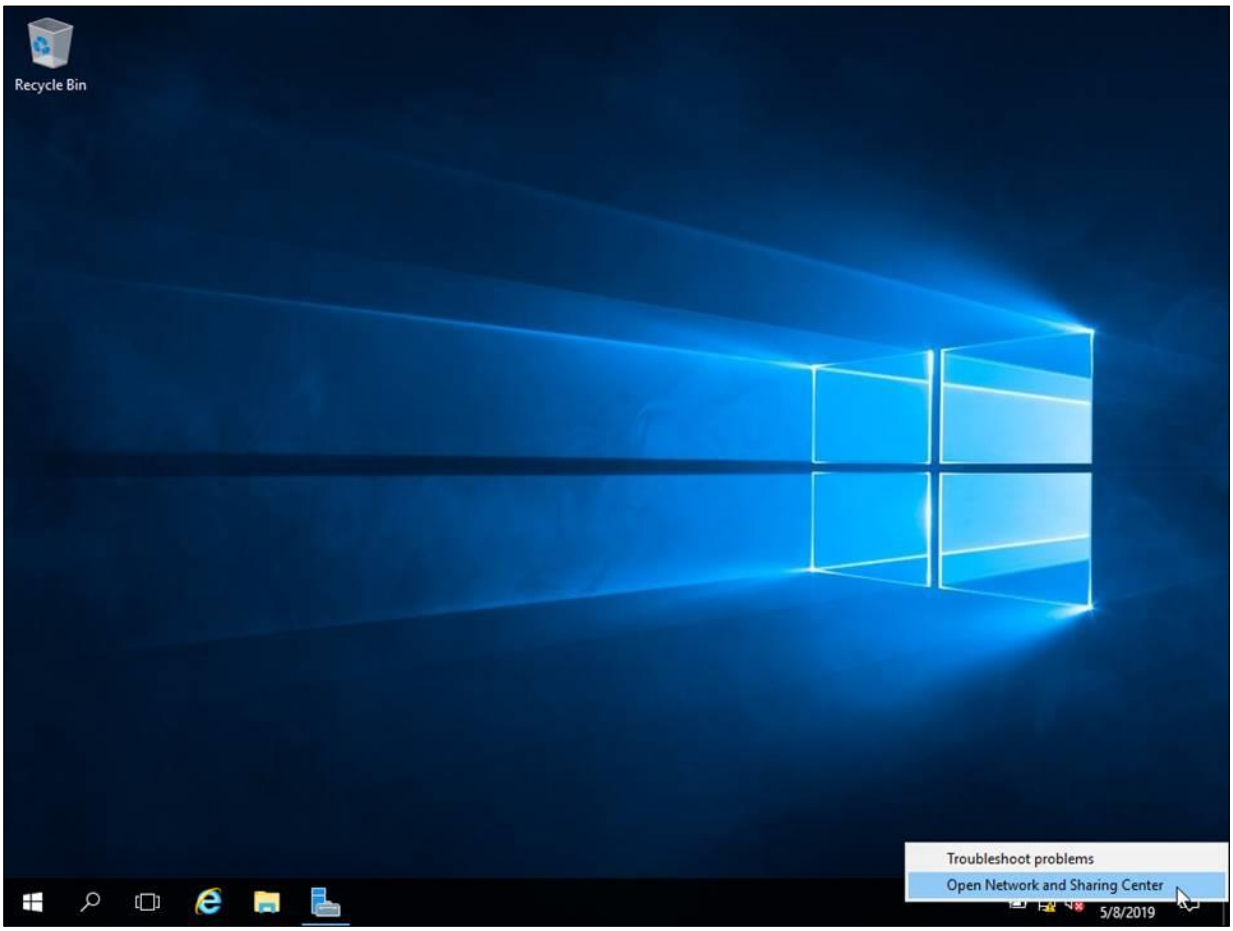


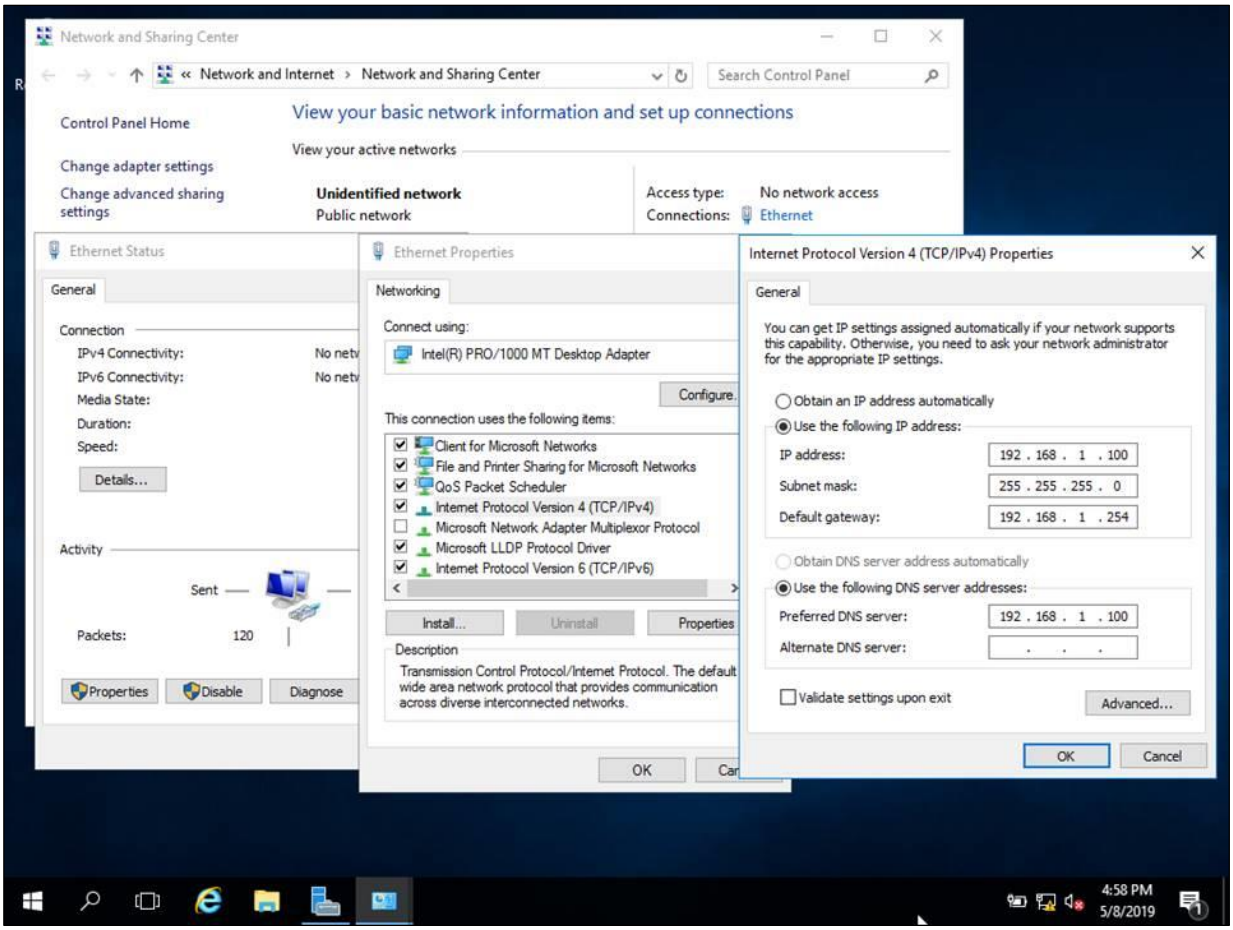

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 2001:e10:6840:105:e8fd:ced5:7e55:36c7
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

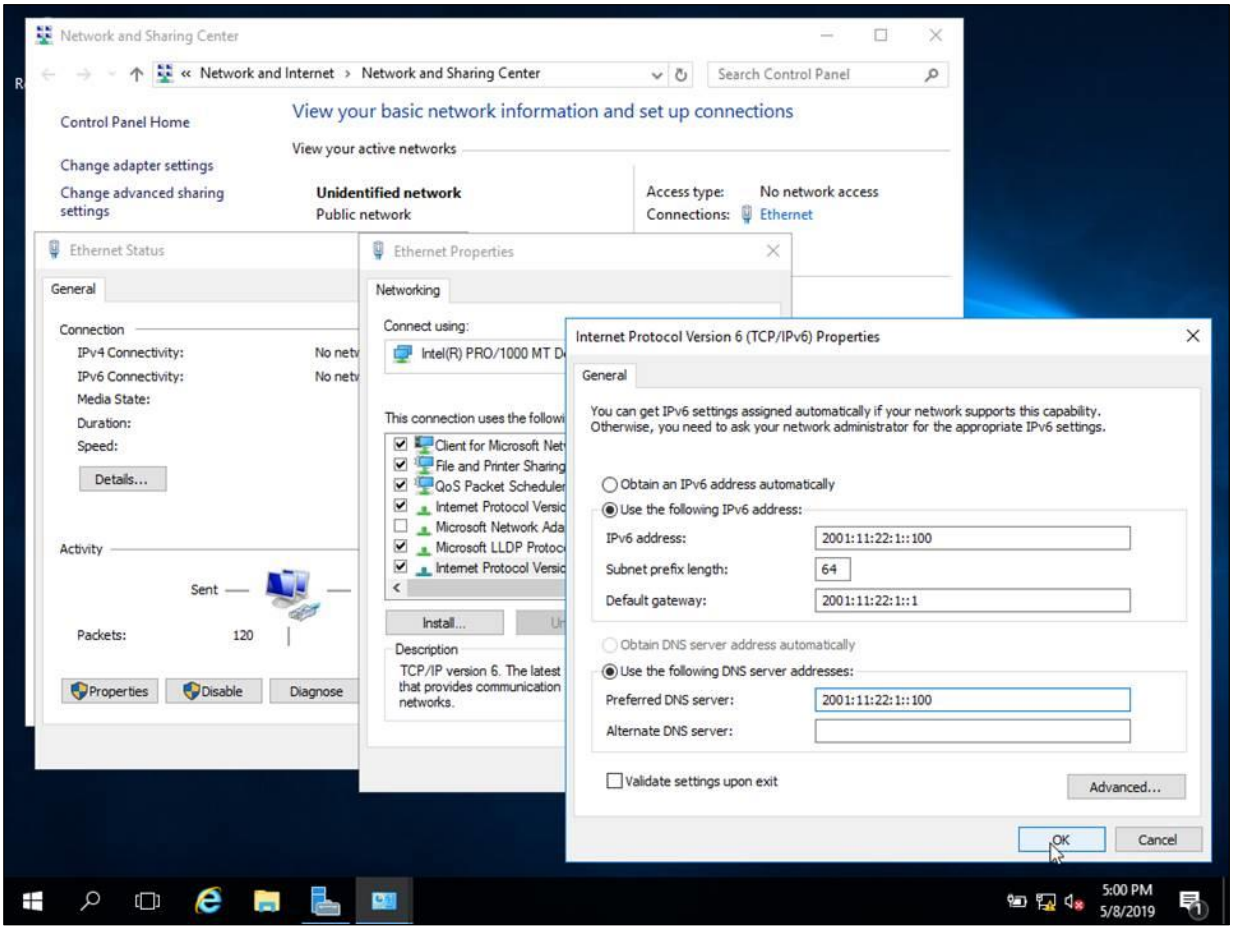

Activities
Settings
11:41
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Power
Network
Devices
Details
Wired
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Method
Automatic (DHCP)
Link-Local Only
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


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
Off

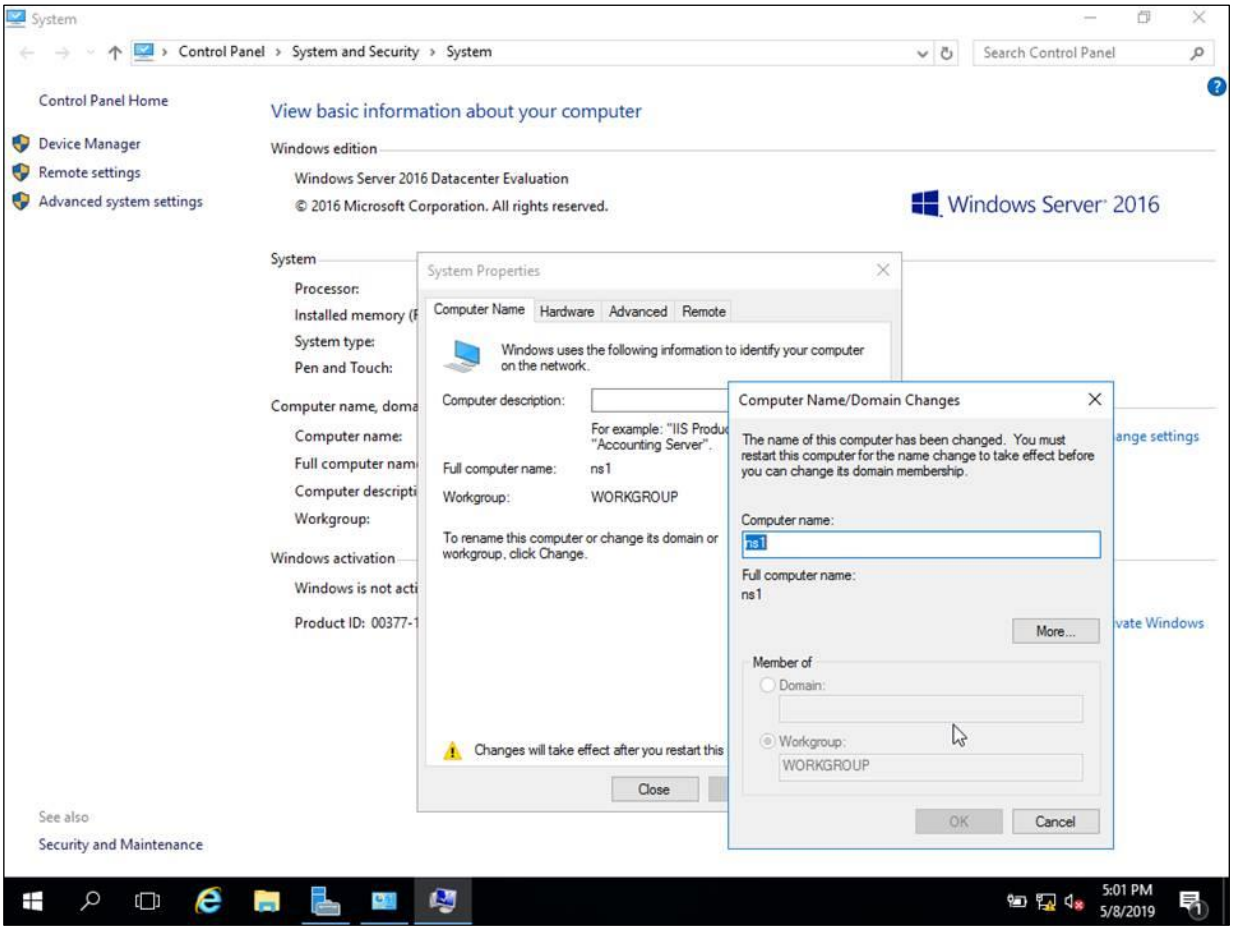
七、 IPv6 建置示範 Windows server 2016 作業系統

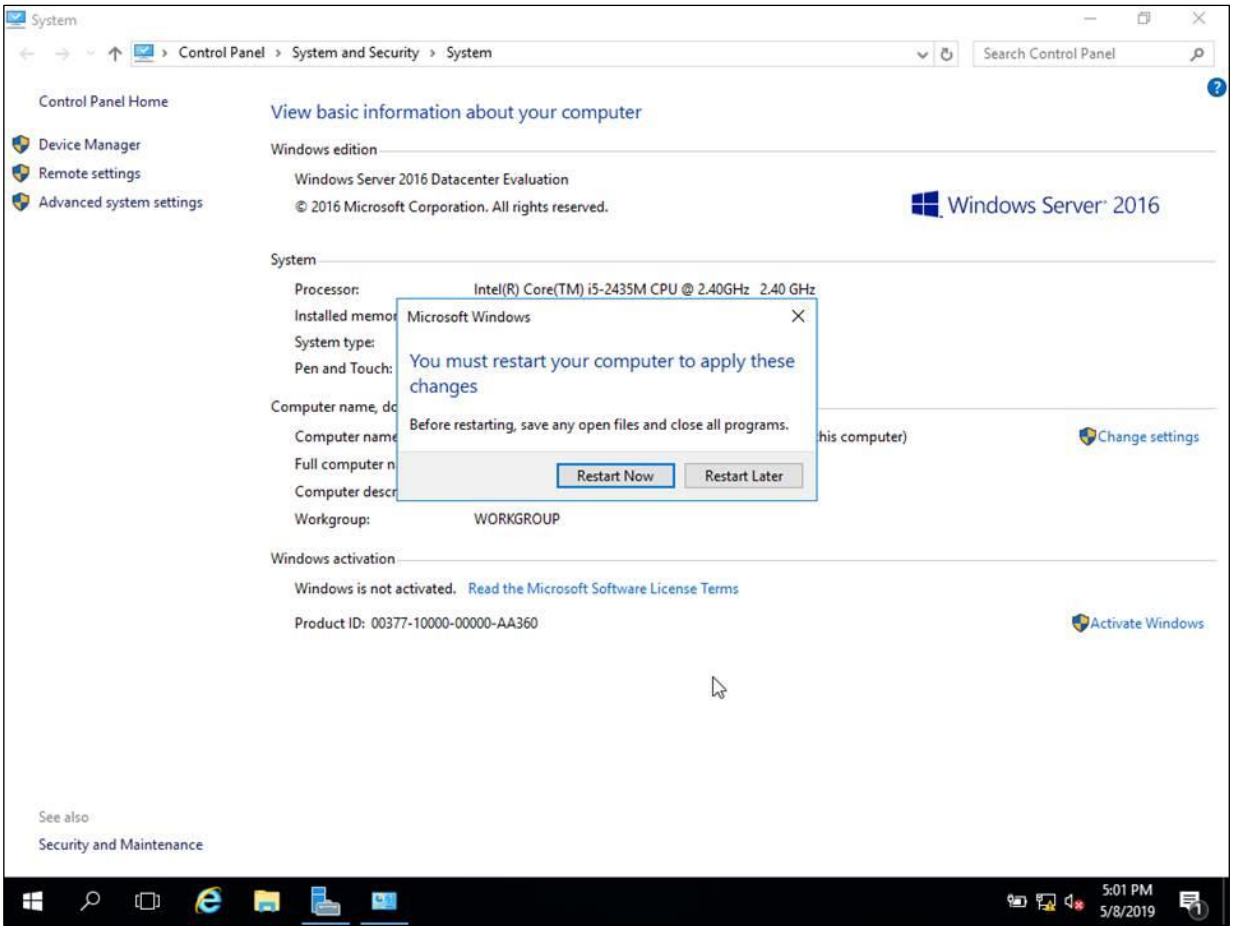


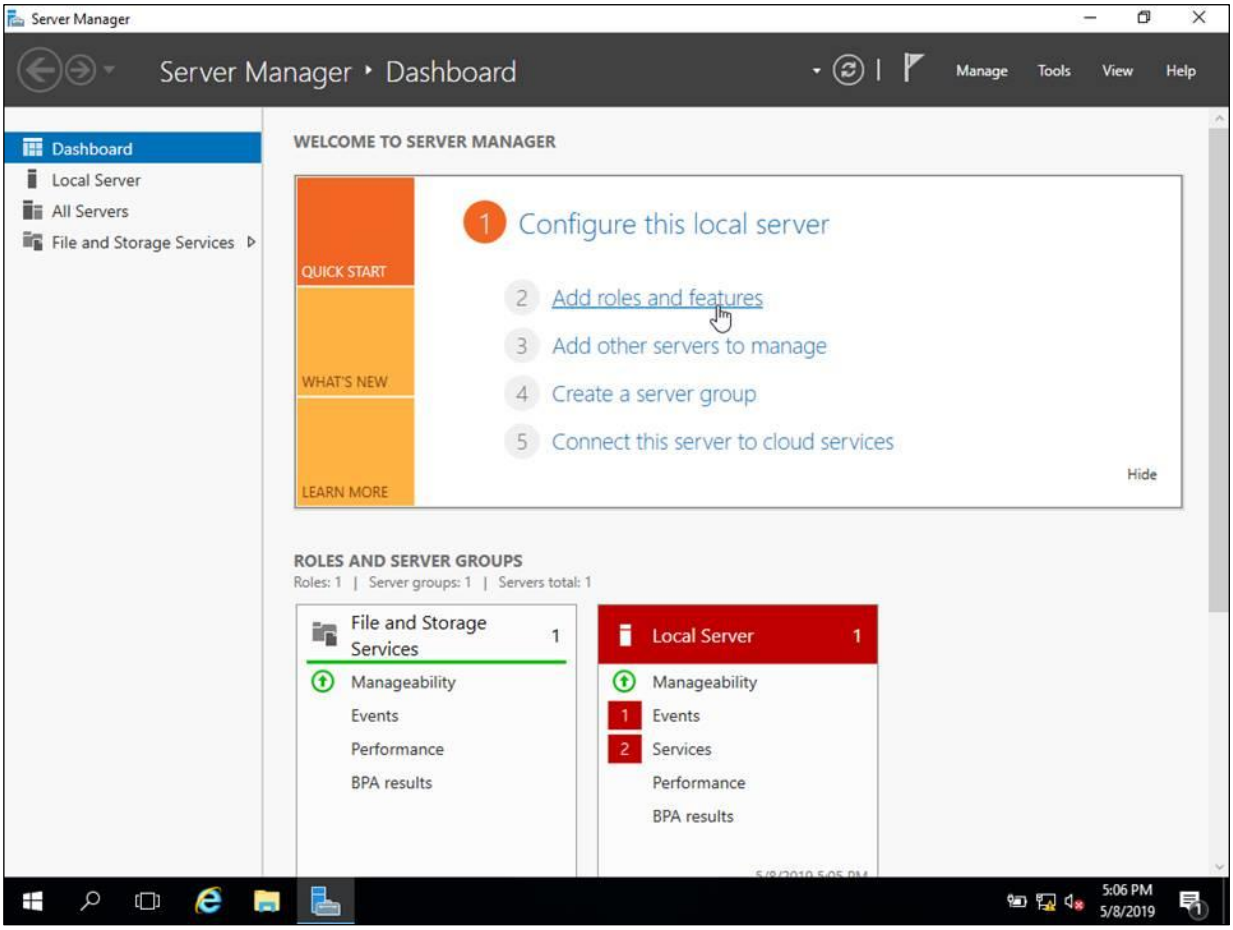

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
Change adapter settings
Change advanced sharing settings
View your active networks
Unidentified network
Public network
Access 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

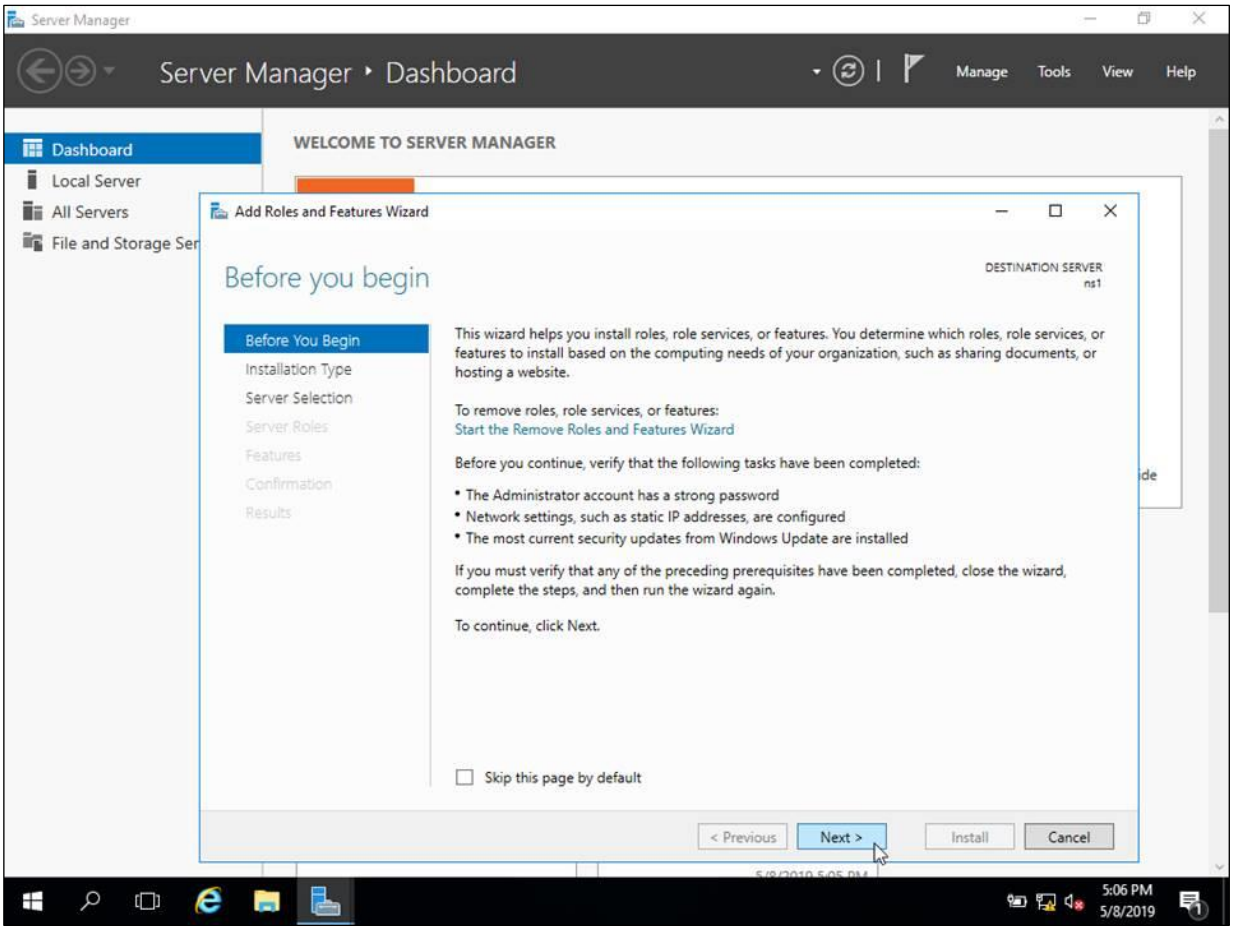

Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
View your basic network information and set up connections
Change adapter settings
Change advanced sharing settings
View your active networks
Unidentified network
Public network
Access 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:
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

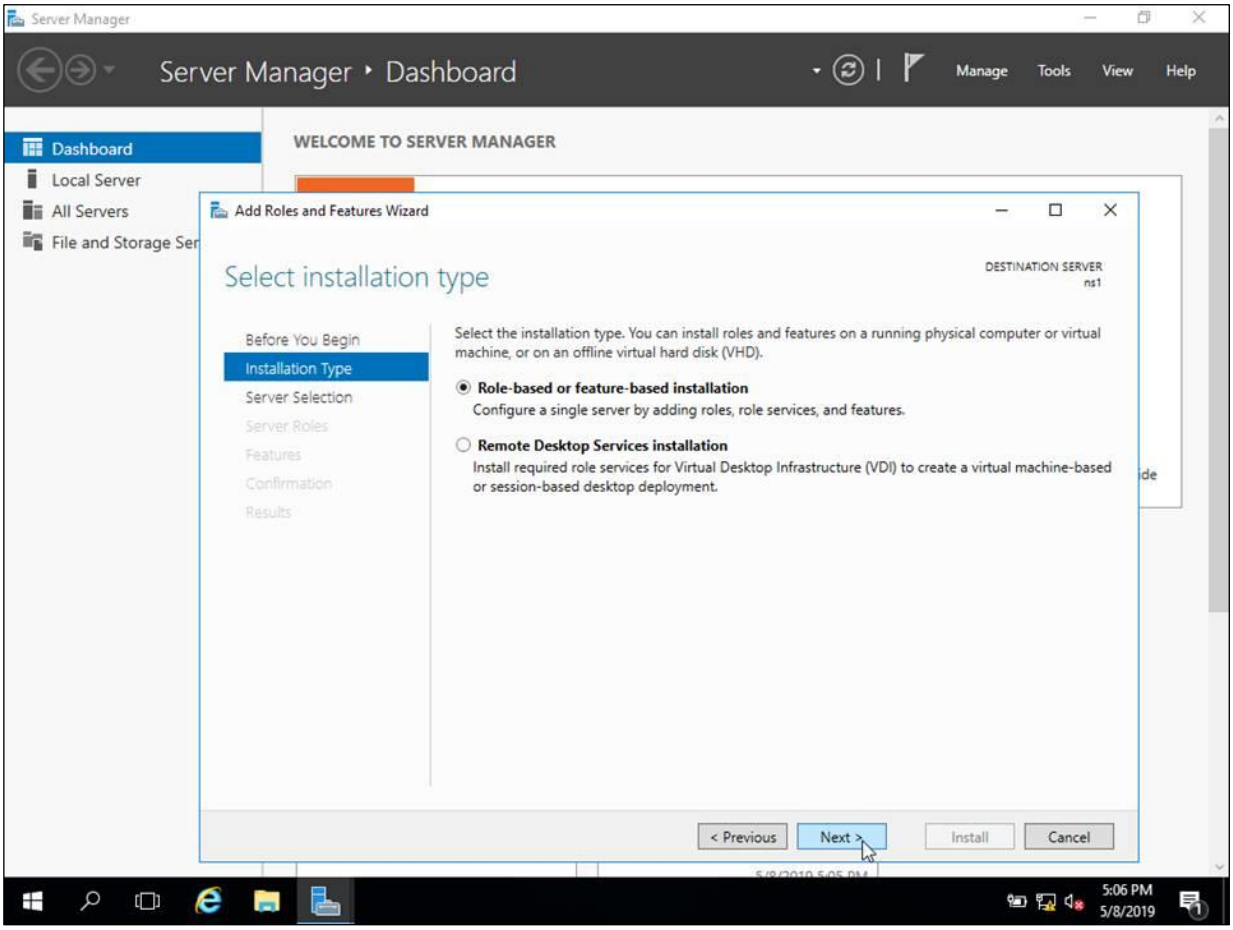
八、 IPv6 建置示範 DNS Server

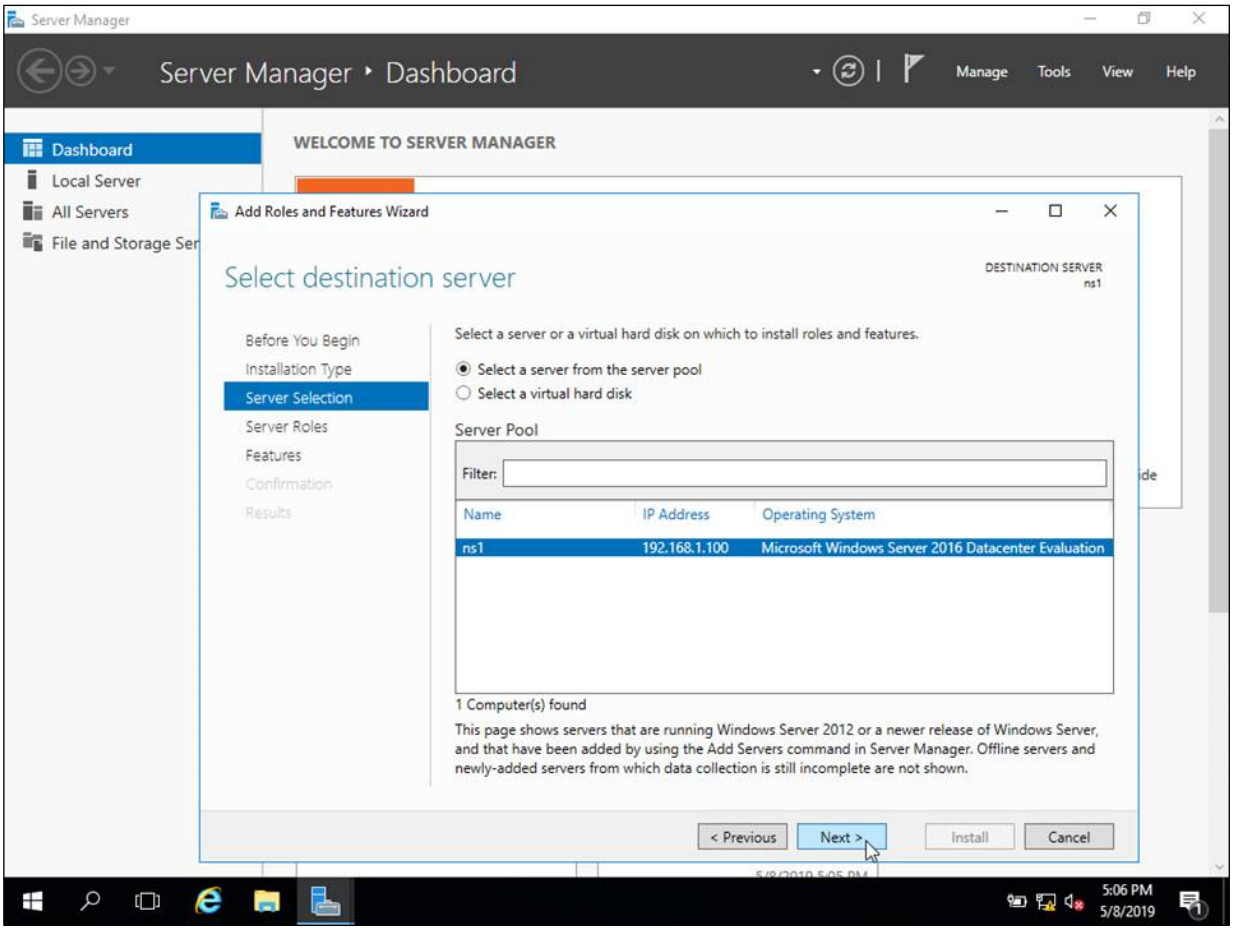


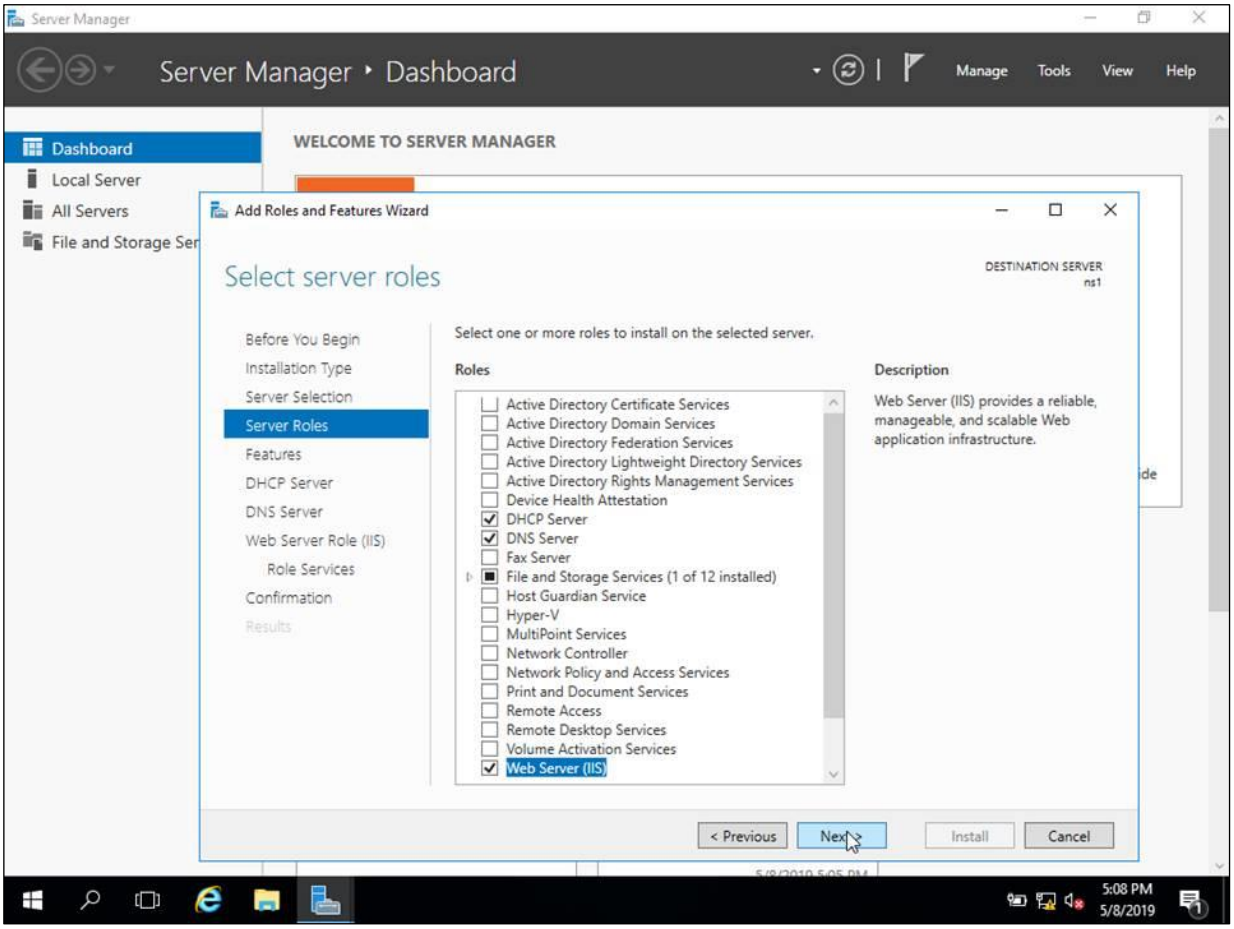

System
Control Panel › System and Security › System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2016 Datacenter Evaluation
© 2016 Microsoft Corporation. All rights reserved.
Windows 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

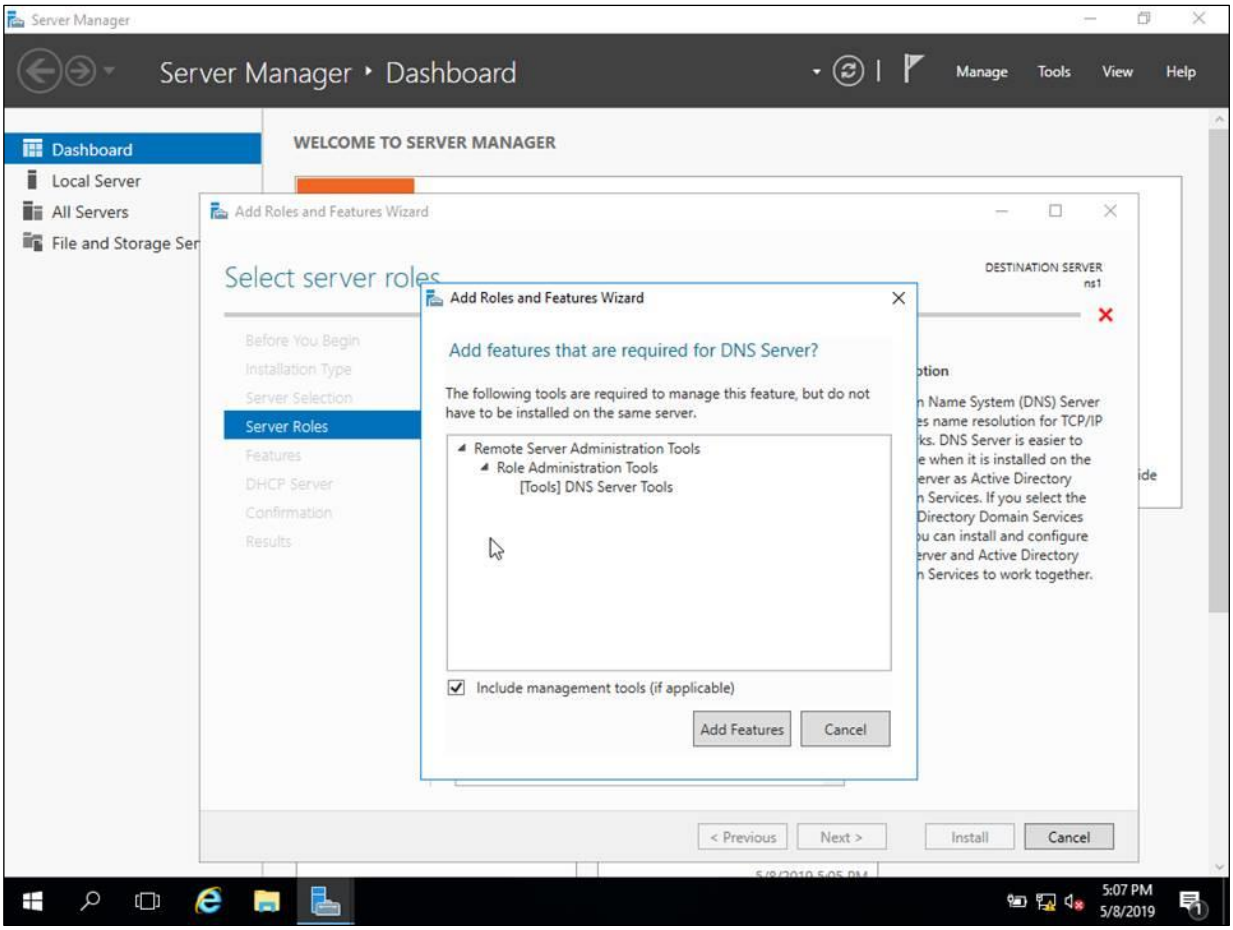

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect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

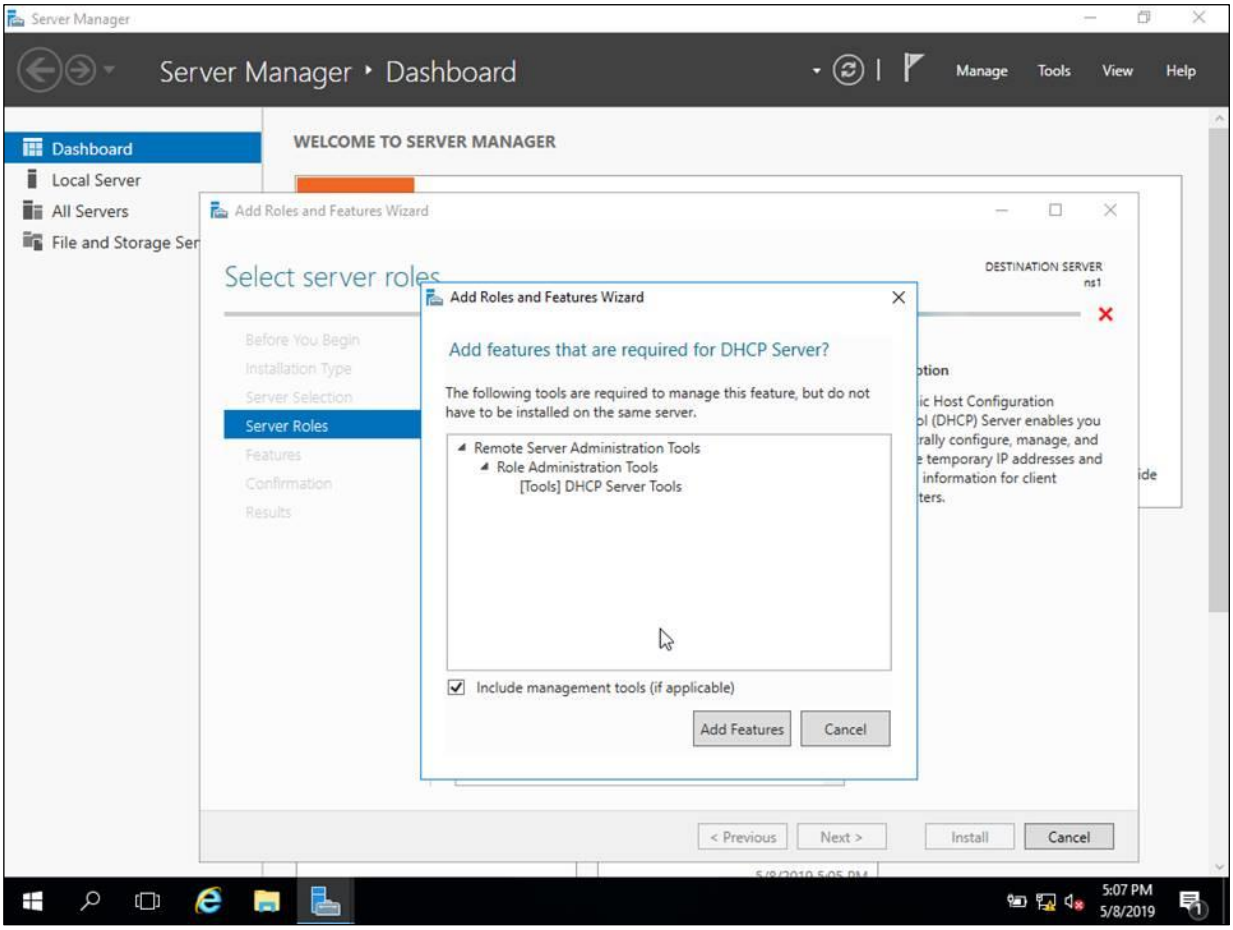

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
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

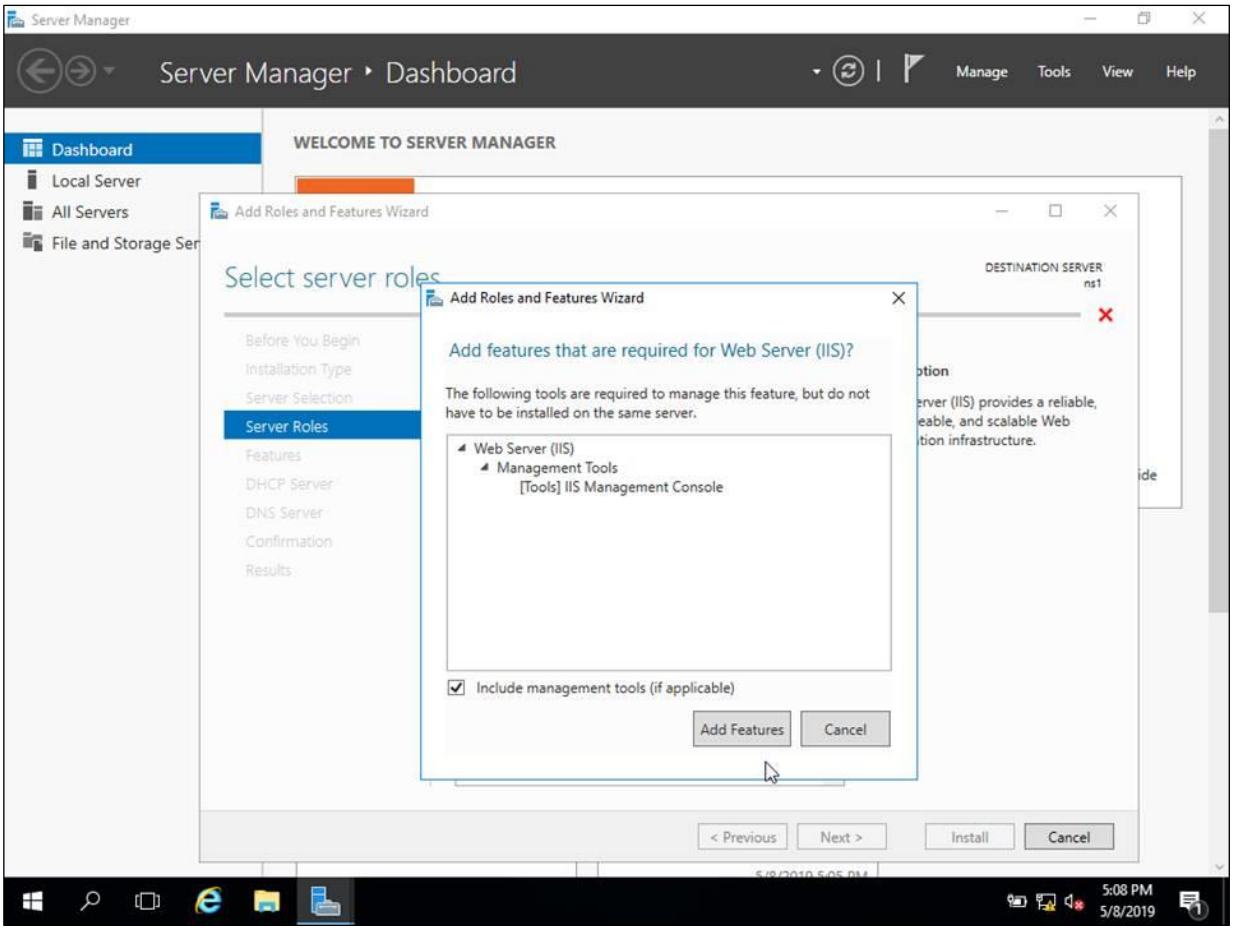

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
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

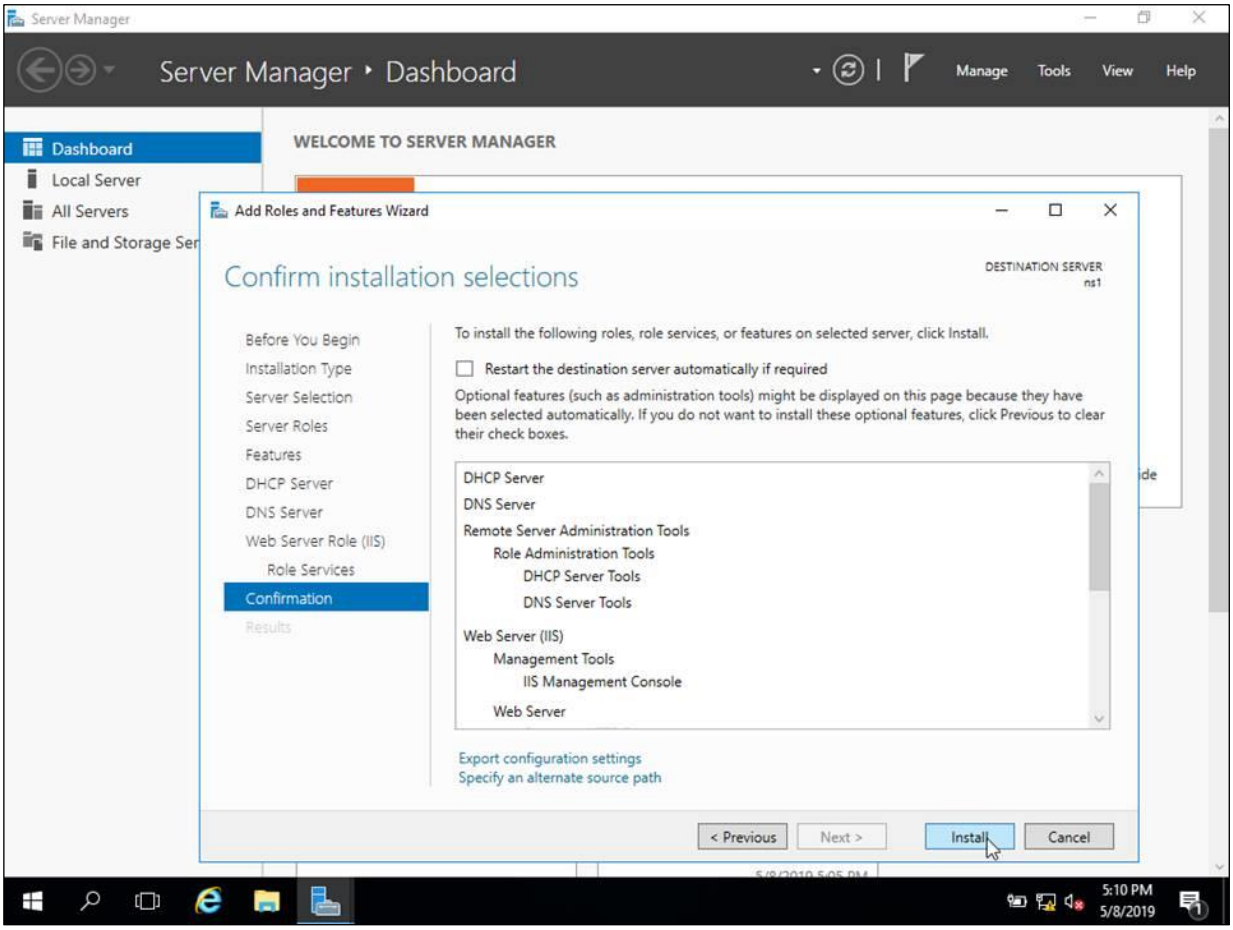

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
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

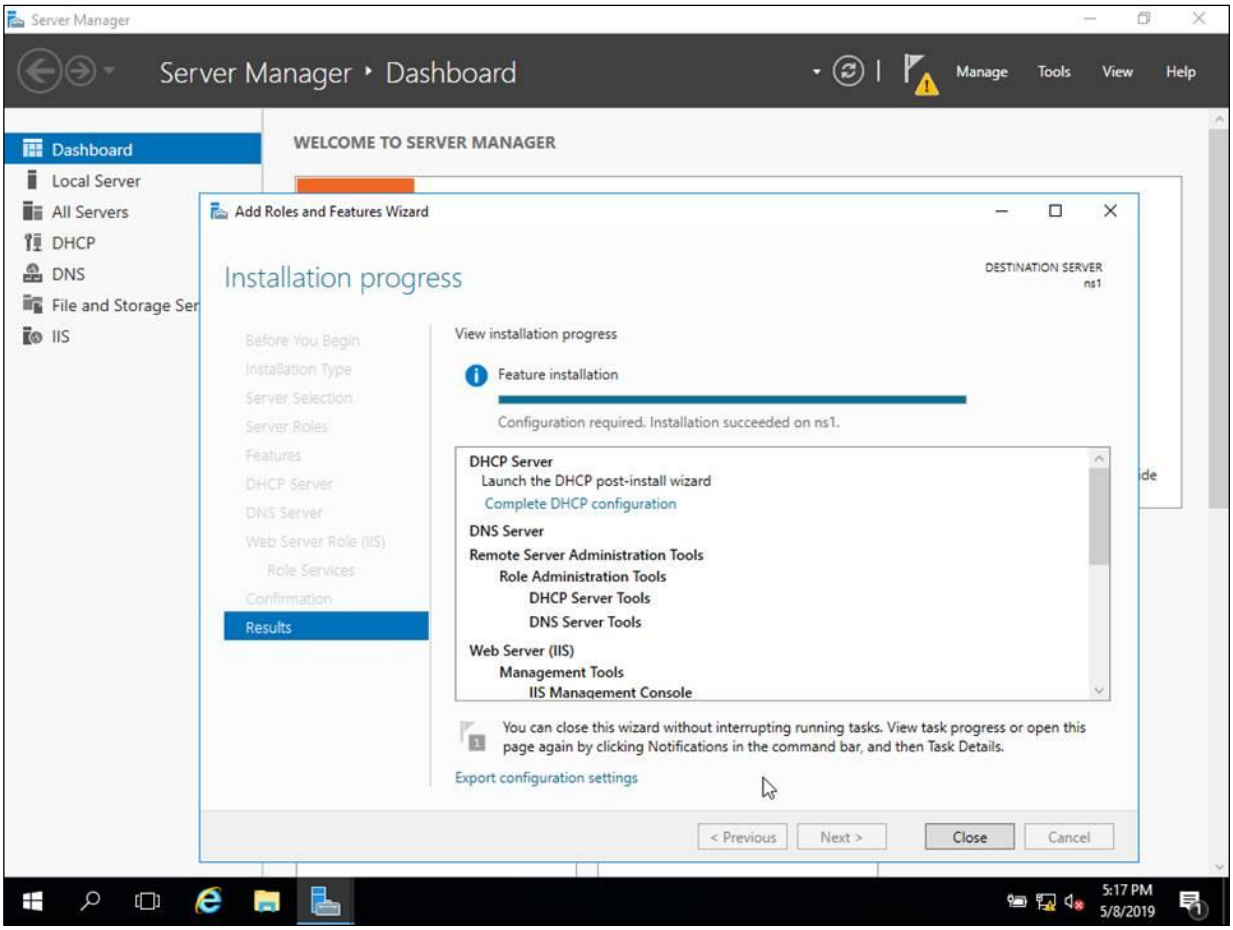

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
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

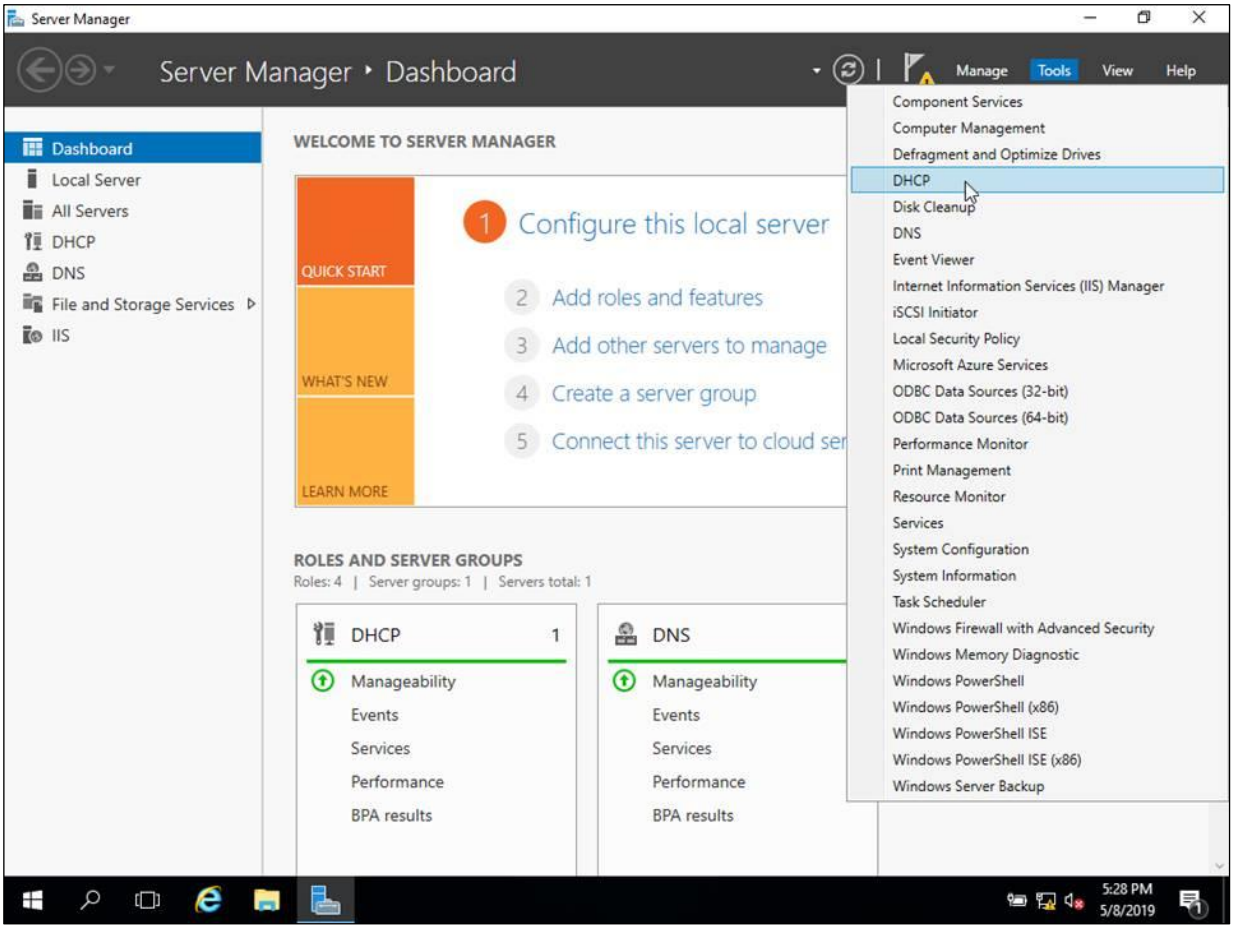

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Add Roles and Features Wizard
Add features that are required for DNS Server?
The 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

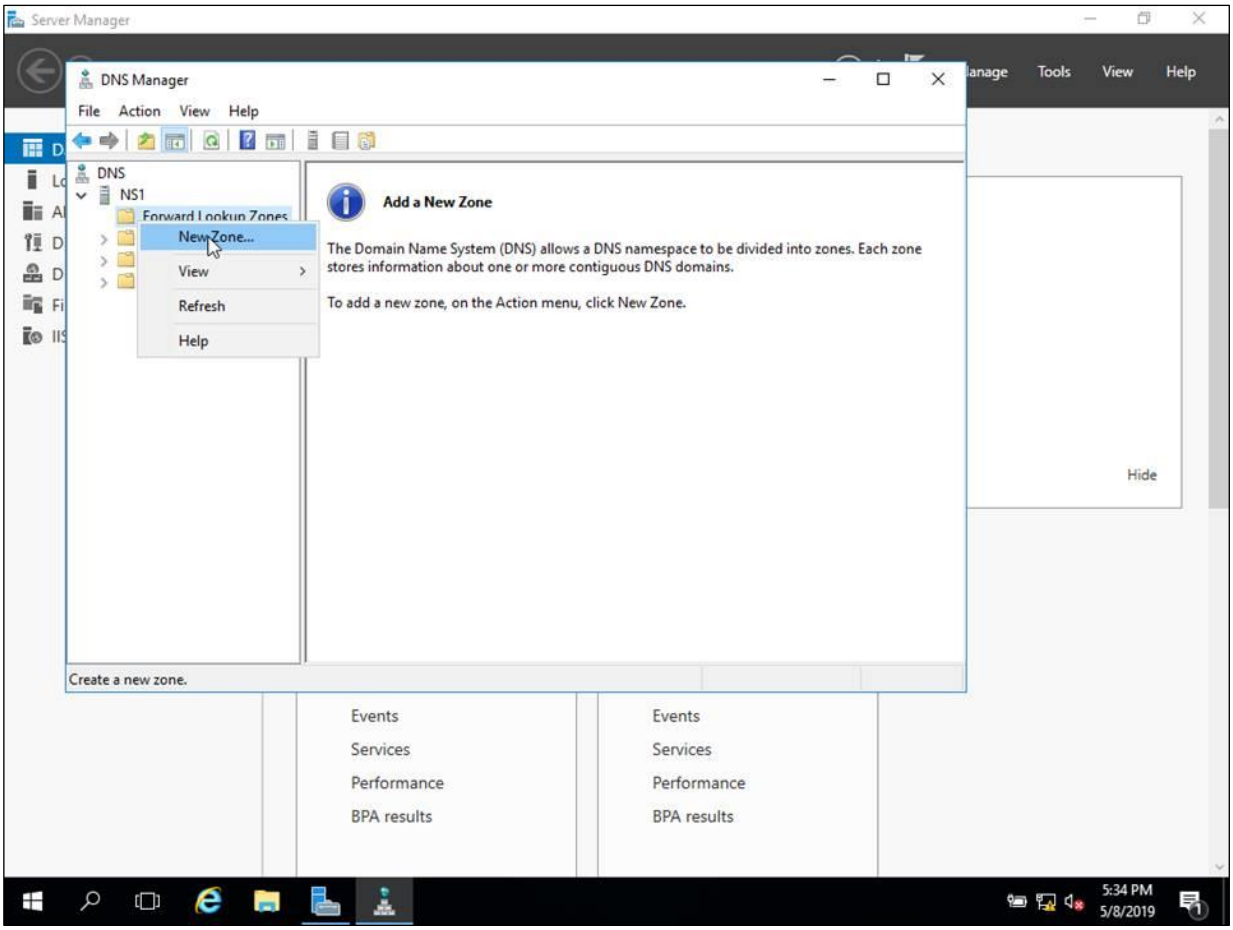

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Add Roles and Features Wizard
Add features that are required for DHCP Server?
The 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
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
< Previous
Next >
Install
Cancel
5:07 PM
5/8/2019

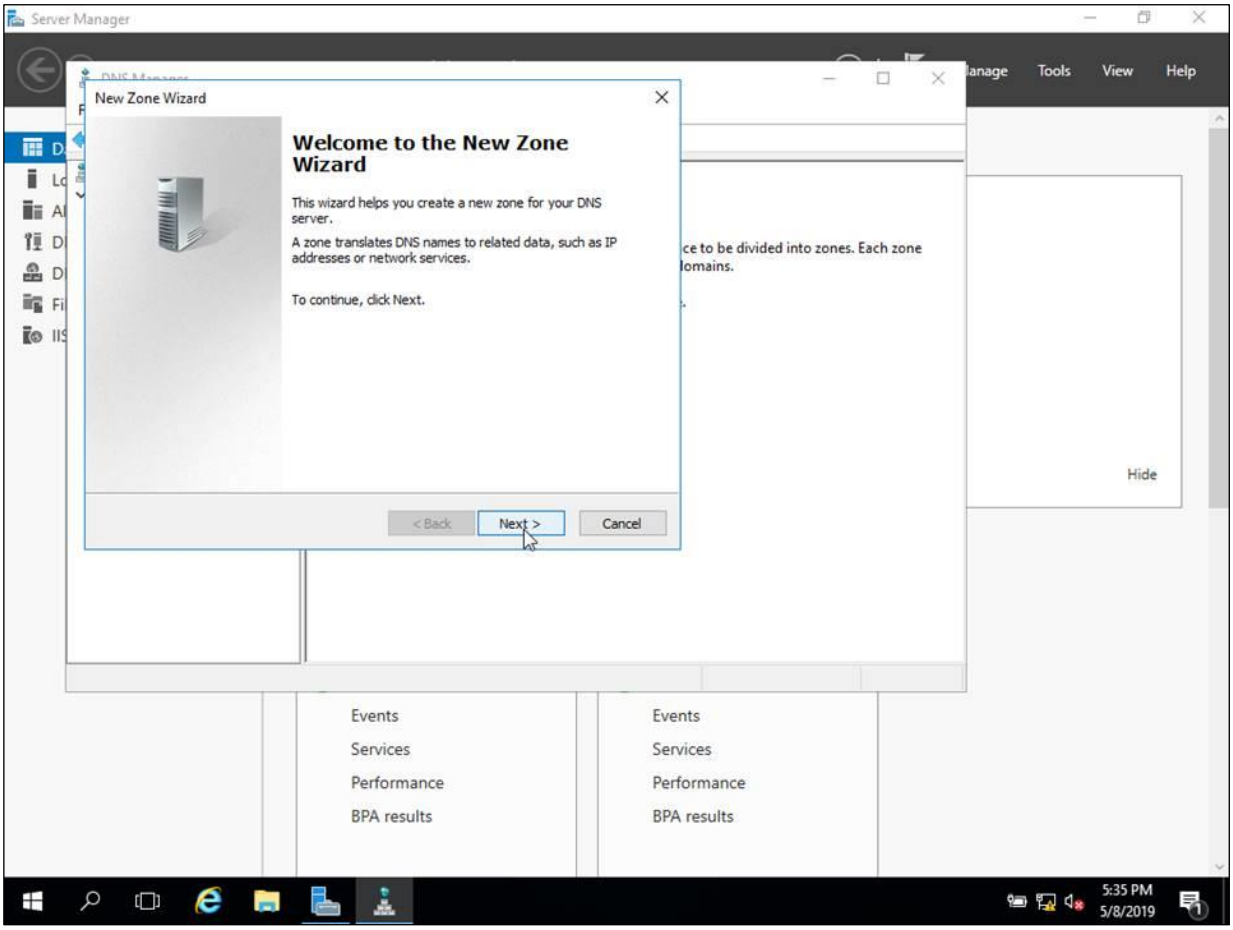

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DHCP Server
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

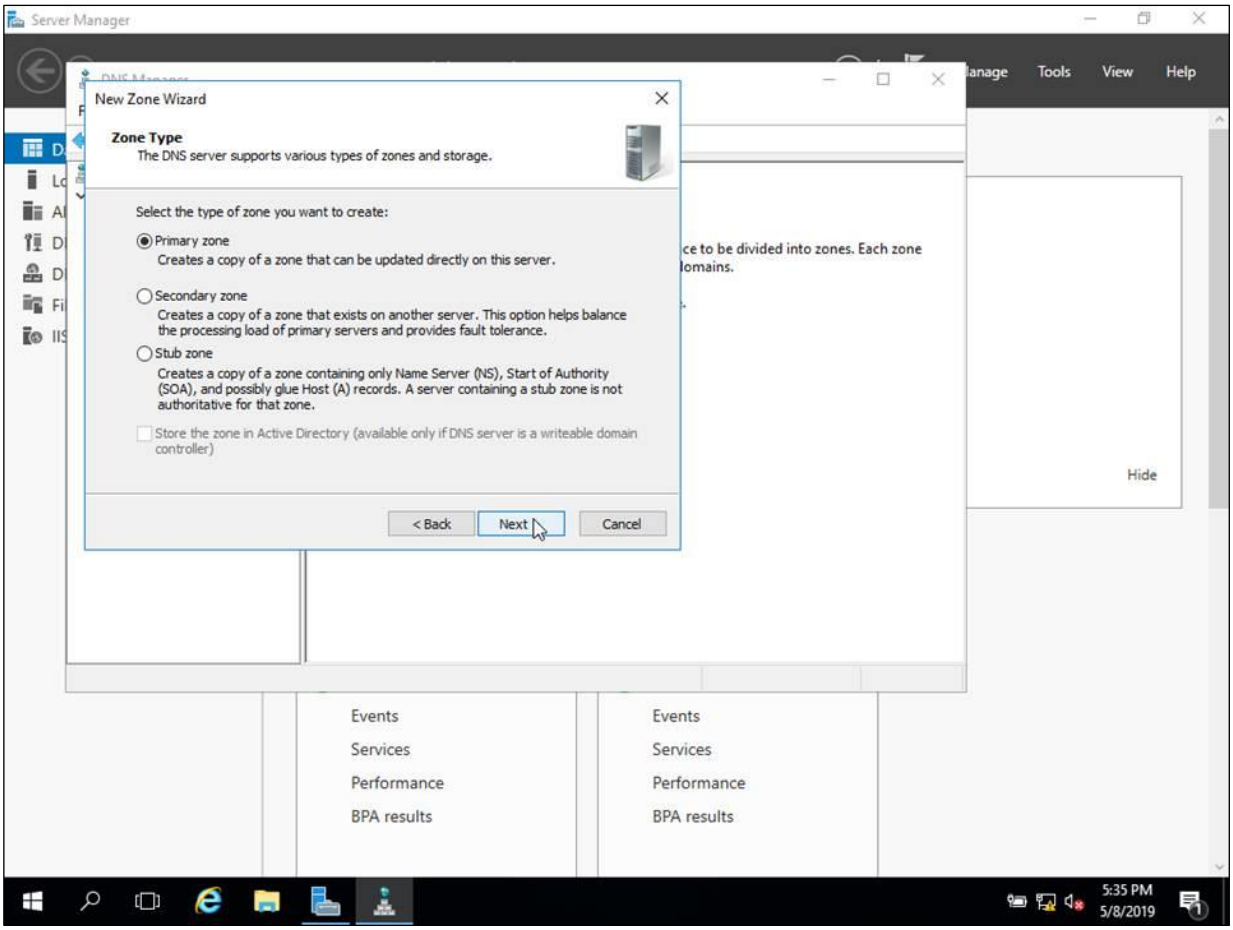

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Ser
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
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

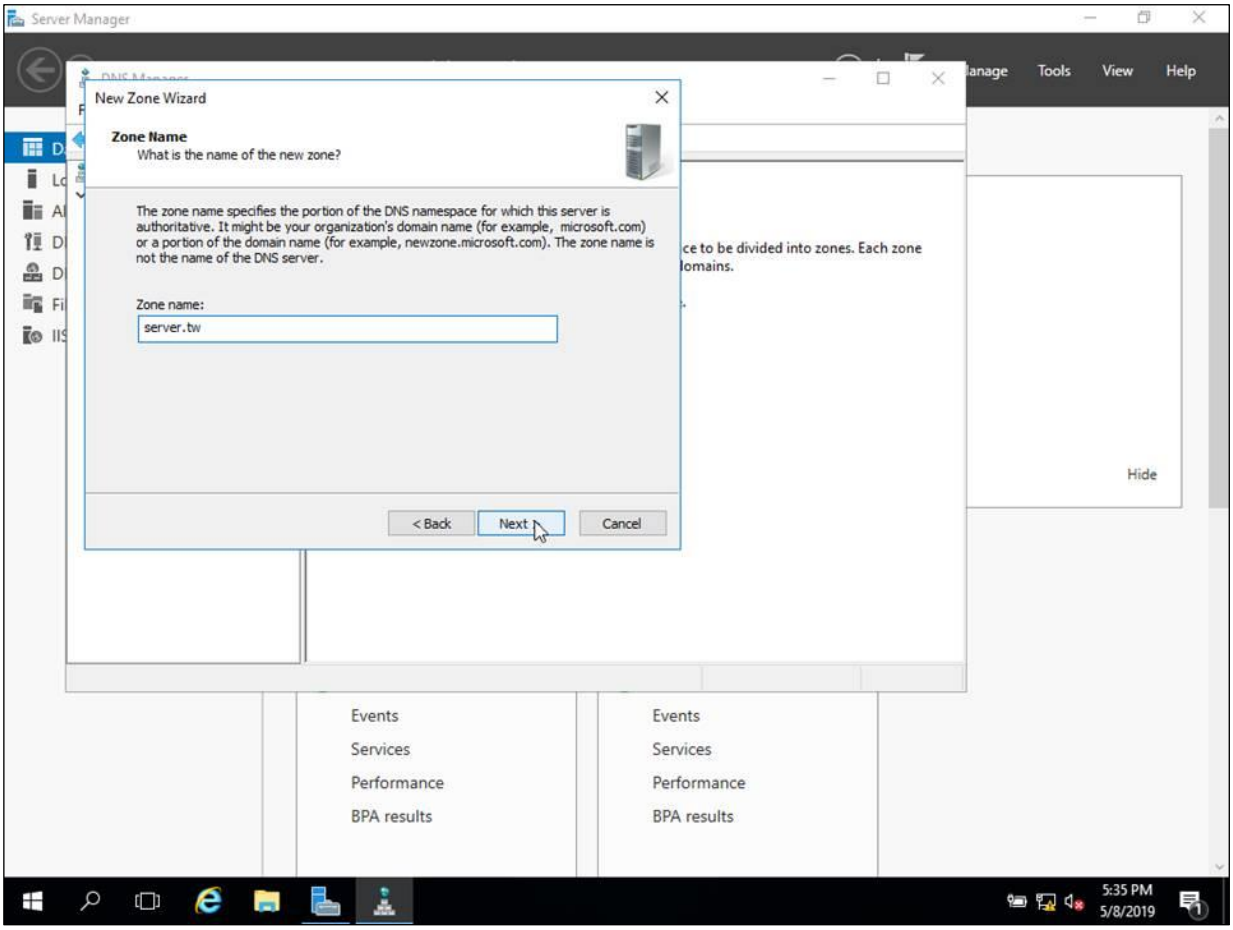

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Ser
IIS
WELCOME TO SERVER MANAGER
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
ns1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
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

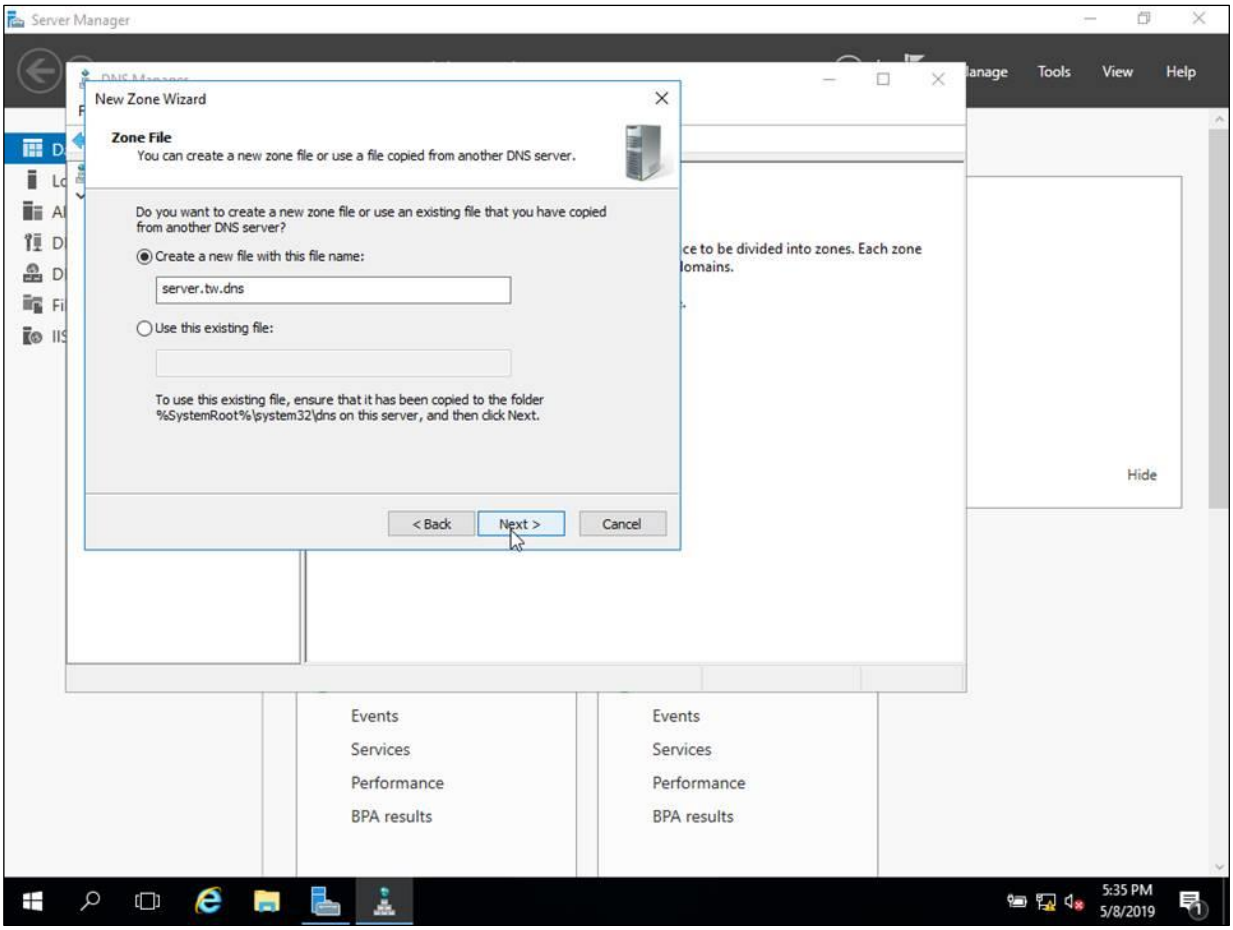

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
DHCP
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server 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

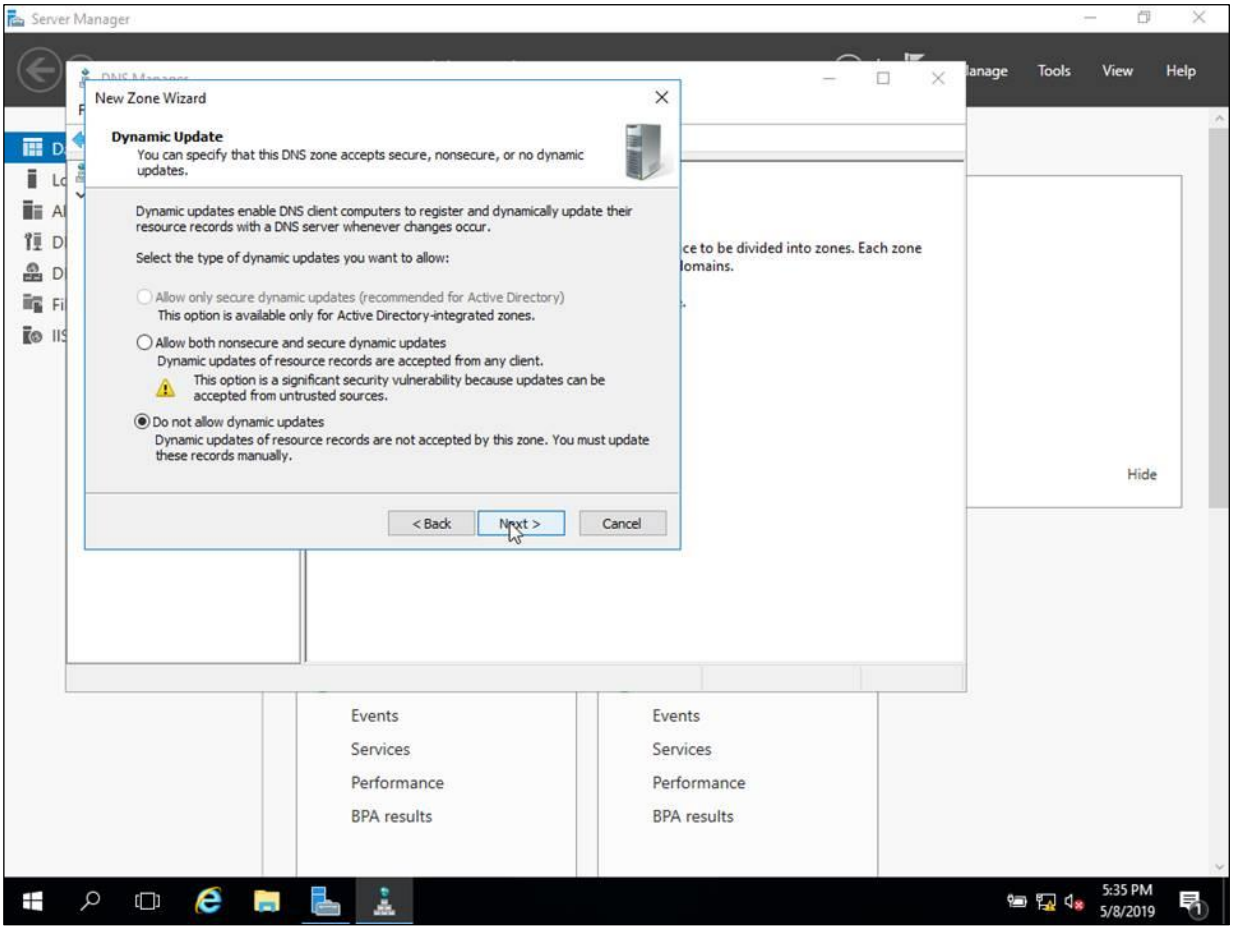

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.
To add a new zone, on the Action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

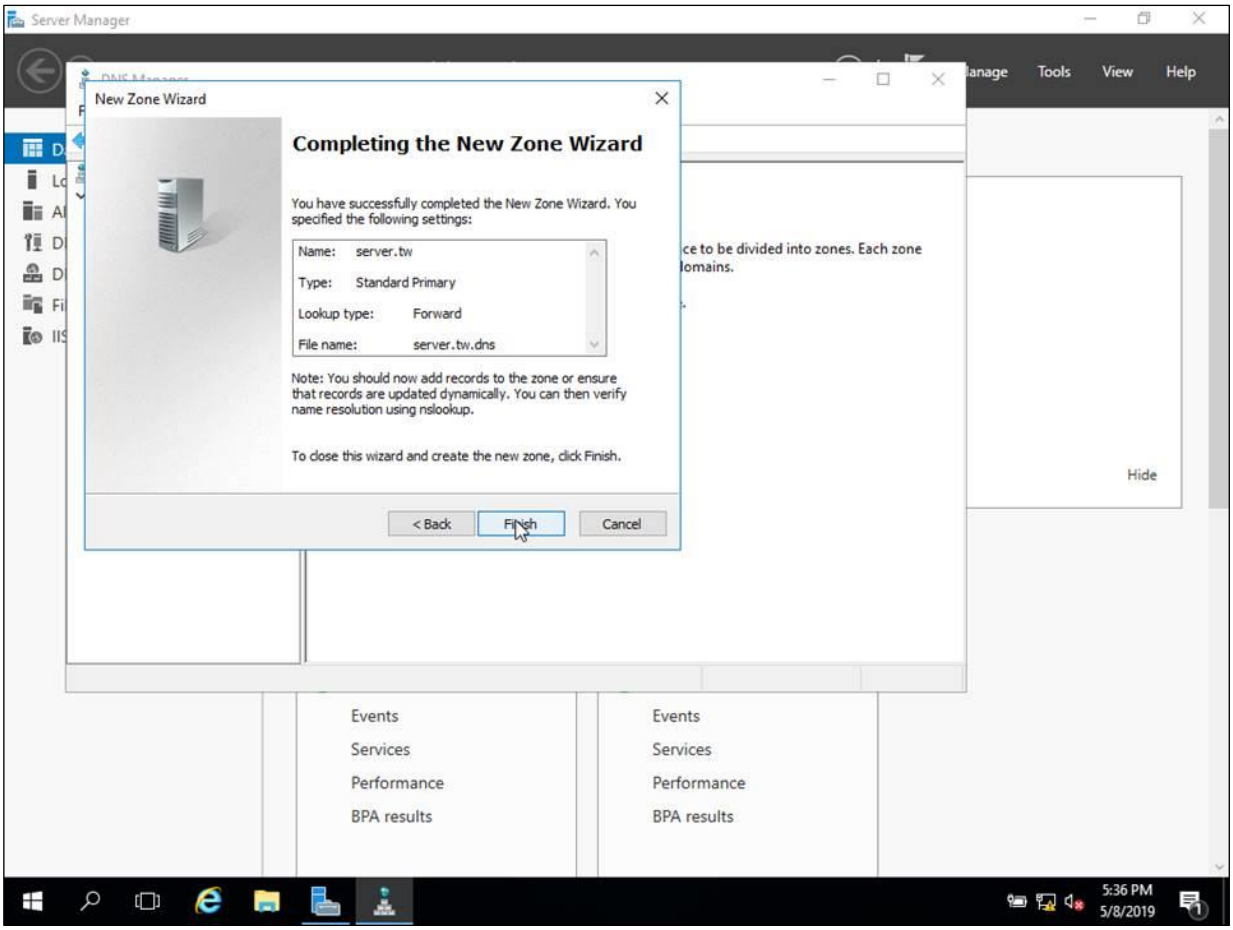

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Manage Tools View Help
Hide
Events
Services
Performance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

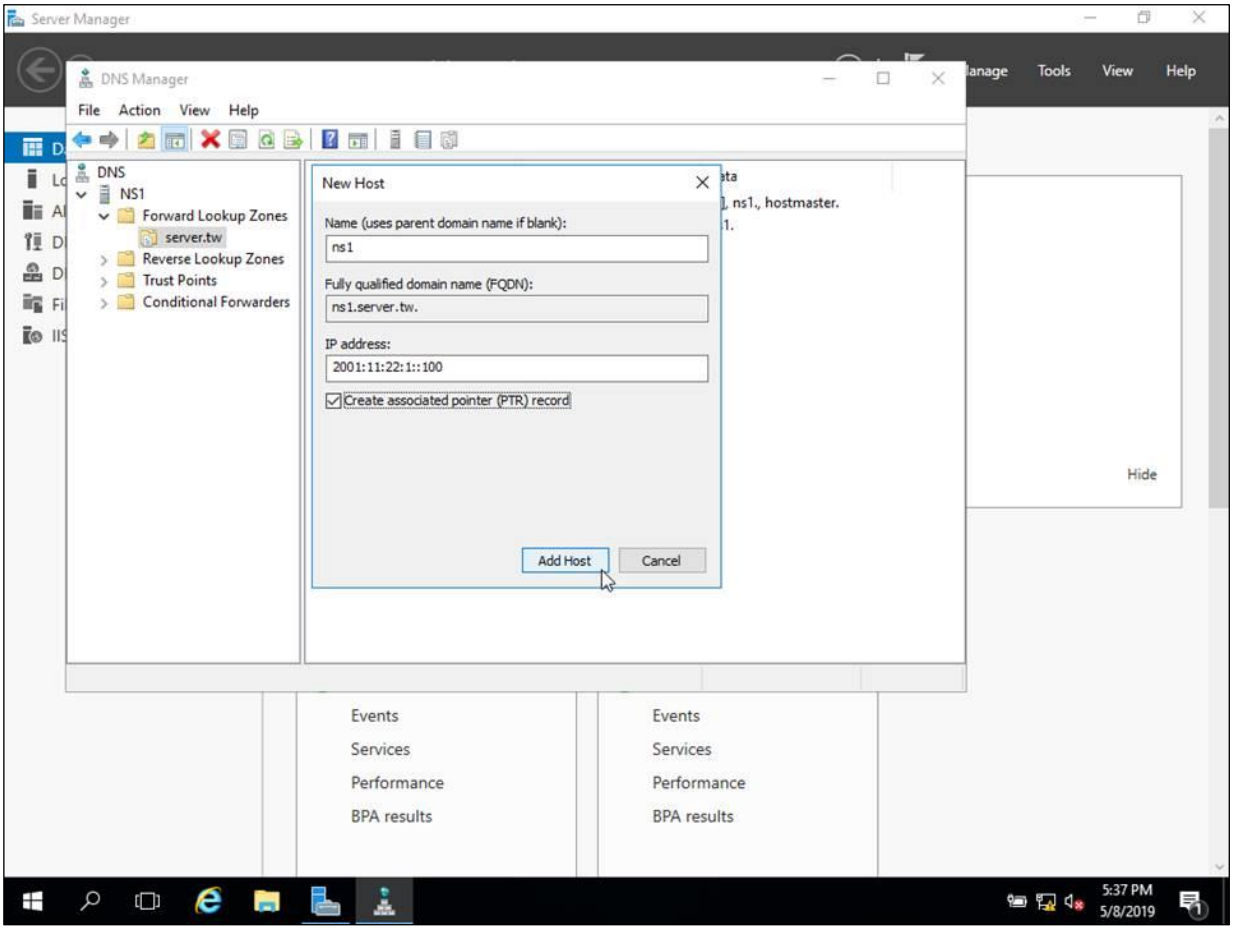

Server Manager
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This 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
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

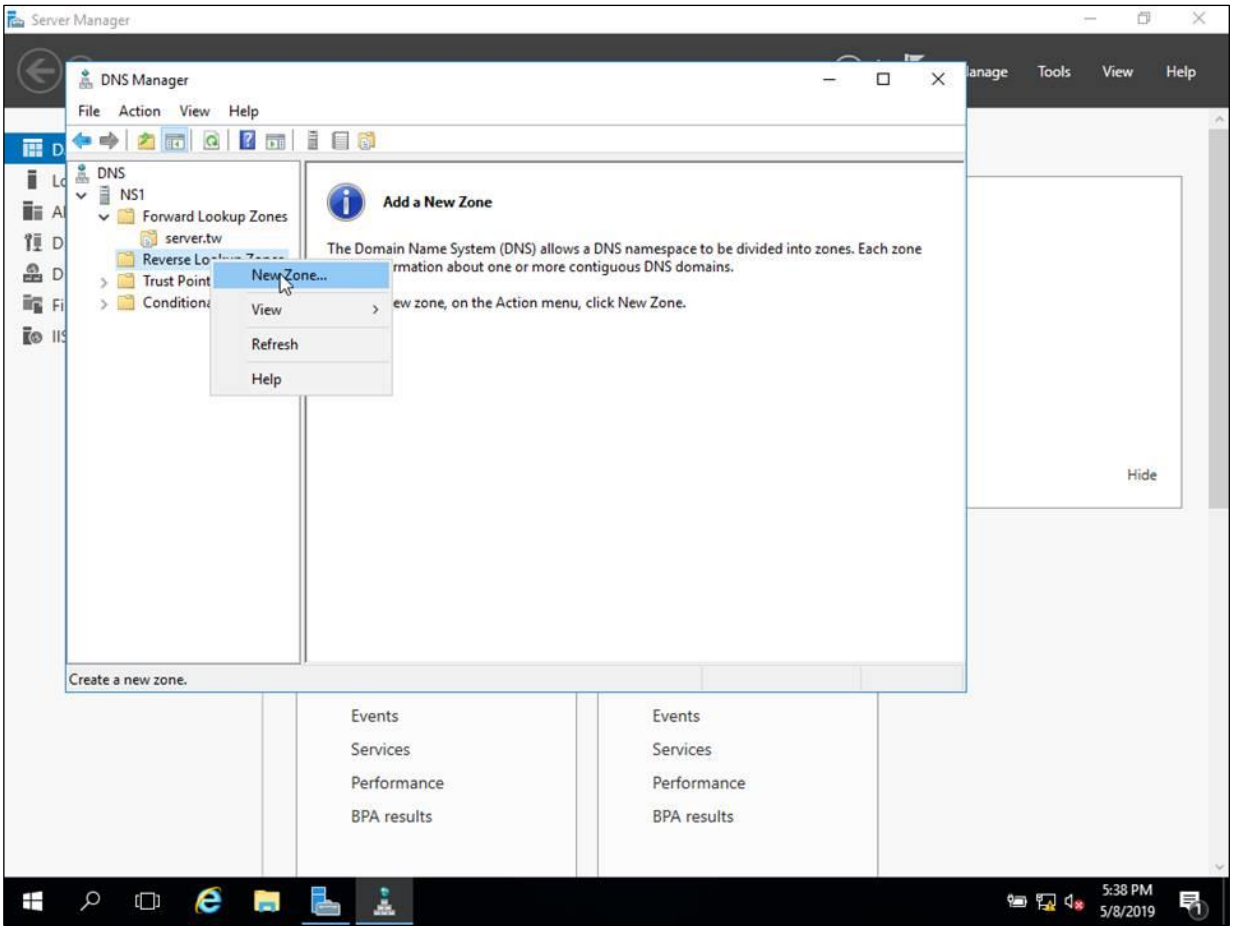

Server Manager
New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com).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

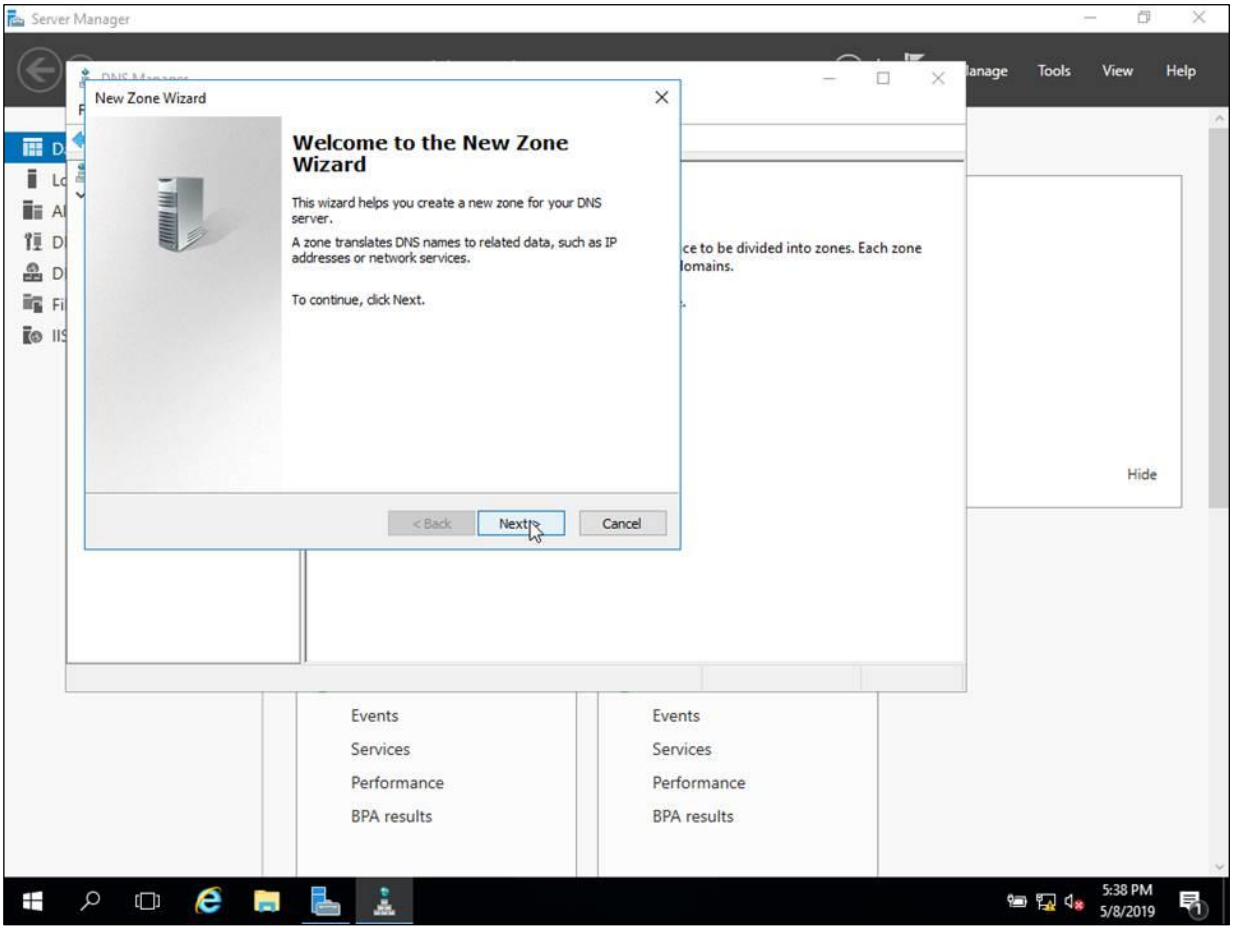

Server Manager
Manage
Tools
View
Help
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
server.tw.dns
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
ce to be divided into zones. Each zone
lomains.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

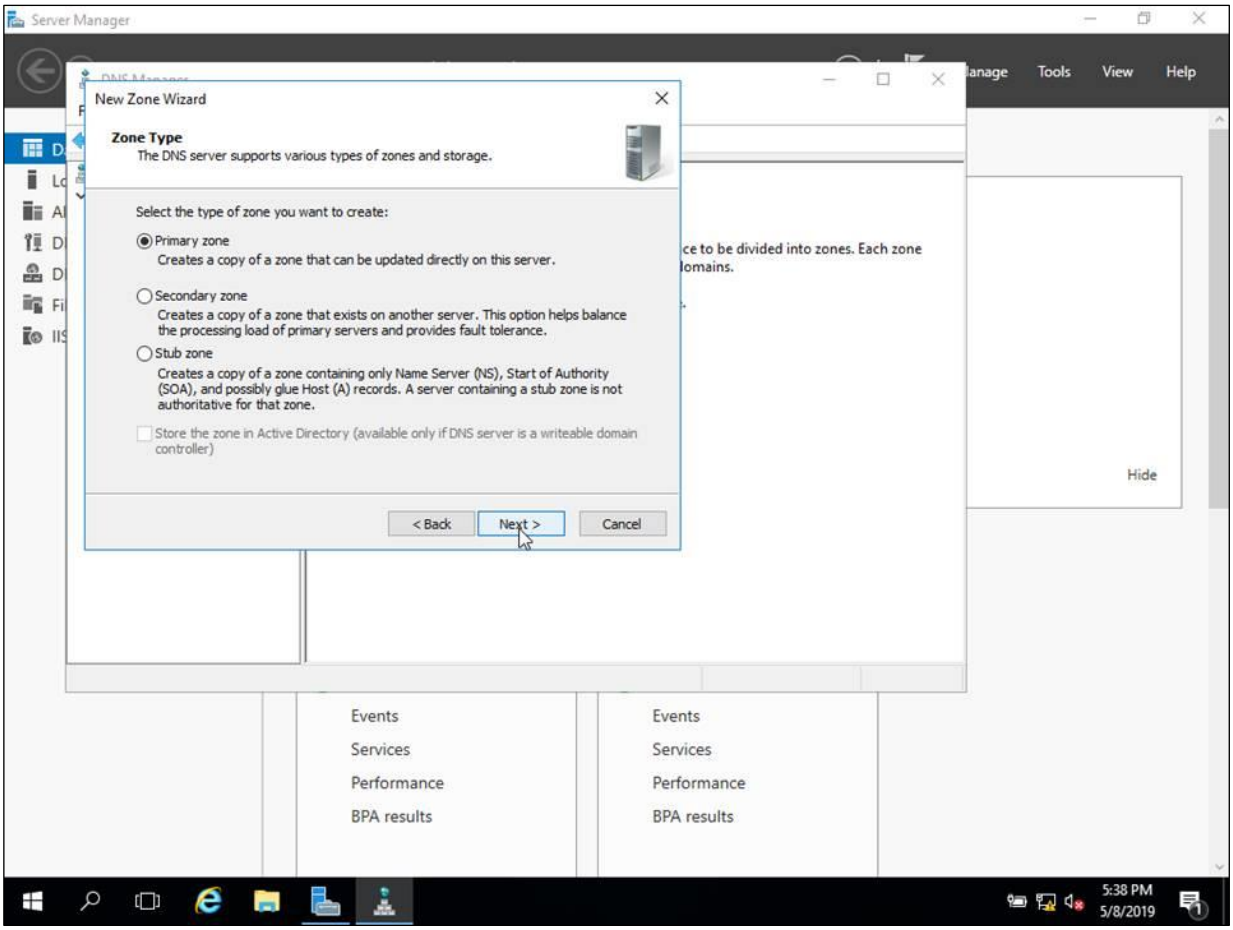

Server Manager
Manage
Tools
View
Help
New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select 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
ce to be divided into zones. Each zone
lomains.
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:35 PM
5/8/2019

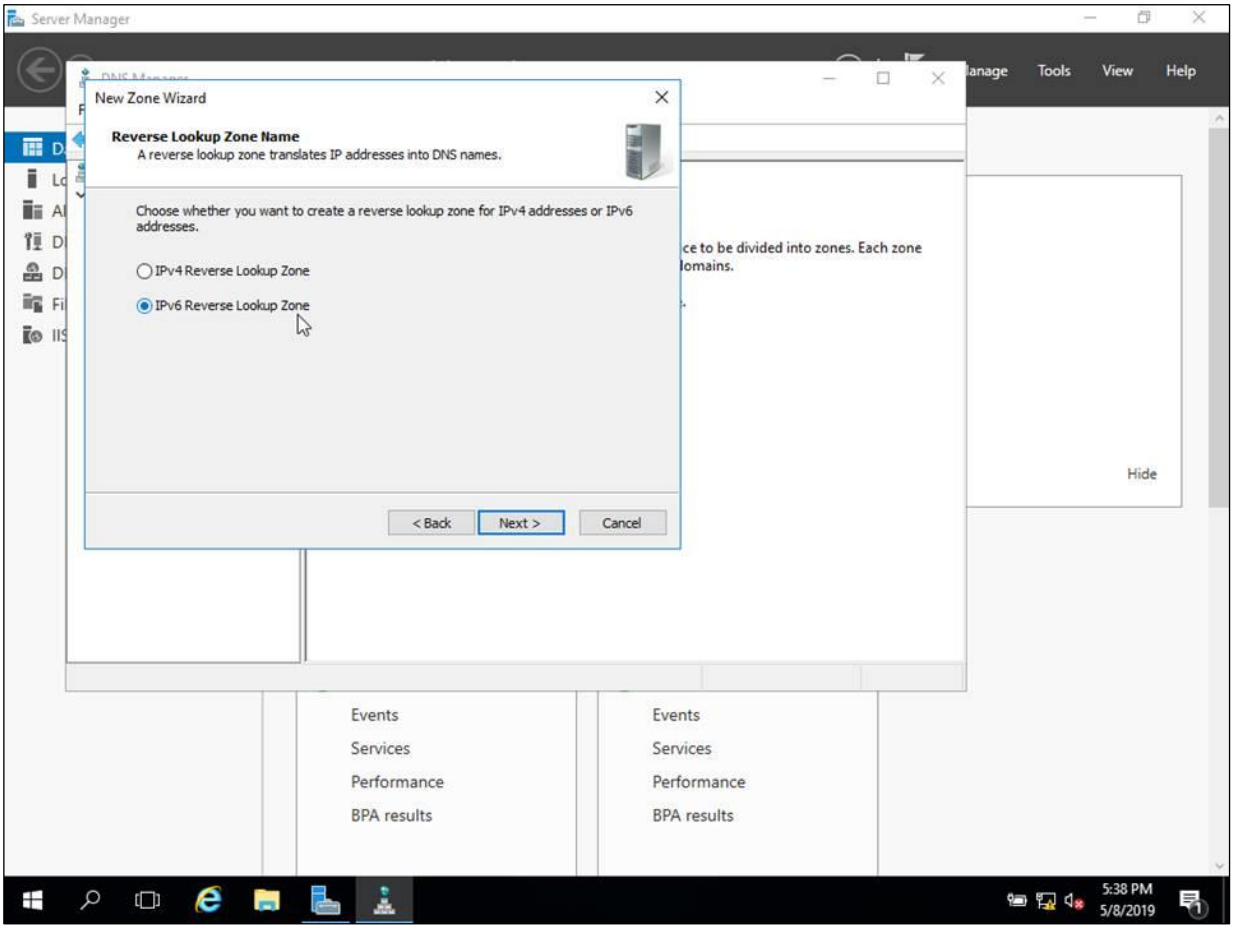

Server Manager
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name: server.tw
Type: Standard Primary
Lookup type: Forward
File name: server.tw.dns
Note: You should now add records to the zone or ensure that records 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
Manage
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:36 PM
5/8/2019

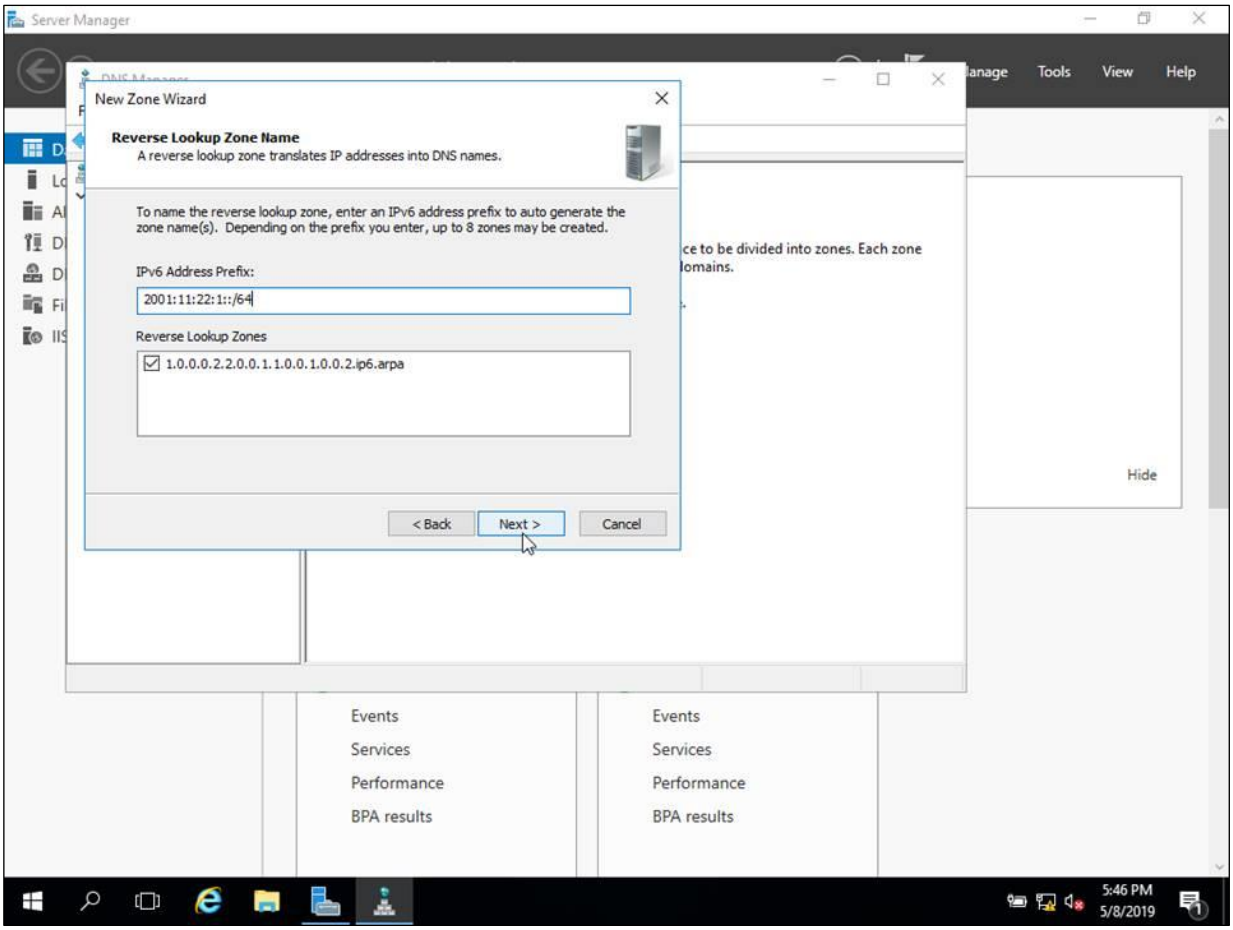

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
Trust Points
Conditional Forwarders
New Host
Name (uses parent domain name if blank):
ns1
Fully qualified domain name (FQDN):
ns1.server.tw.
IP address:
2001:11:22:1::100
Create associated pointer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

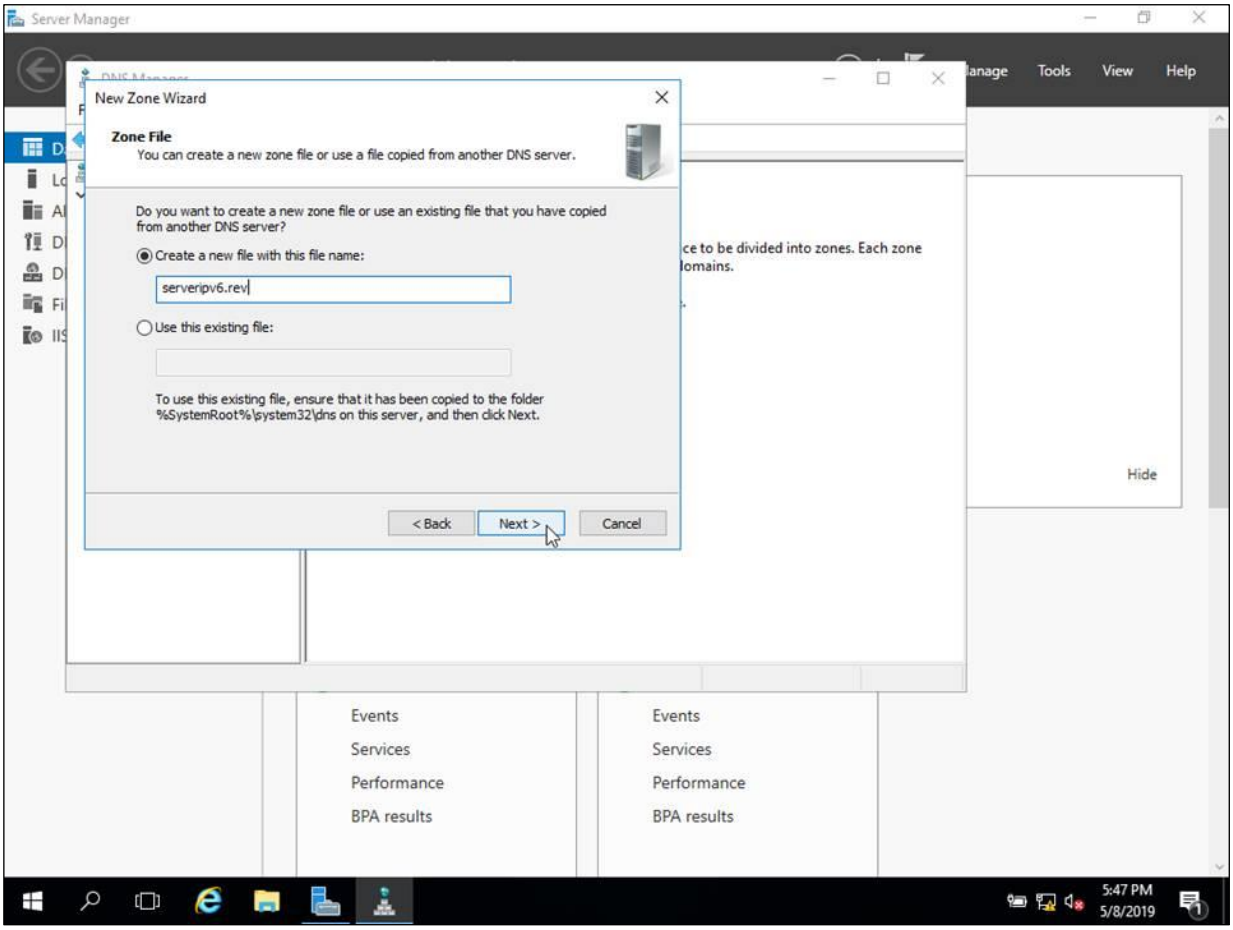

Server Manager
DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lo
Trust Point
Conditiona
New Zone...
View
Refresh
Help
Add a New Zone
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone
rmation about one or more contiguous DNS domains.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

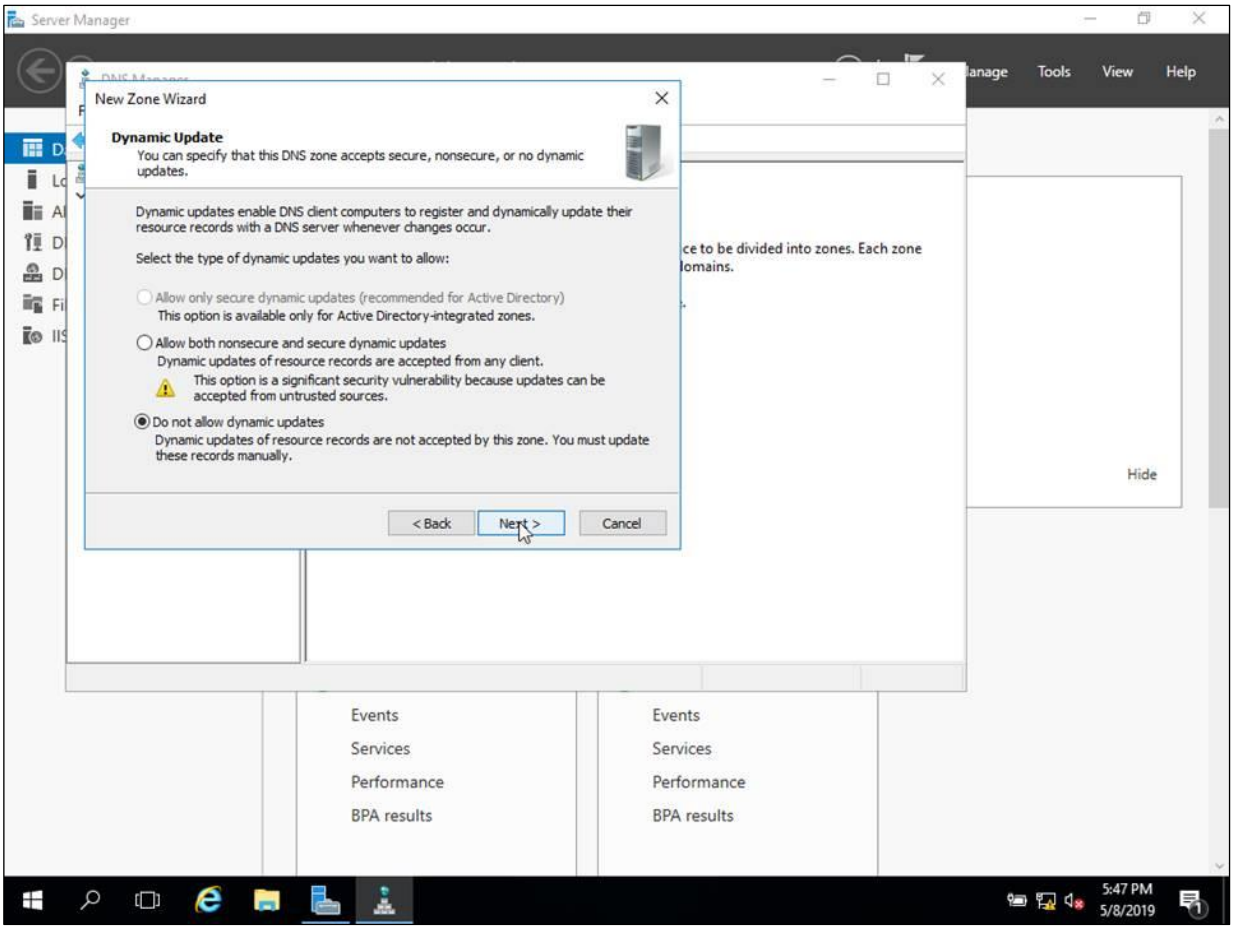

Server Manager
New Zone Wizard
Welcome to the New Zone Wizard
This wizard helps you create a new zone for your DNS server.
A zone translates DNS names to related data, such as IP addresses or network services.
To continue, click Next.
< Back
Next >
Cancel
Tools View Help
Hide
Events
Services
Performance
BPA results
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

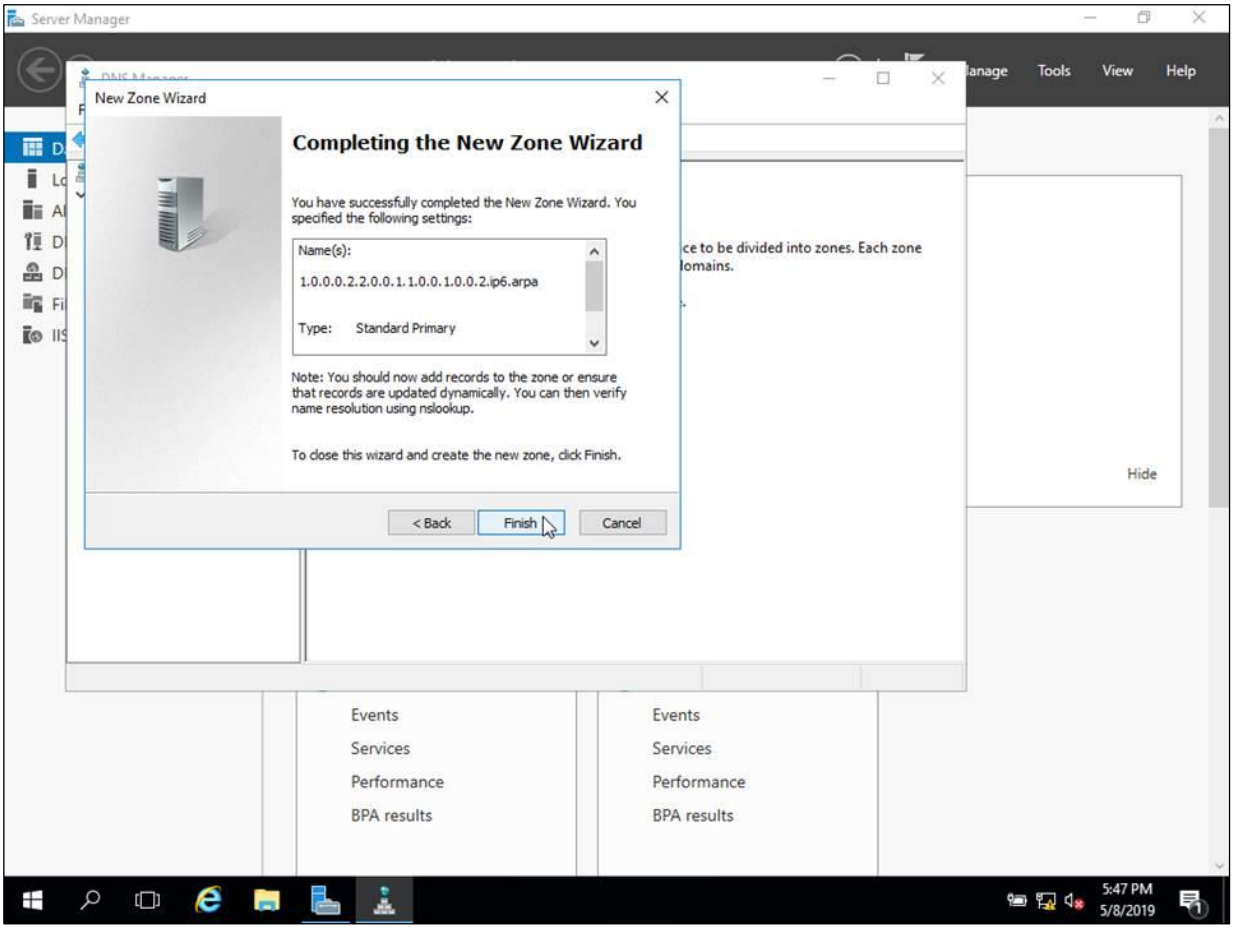

Server Manager
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This 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
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:38 PM
5/8/2019

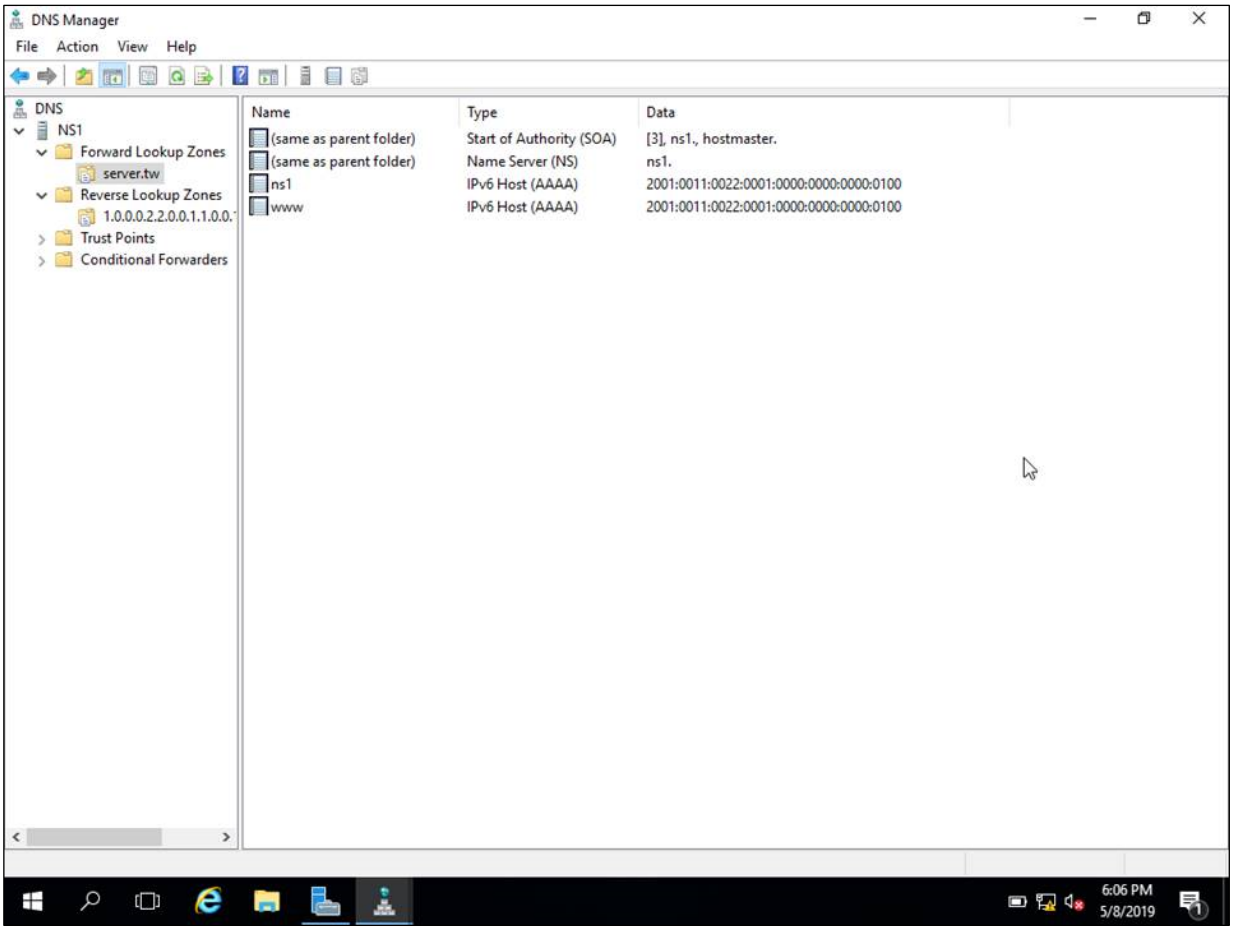

Server Manager
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.
IPv4 Reverse Lookup Zone
IPv6 Reverse Lookup Zone
< Back
Next >
Cancel
Tools
View
Help
Hide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

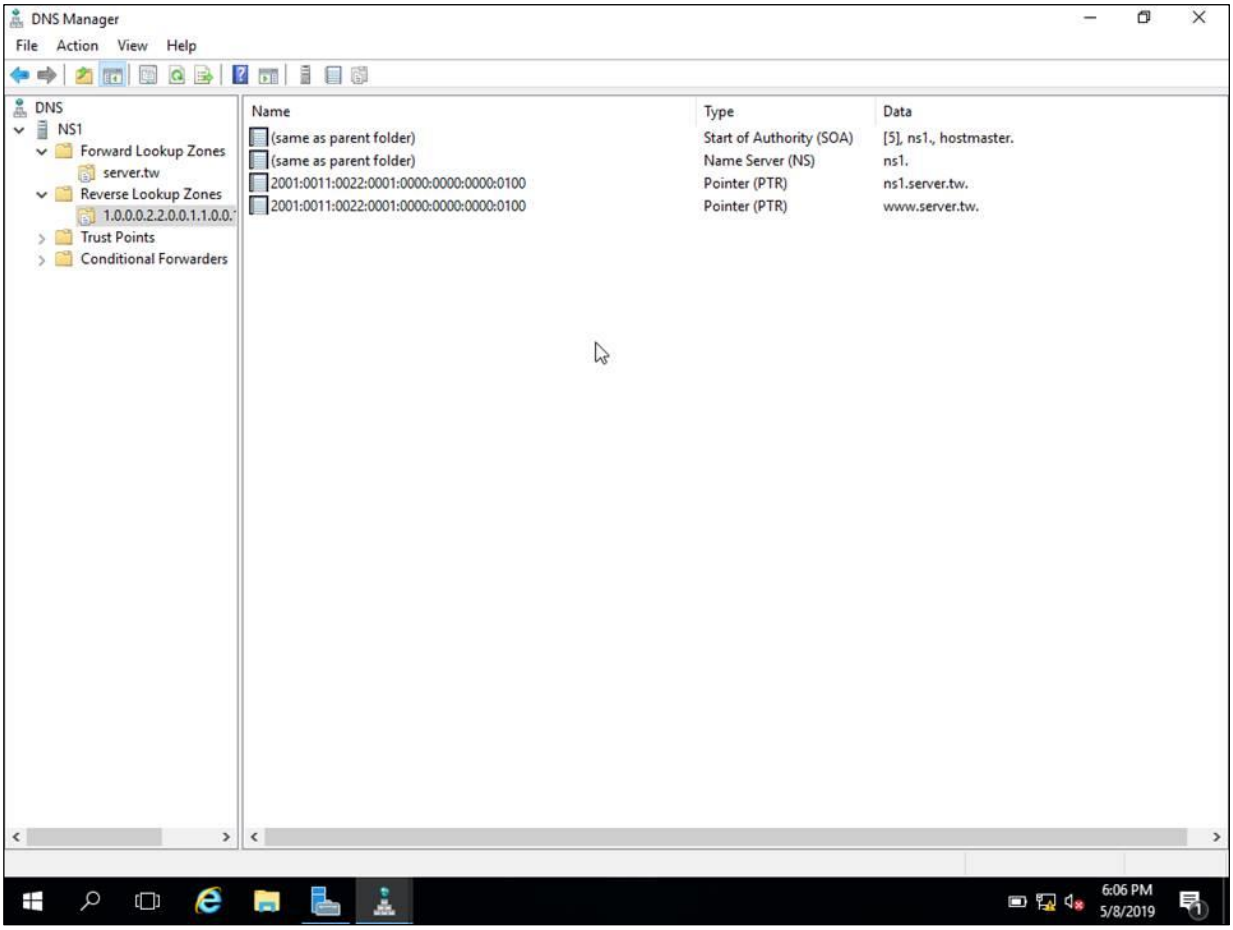

Server Manager
New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.
IPv6 Address Prefix: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

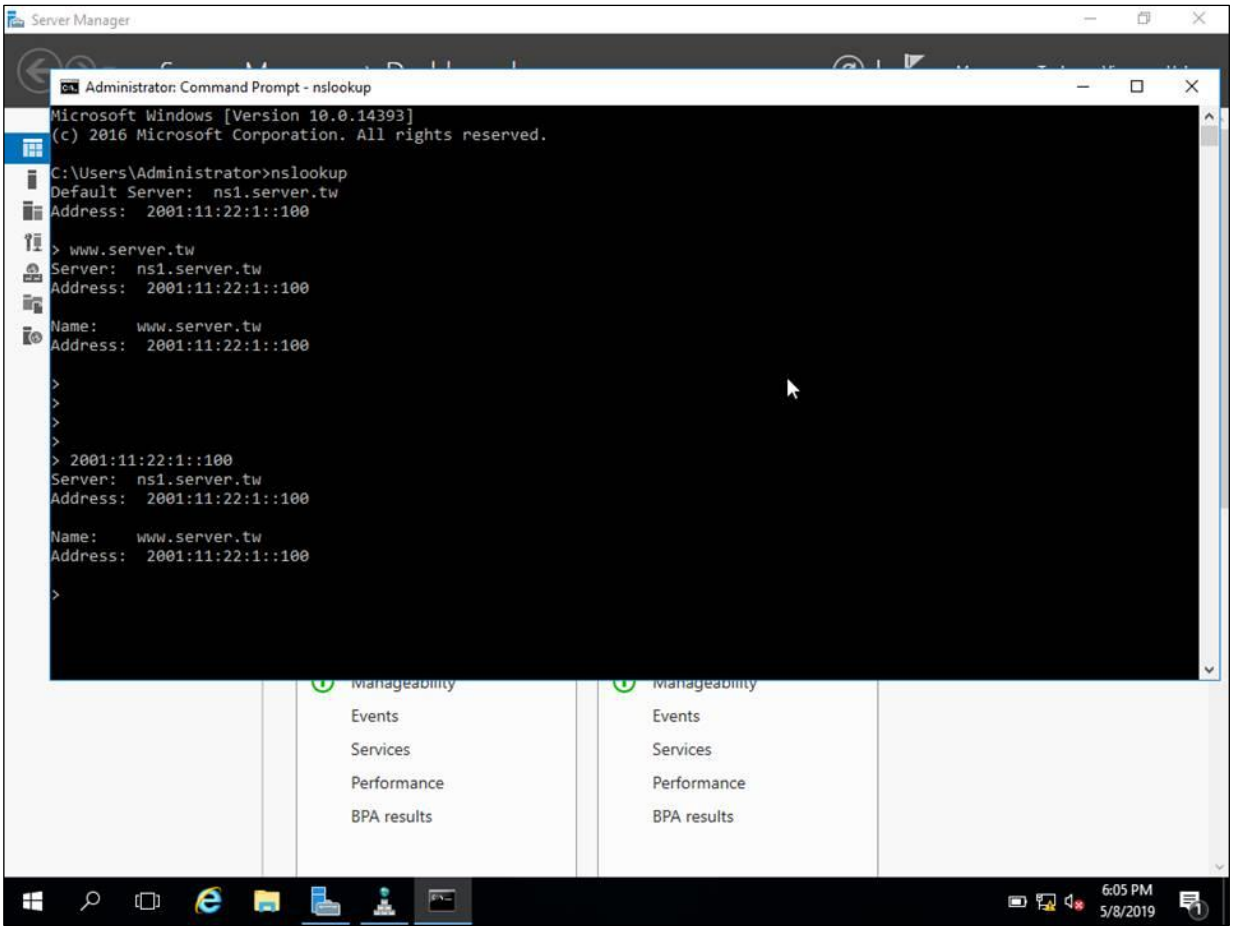

Server Manager
New Zone Wizard
Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?
Create a new file with this file name:
serveripv6.rev
Use this existing file:
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
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:47 PM
5/8/2019


Server Manager
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
Tools
View
Help
Hide
Events
Services
Performance
BPA results
5:47 PM
5/8/2019

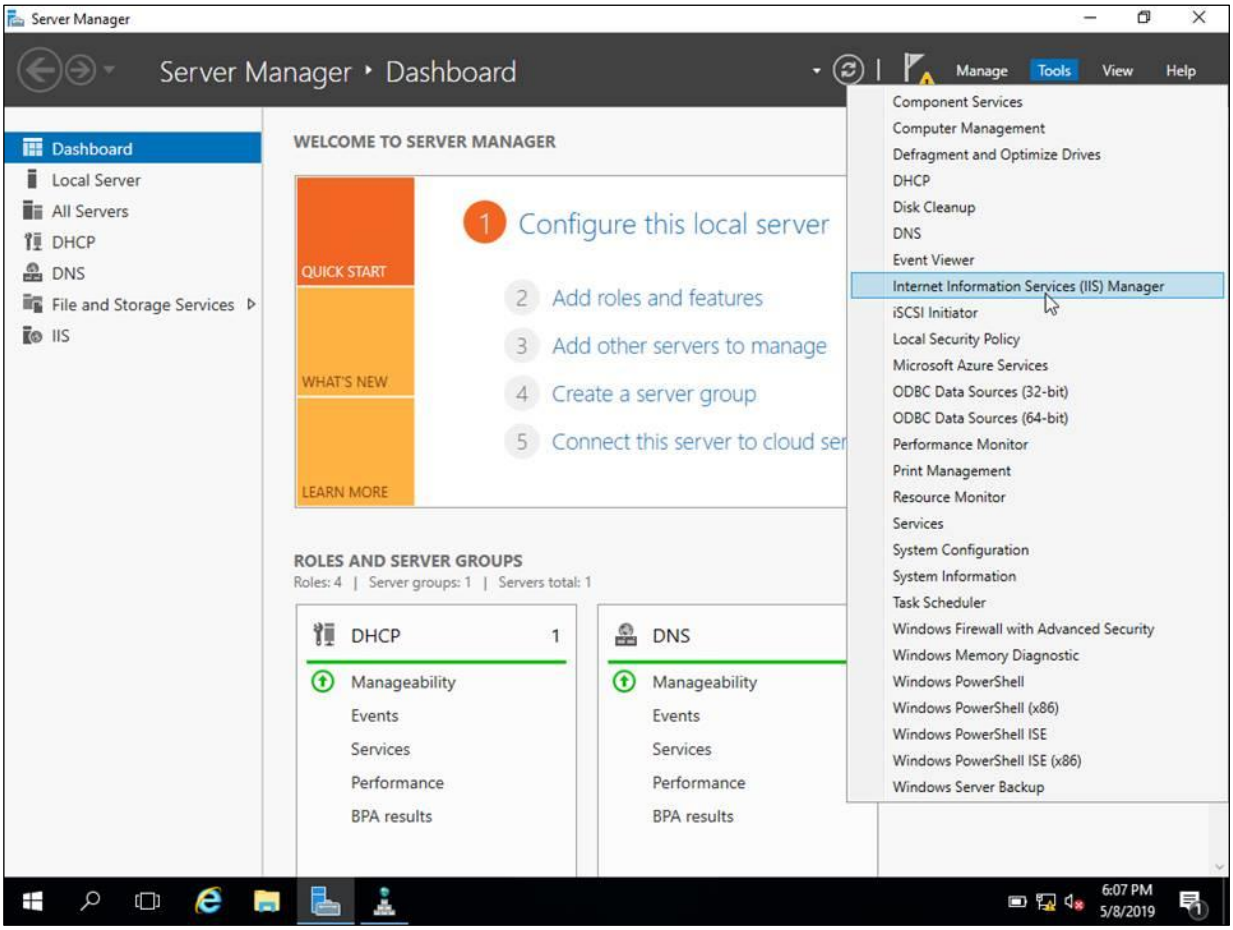

Server Manager
New Zone Wizard
Completing the New Zone Wizard
You have successfully completed the New Zone Wizard. You specified the following settings:
Name(s):
1.0.0.0.2.2.0.0.1.1.0.0.1.0.0.2.ip6.arpa
Type: Standard Primary
Note: You should now add records to the zone or ensure that records are updated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

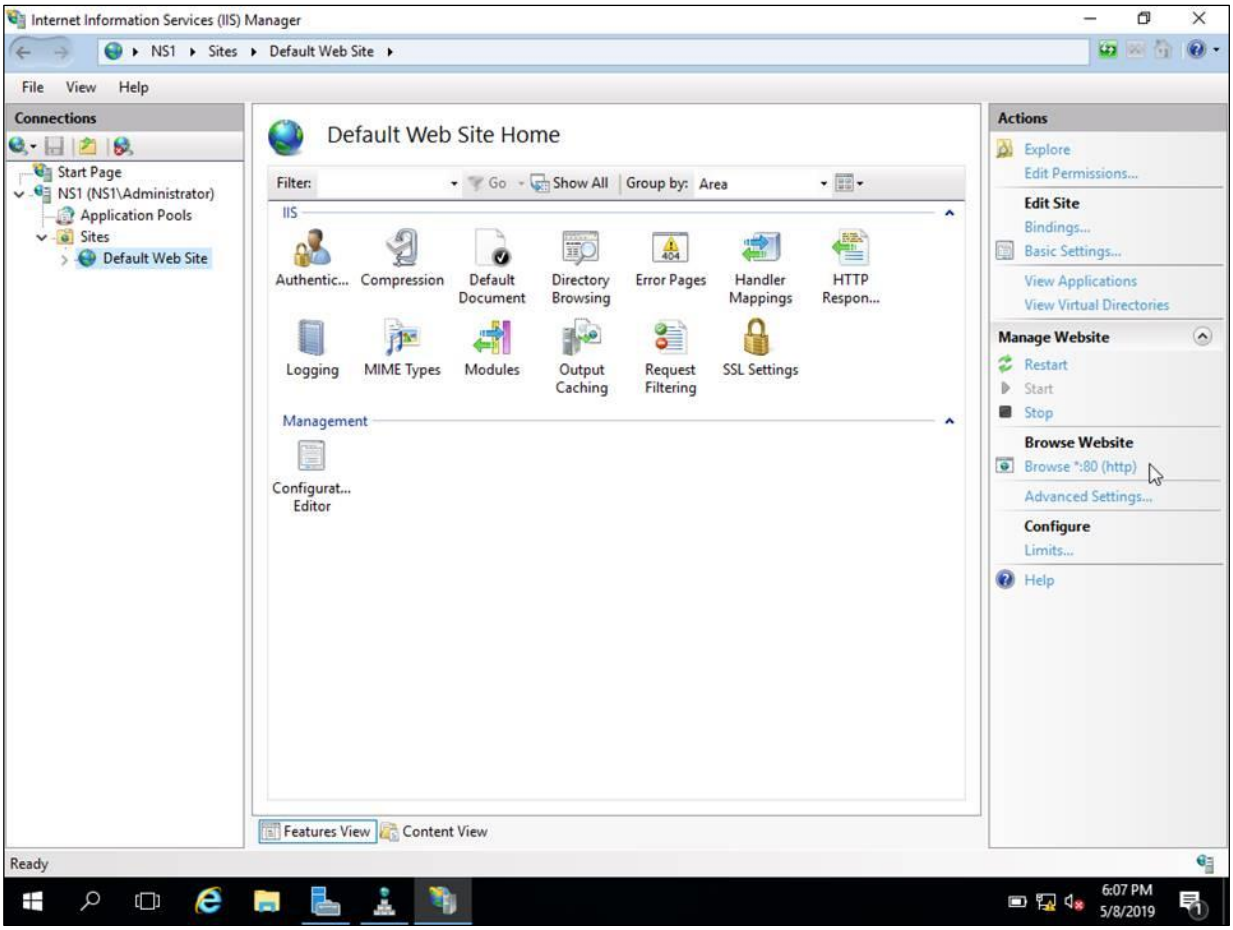

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[3], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
ns1
IPv6 Host (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

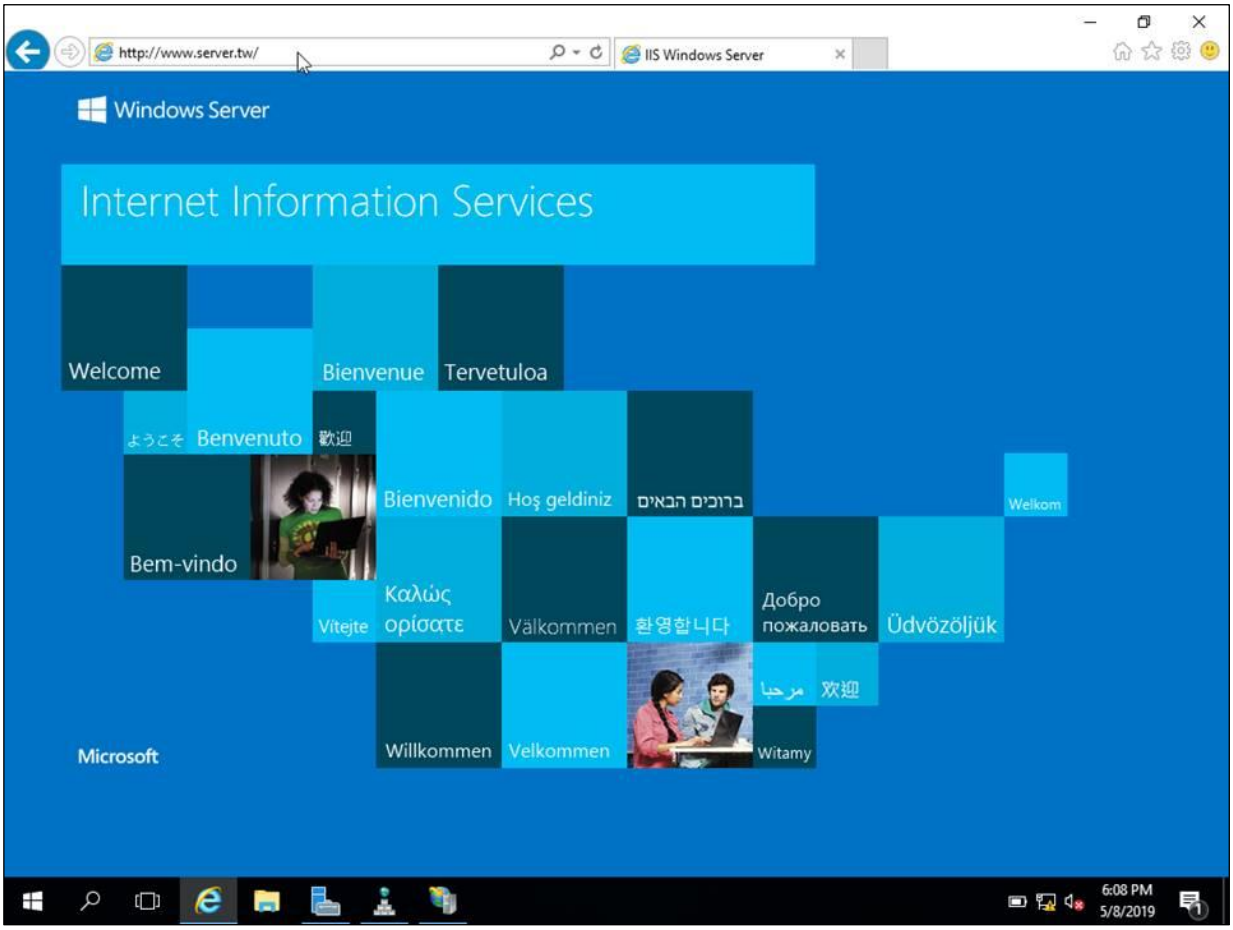

DNS Manager
File Action View Help
DNS
NS1
Forward Lookup Zones
server.tw
Reverse Lookup Zones
1.0.0.0.2.2.0.0.1.1.0.0.
Trust Points
Conditional Forwarders
Name
Type
Data
(same as parent folder)
Start of Authority (SOA)
[5], ns1., hostmaster.
(same as parent folder)
Name Server (NS)
ns1.
2001:0011:0022:0001:0000:0000:0000:0100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

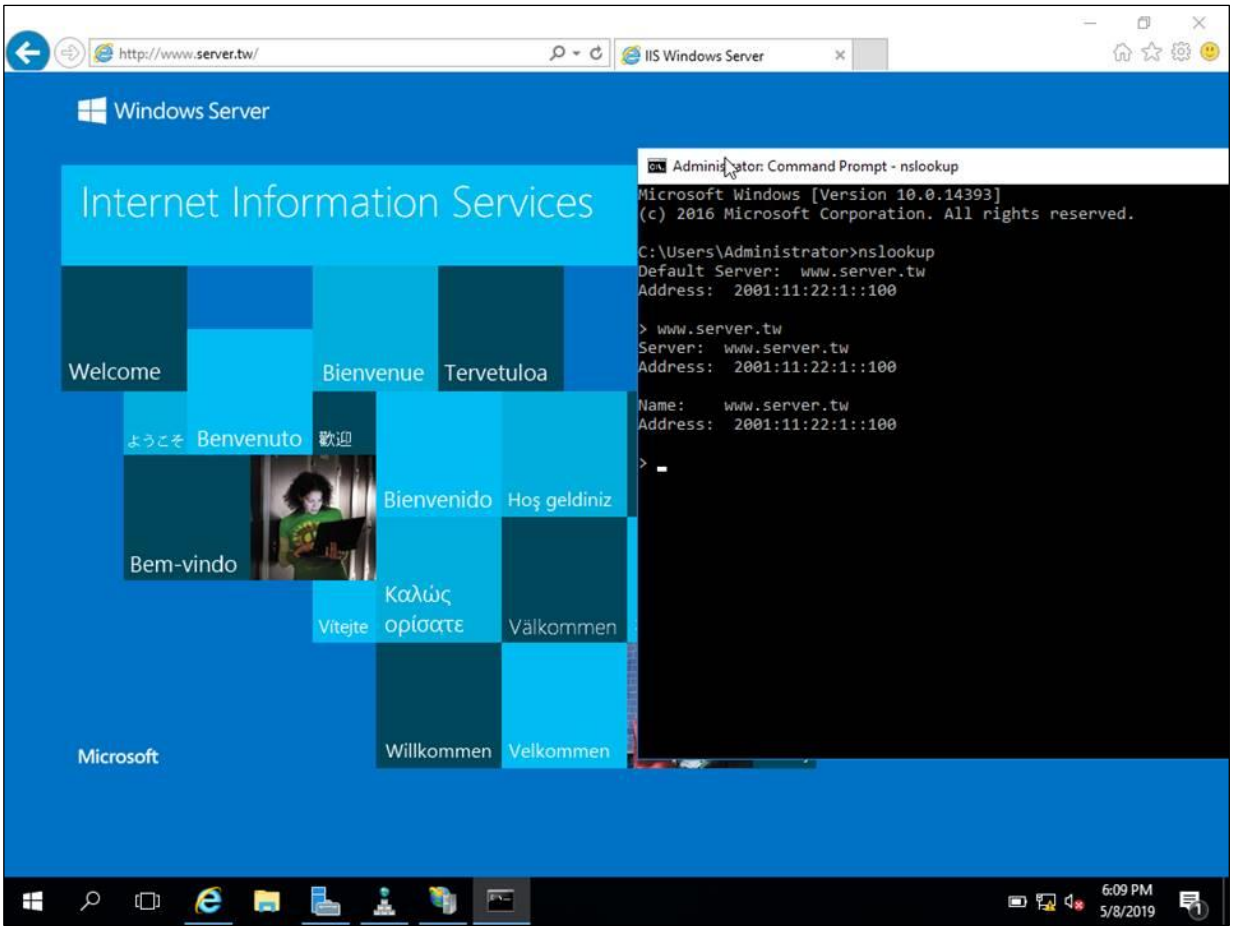

Server Manager
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nslookup
Default Server: ns1.server.tw
Address: 2001:11:22:1::100
> www.server.tw
Server: ns1.server.tw
Address: 2001:11:22:1::100
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

九、 IPv6 建置示範 IIS 系統設定

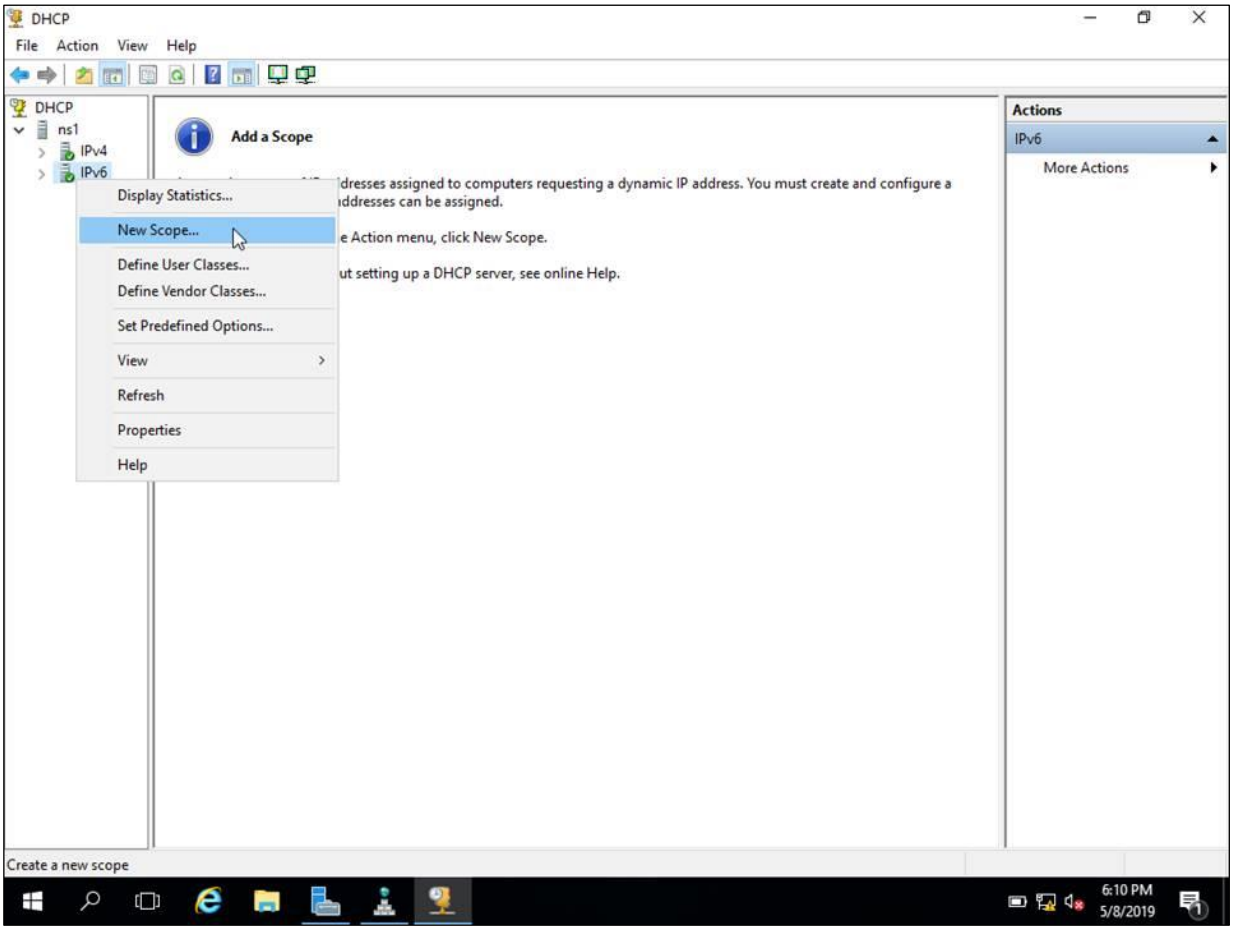


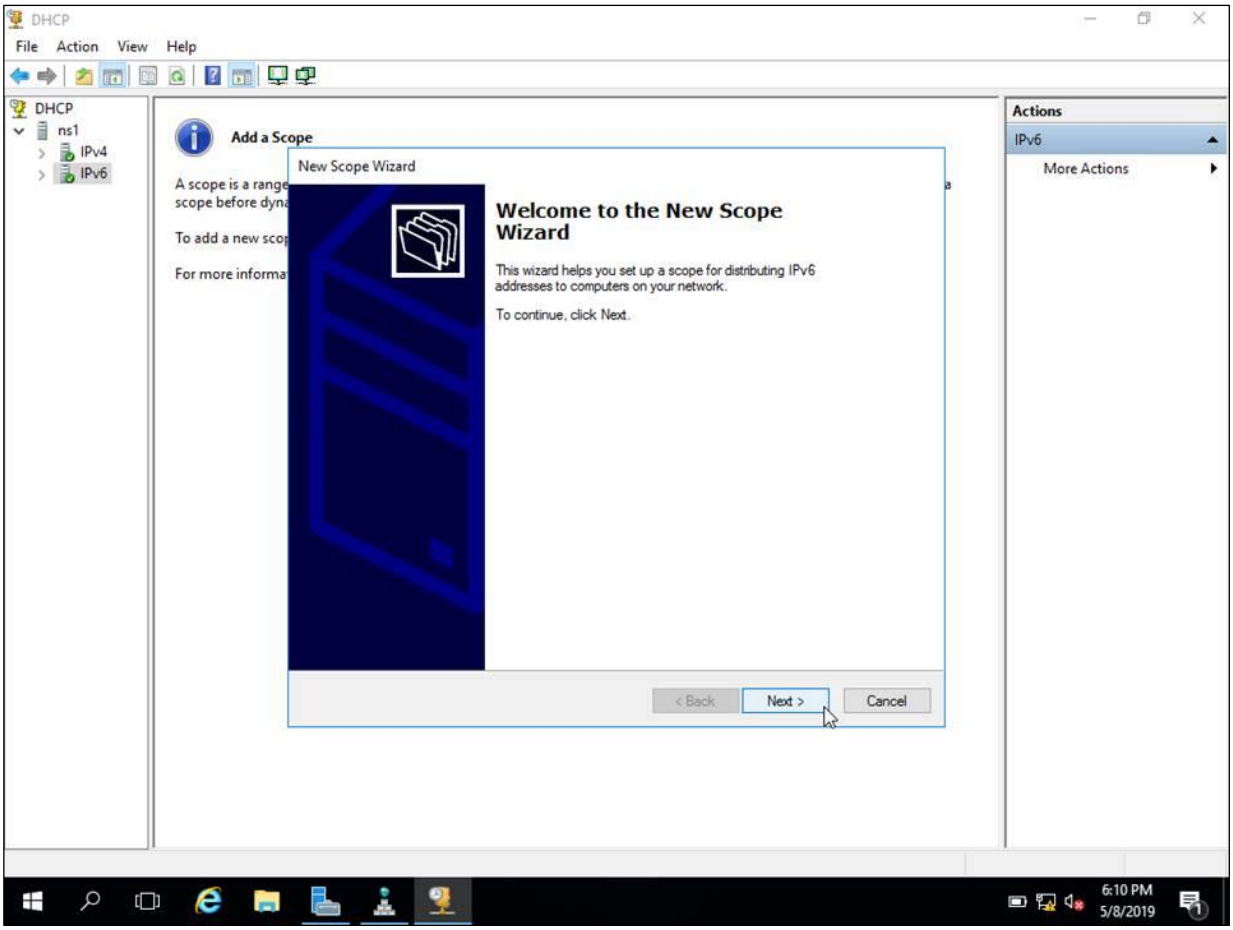

Internet Information Services (IIS) Manager
NS1 ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
NS1 (NS1\Administrator)
Application Pools
Sites
Default Web Site
Default Web Site Home
Filter:
Go
Show All
Group by: Area
IIS
Authentic...
Compression
Default Document
Directory Browsing
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

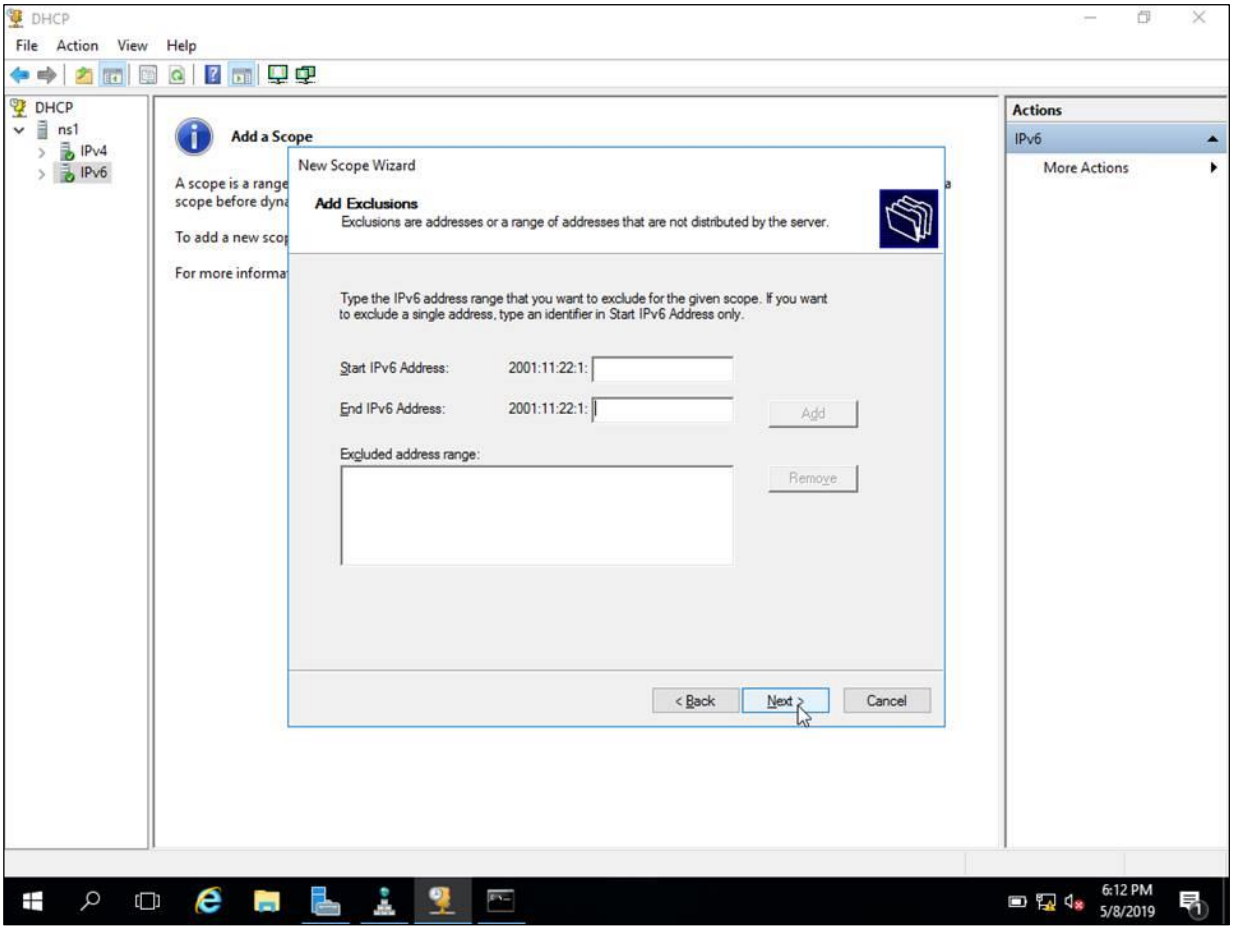

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
ברוכים הבאים
Welkom
Bem-vindo
Vitejte
Καλώς ορίσατε
Välkommen
환영합니다
Добро пожаловать
Üdvözöljük
مرحبا
欢迎
Willkommen
Velkommen
Witamy
Microsoft
6:08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

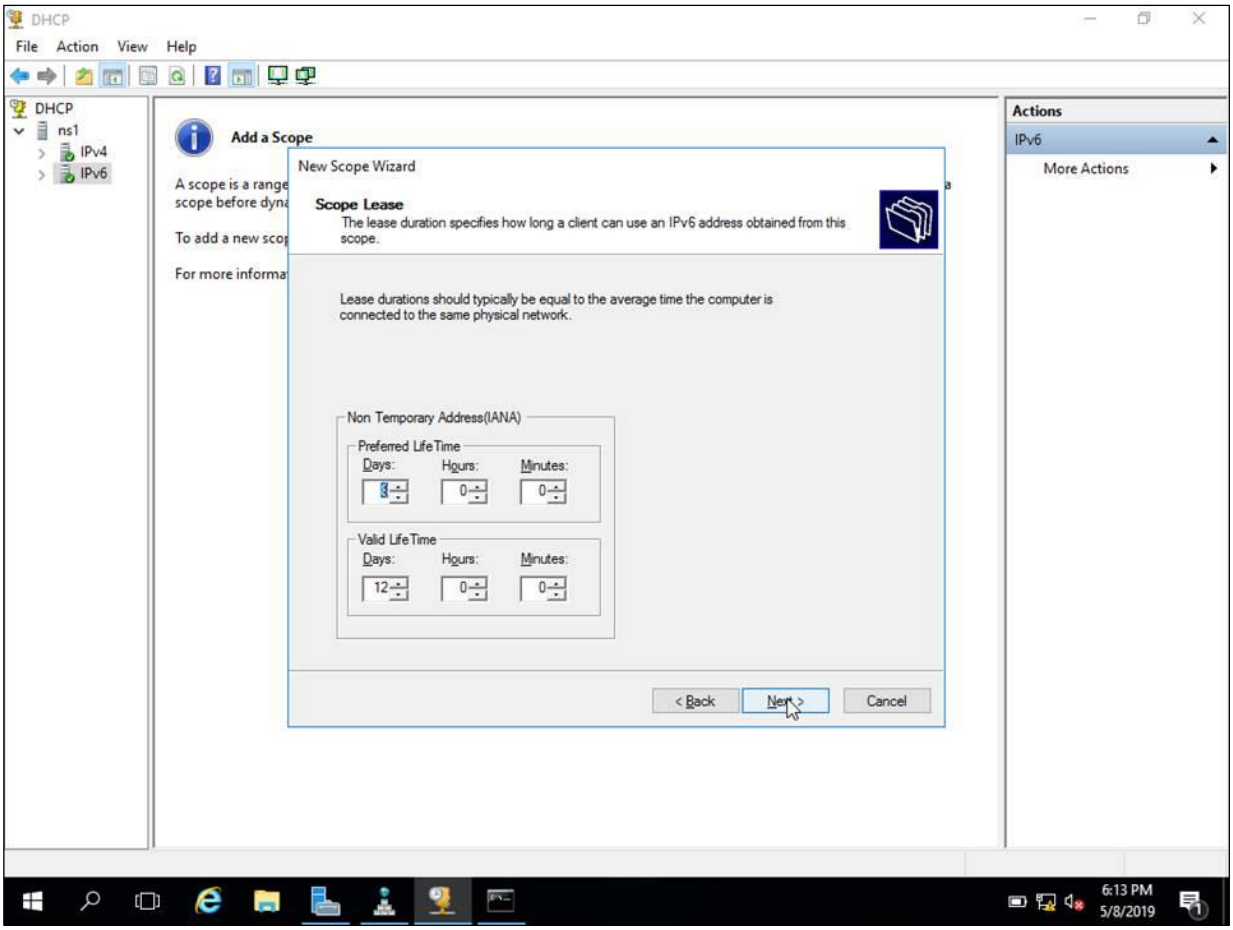

http://www.server.tw/
IIS Windows Server
Windows Server
Internet Information Services
Welcome
Bienvenue
Tervetuloa
ようこそ
Benvenuto
歡迎
Bienvenido
Hoş geldiniz
Bem-vindo
Vítejte
Καλώς ορίσατε
Välkommen
Willkommen
Velkommen
Microsoft
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(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

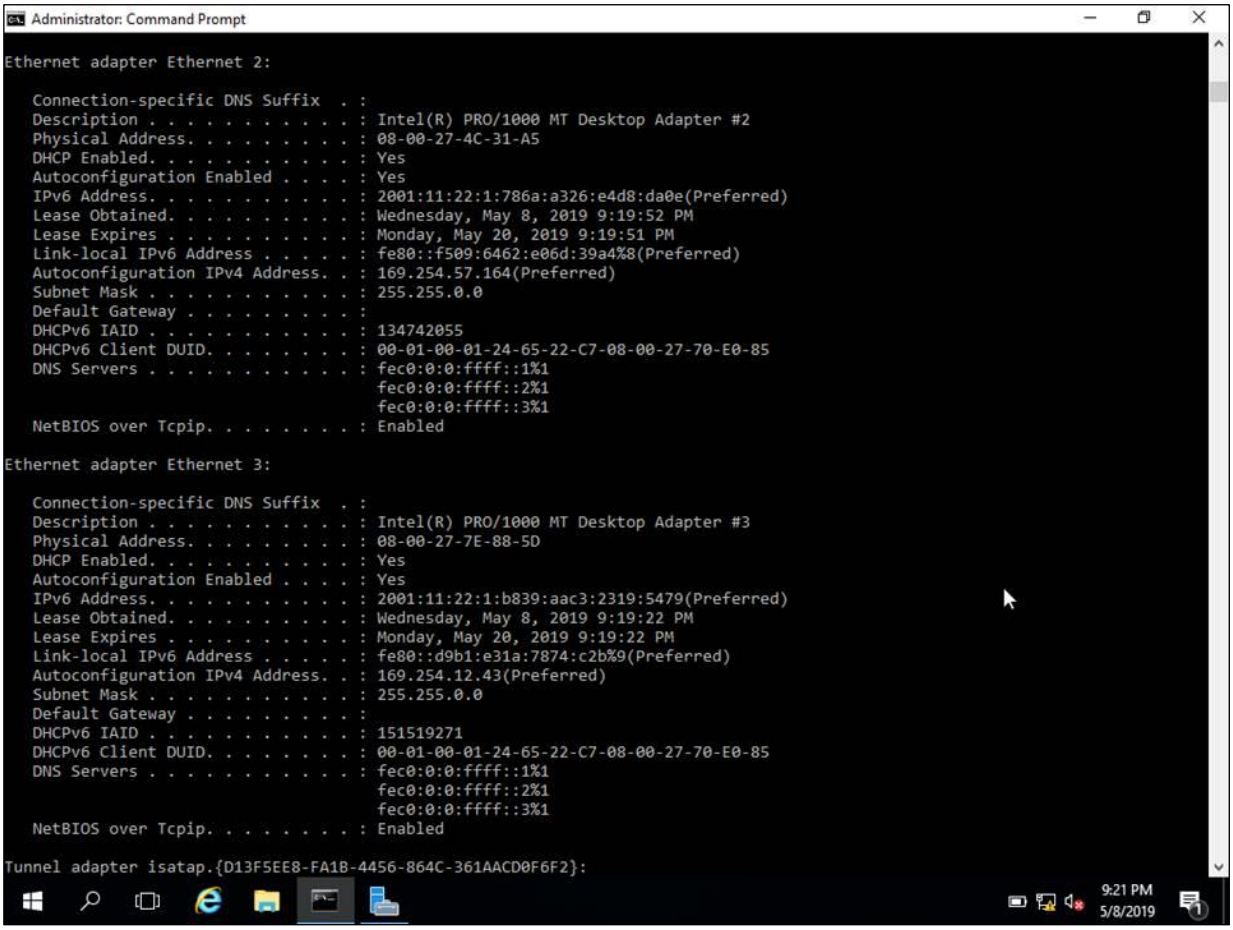
十、 IPv6 建置示範 DHCP 系統設定



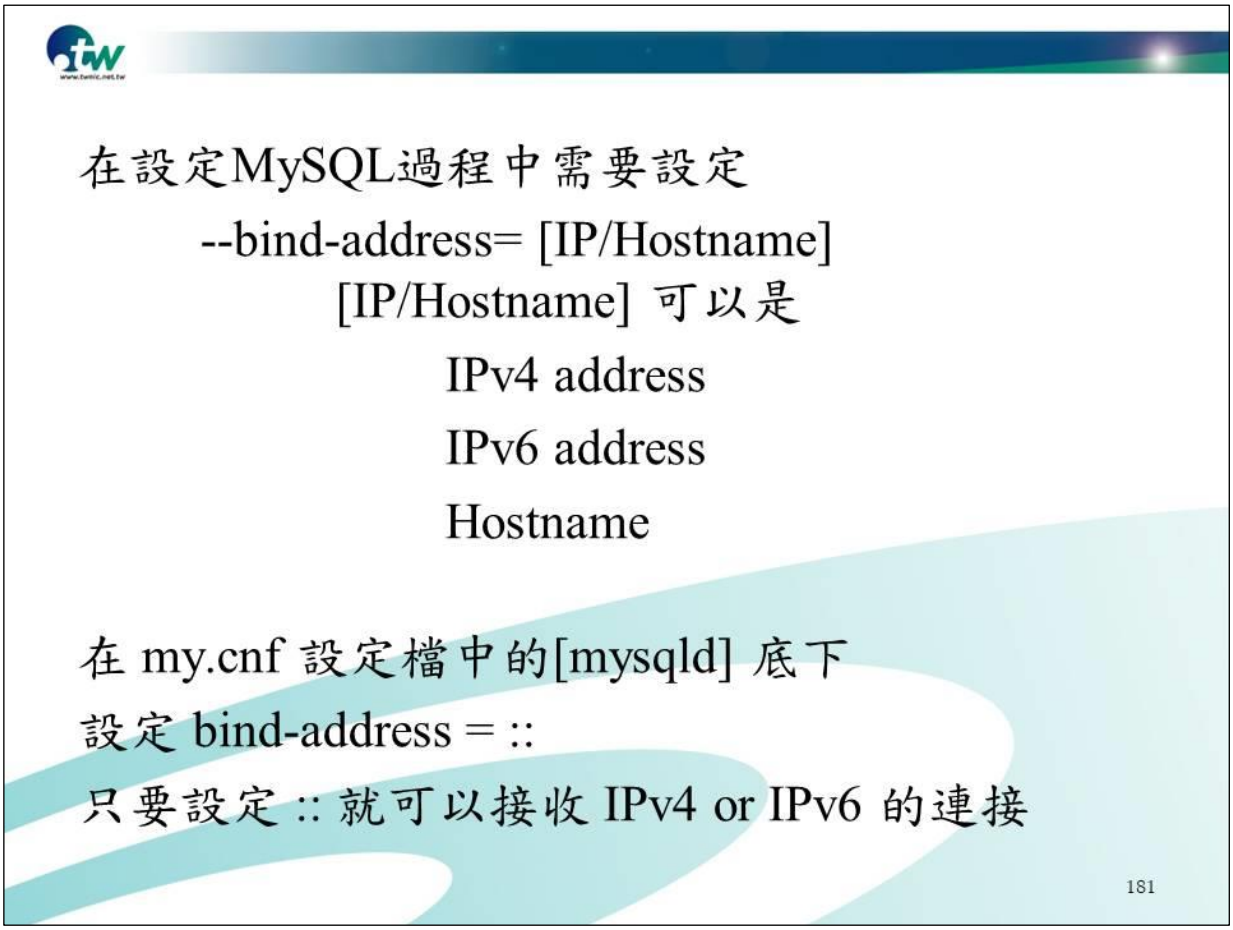

DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
A scope is a range
scope before dyna
To add a new scop
For more informa
New Scope Wizard
Welcome to the New Scope Wizard
This wizard helps you set up a scope for distributing IPv6 addresses to computers on your network.
To continue, click Next.
< 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
A scope is a range
scope before dyna
To add a new scop
For more informa
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

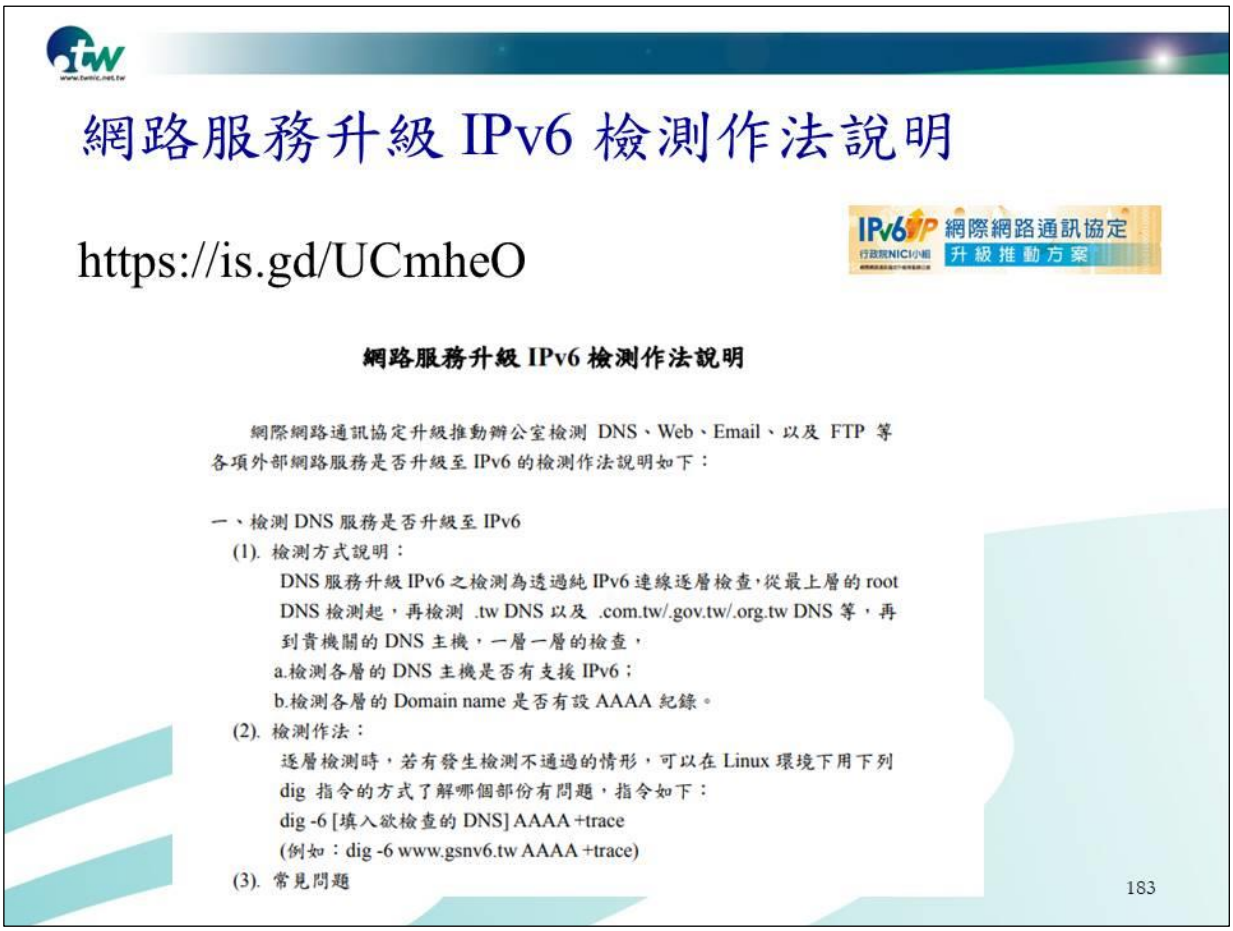

DHCP
File Action View Help
DHCP
ns1
IPv4
IPv6
Add a Scope
New Scope Wizard
Scope Lease
The lease duration specifies how long a client can use an IPv6 address obtained from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network.
Non Temporary Address(IANA)
Preferred LifeTime
Days: Hours: Minutes:
8 0 0
Valid LifeTime
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

十一、 資料庫 IPv6 調整示範



十二、 作業系統與網站升級流程步驟和檢查項目清單



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

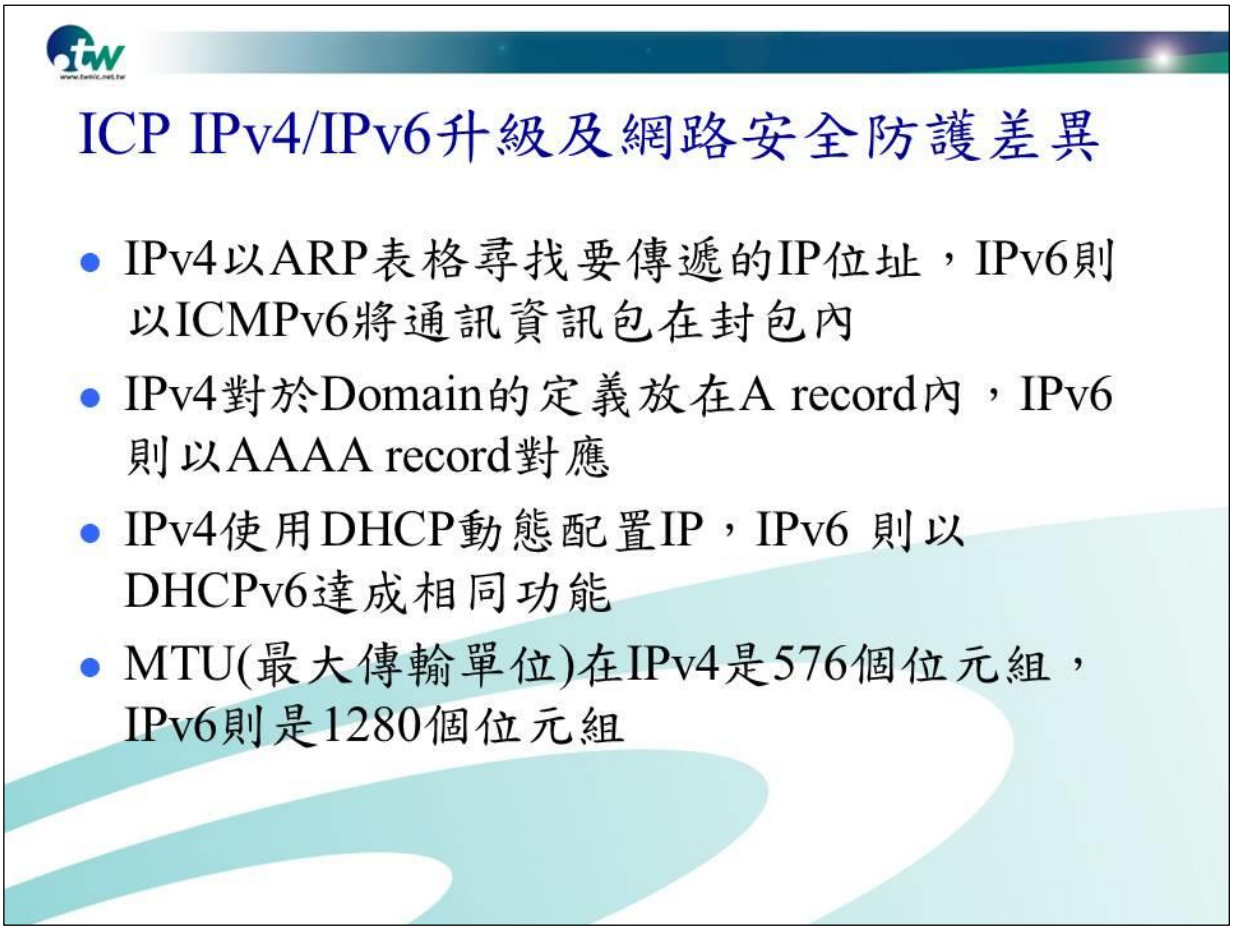
若是檢測一般Web網站，前面請加 http:// ，例如 http://www.twnic.net.tw
若是檢測 https 網站，前面請加 https:// ，例如 https://www.gsnv6.tw
若是檢測 Email, DNS, FTP，請直接輸入主機名稱(domain name)，例如 dns2.twnic.net.tw
本網站 www.gsnv6.tw 的IPv6位址為：2001:c50:ffff:1::9016

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

184

十三、 IPv4/IPv6 雙軌環境下資訊安全規劃概述



- 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

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> ! 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

(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

(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。

(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

(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

(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

(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)。

(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

(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

211

(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。

212

(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。

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

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

- 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

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：

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。

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。

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。

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

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

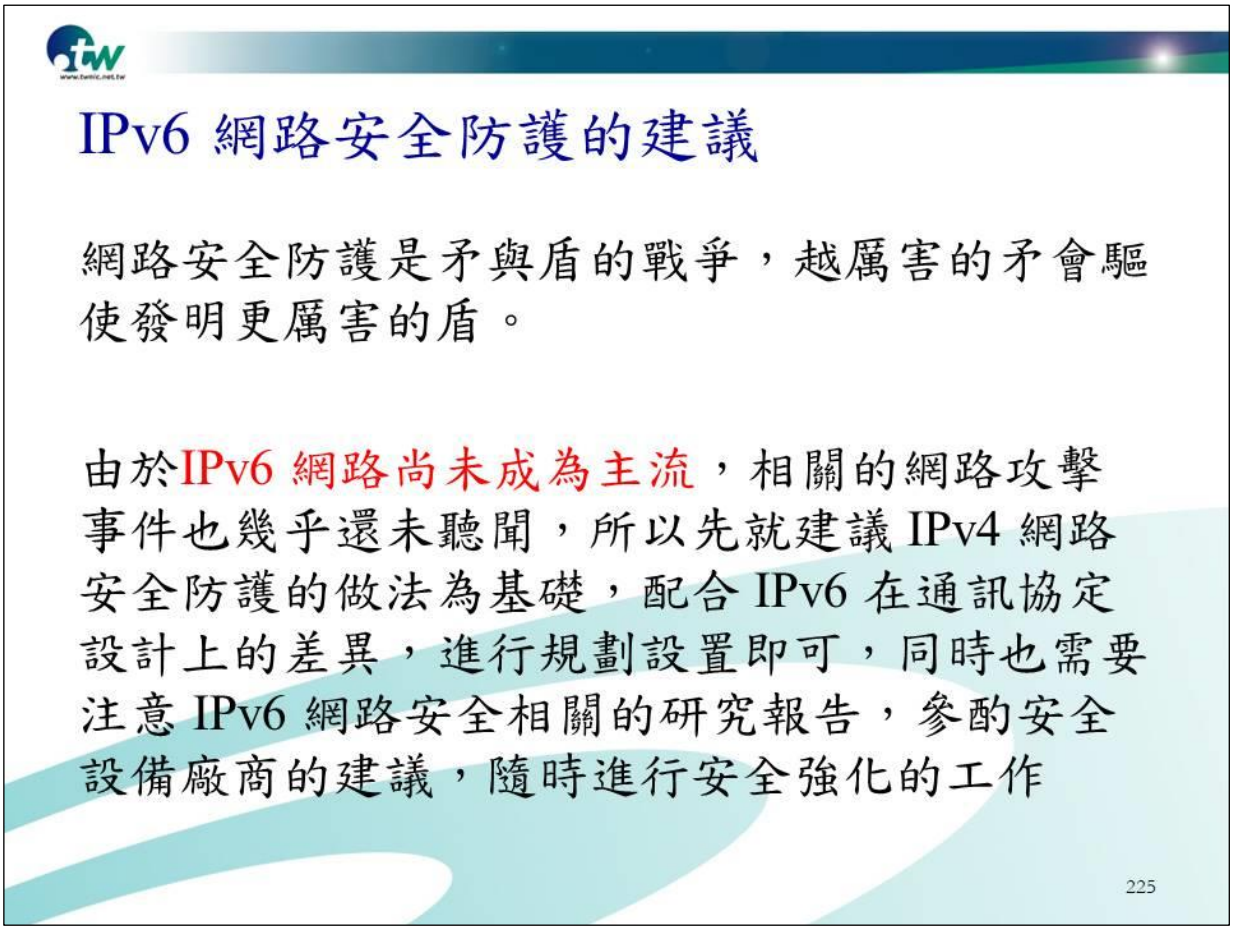
- Spoofing 議題：欺騙技術仍然可能發生在IPv6 網路中，但由於Neighbor Discovery，Spoofing 欺騙的位址範圍僅侷限在內部網域。

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。

十四、 IPv4/IPv6 雙軌環境之資訊安全軟體與硬體設定



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。

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。

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

228

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

229

(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。

230

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

231

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

異常位址追蹤與控管

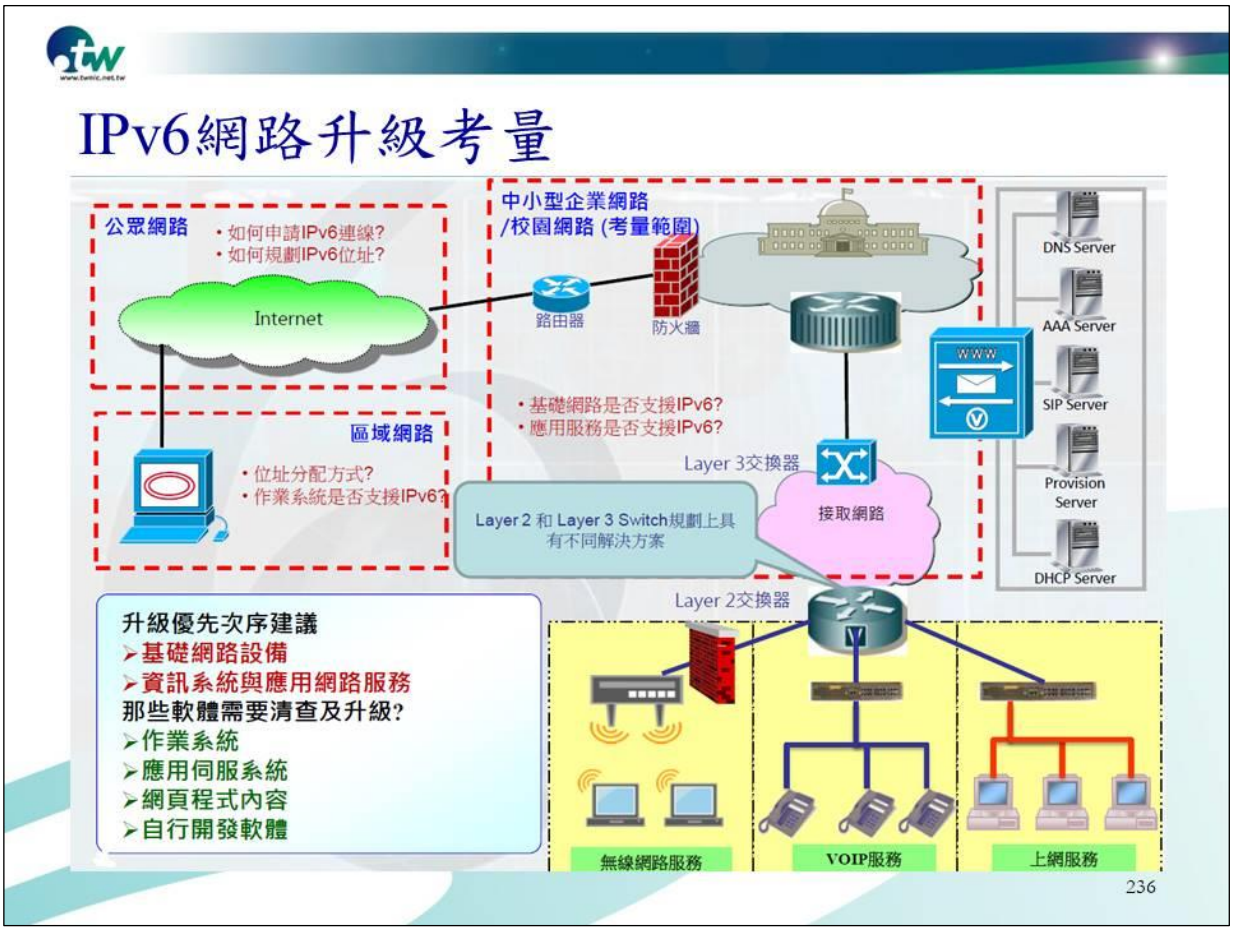
IPv6 用戶端位址的自動核發機制主要為 SLAAC (包含 SLAAC RDNSS 及 SLAAC + Stateless DHCPv6) 以及 Stateful DHCPv6，建議優先選用 Stateful DHCPv6 的位址核發機制，可以如同 IPv4 DHCP 的管理方式，記錄 IPv6 位址的核發記錄，並控管位址的核發原則，例如依據 MAC 位址綁定 IPv6 位址，或依據 MAC 位址管制是否核發 IPv6 位址。

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

十五、 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)



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

237

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

238

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？

239

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？

240

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：

241

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..

242

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)：

243

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…

244

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…

245

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…

246

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)

247

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)…

248

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

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

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

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

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

253