

台北市教育網路中心DNS集中管理資料設定

1.管理網址: <https://dnsmng.tp.edu.tw>

2.登入帳密: 請使用貴校行政代碼(六位數)做為預設帳號密碼登入, 以龍門國中為例, 使用333508為代碼密碼登入



帳號:

密碼:

限由學校IP登入

臺北市府教育局 資訊教育科
臺北市教育網路中心

3.管理介面說明:

<p>基本資料: 在此檢視網域的基礎資訊及變更密碼 (詳基本資料設定說明)</p> <p>DNS模式設定: 指定貴校將採用教網中心代管或自行管理DNS設定 (詳DNS模式設定說明)</p> <p>正解: 指定貴校所屬網域DNS正解資料 (詳正解設定說明)</p> <p>反解: 指定貴校所屬網域DNS反解資料 (詳反解設定說明)</p>	 <p>The screenshot shows the main interface of the Taipei Education Network Center's DNS Management System. At the top is the center's logo. Below it, the school name "學校: 龍門國中(333508)" is displayed. A tree view on the left shows the following structure:</p> <ul style="list-style-type: none">設定:<ul style="list-style-type: none">基本資料DNS模式設定正解:<ul style="list-style-type: none">lmjh.tp.edu.tw ↓反解<ul style="list-style-type: none">IPv4<ul style="list-style-type: none">210.243.35.0/24 ↓IPv6<ul style="list-style-type: none">2001:288:1269::/48 <p>At the bottom of the interface is a "登出" (Logout) button with a right-pointing arrow icon.</p>
--	---

基本資料設定說明

學校: 龍門國中(333508)

Domain Name:

1. [lmjh.tp.edu.tw](#).

IPv4:

1. [210.243.35.0/24](#)

IPv6:

1. [2001:288:1269::/48](#)

[更換密碼](#)

此處將顯示貴校DNS基本網域資訊, 其中包含

1. Domain Name: 即貴校網域名稱 (如 [lmjh.tp.edu.tw](#))
2. IPv4: 貴校所擁有IP範圍, 並採用掩碼形式表示(如 [210.243.35.0/24](#))
3. IPv6: 貴校所擁有IPv6範圍, 並採用掩碼形式表示(如 [2001:288:1269::/48](#))
4. 更換密碼: 更換貴校登入本系統用的密碼, **請務必儘快修改**

DNS模式設定說明

正解網域名稱(Domain Name):

網域名稱	目前狀態	更新日期	我要.....
lmjh.tp.edu.tw	自行建置管理	2019/3/25 上午 10:36:22	使用市網DNS 設定授權資料(NS)

IPv4反解:

IP位址	目前狀態	更新日期	我要.....
210.243.35.0/24	自行建置管理	2019/4/9 上午 10:37:28	使用市網DNS

IPv6反解:

IP位址	目前狀態	更新日期	我要.....
2001:288:1269::/48	自行建置管理	2018/1/12 下午 09:36:03	使用市網DNS 設定授權資料(NS)

1.初次進入DNS模式設定時, 貴校的目前狀態應顯示 **自行建置管理**, 而後面的按鈕則會顯示 **使用市網DNS** 也就是貴校的DNS模式是由貴校的資訊人員自行建置DNS伺服器, 相關DNS紀錄都由貴校自行維護

**請注意, 當您將設定都建置的差不多後, 您可以準備做代管作業, 此時強烈建議您先聯繫市網管理人員: 蔡政道老師(Email:jdtasai@tp.edu.tw 或 jdtasi@slhs.tp.edu.tw), 請蔡老師先協助您檢查一下DNS內容是否有沒有異常, 完成回報之後您就可以進行託管

2.當貴校在此系統上已經完成相關的DNS紀錄設定之後，可以在此處點選 **使用市網DNS** 即可將貴校DNS紀錄資訊，交由教網中心的DNS集中管理系統，當送交給市網中心管理後，畫面即會修正為

正解網域名稱(Domain Name):

網域名稱	目前狀態	更新日期	我要.....
lmjh.tp.edu.tw.	使用市網DNS	2019/5/22 下午 03:45:04	自行建立DNS

IPv4反解:

IP位址	目前狀態	更新日期	我要.....
210.243.35.0/24	使用市網DNS	2019/5/22 下午 03:45:10	自行建立DNS 產生上傳教育部資料

IPv6反解:

IP位址	目前狀態	更新日期	我要.....
2001:288:1269::/48	使用市網DNS	2019/5/22 下午 03:45:21	自行建立DNS

也就是貴校的目前狀態顯示 **使用市網DNS**，而後面的按鈕則會顯示 **自行建立DNS** 也就是貴校的DNS模式是由市網的DNS統一管理對外查詢服務，但是請注意!! 相關DNS紀錄 **還是由貴校自行維護**，因此校內如果有DNS紀錄需要更正，須請貴校管理人員到此系統內修改DNS紀錄

- 3.爾後貴校如果有更新DNS紀錄時，請直接在此系統當中的紀錄做適時修正
- 4.貴校採用市網DNS集中管理功能之後，校內原本運作的DNS伺服器即可終止服務
- 5.貴校防火牆上接受外部DNS查詢的設定亦可中止/拒絕存取(徹底杜絕外面DNS侵擾，此亦為DNS集中管理主要精神)

正解設定說明

 網域名稱: lmjh.tp.edu.tw

FQDN	TTL	Type	RData
------	-----	------	-------

初次進入正解設定時, 由於完全沒有設定資料, 因此是一片空白無誤, 此時只要點選綠色的加號圖示, 即可開始進行貴校的網域名稱解析資料設定

新增正解記錄(RR, Resource Record)

Record Type:

FQDN: lmjh.tp.edu.tw

TTL: 秒

IPv4位址:

自動設定反解

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

MX: RDATA輸入之名稱不可用CNAME設定出來的, 須有對應之A記錄, 或為外界Mail Server只文字網域名稱.

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA欄位.

此處將進行較為詳盡的解說

Record Type: 指定正解紀錄的類型, 可以選擇的項目有以下幾項:

- 1.A: 也就是將網域名稱轉譯為IPv4格式
- 2.AAAA: 也就是將網域名稱轉譯為IPv6格式
- 3.MX: 指定電子郵件在轉寄的時候, 應轉送到哪個網域去
- 4.CNAME: 指定同一個網域名稱的別名

5.TXT:針對某一個網域名稱做文字的描述, 並且可用來作為驗證所屬網域的用途上(類似在此放入金鑰以確保此網域真的受此DNS管理), 比方說貴校如果有申請Google G-Suite服務, 那麼貴校的DNS設定內就必定有TXT紀錄

針對以上的類型設定, 我們在此做一些簡單的例子解說

類型	對應網域	指定值	意義
A	www.lmjh.tp.edu.tw	210.243.35.1	當使用者查詢 www.lmjh.tp.edu.tw 網址時, DNS會解譯為210.243.35.1這個IPv4
AAAA	www.lmjh.tp.edu.tw	2001:288:1269::1	當使用者查詢 www.lmjh.tp.edu.tw 網址時, DNS會解譯為2001:288:1269::1這個IPv6
MX	mail.lmjh.tp.edu.tw	1	當Email轉寄至本網域的時候, 第一順位優先轉至mail.lmjh.tp.edu.tw這個網址
MX	m2.lmjh.tp.edu.tw	2	當Email轉寄至本網域的時候, 如果前面的mail.lmjh.tp.edu.tw因為各種原因未正常將信件收下或告知應該退信, 第二順位將轉至m2.lmjh.tp.edu.tw這個網址
CNAME	www.lmjh.tp.edu.tw	w3	原本已經有指定IP的網址, 另有一個別名w3, 意即www.lmjh.tp.edu.tw也同時擁有w3.lmjh.tp.edu.tw這個網址
TXT	www.lmjh.tp.edu.tw	"this is test"	當對方查詢www.lmjh.tp.edu.tw這個網址時, 將額外提供this is a website這行資訊給對方
SRV	lmjh.tp.edu.tw	詳情請看以下 有關SRV的設定說明	

那麼就來設定貴校的網域名稱資料吧! 首先我們把正解的資料輸入進去, 此系統已經具有反解自動加進去的功能, 除非貴校正解與反解資訊有所不同, 否則正解資料輸入完成之後, 基本上貴校的DNS資料就幾乎建置完備了!

點選網域名稱旁邊的綠色加號按鈕, 右側建置功能選單即會顯示出來



新增正解記錄(RR, Resource Record)

Record Type: A ▼

FQDN: .lmjh.tp.edu.tw.

TTL: 秒

IPv4位址:

自動設定反解

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

**MX: RDATA輸入之名稱不可用CNAME設定出來的, 須有對應之A
記錄, 或為外界Mail Server 只文字網域名稱.**

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA欄位.

確定

離開

以上述這個例子, 即表示我們將建立一筆A類型的正解紀錄, 此紀錄會將www.lmjh.tp.edu.tw網址解譯為210.243.35.11, 並且在按下確定之後, 自動為此筆紀錄設定反解(也就是當網路查詢到210.243.35.11時, 會認得www.lmjh.tp.edu.tw這個網址)

在按下確定之後, 貴校的正解清單就會出現剛才設定的正解資料

 網域名稱: lmjh.tp.edu.tw,

FQDN	TTL	Type	RData	
www	14400	A	210.243.35.11	  

現在讓我們再做一次, 這次一樣點選綠色加號按鈕, 但我們改選擇設定AAAA類型

新增正解記錄(RR, Resource Record)

Record Type: AAAA ▾

FQDN: www.lmjh.tp.edu.tw

TTL: 14400 秒

IPv6位址: 2001:288:1269::11

自動設定反解

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

MX: RDATA輸入之名稱不可用CNAME設定出來的, 須有對應之A記錄, 或為外界Mail Server只文字網域名稱.

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA欄位.

確定

離開

以上述這個例子, 即表示我們將建立一筆AAAA類型的正解紀錄, 此紀錄會將www.lmjh.tp.edu.tw網址解譯為2001:288:1269::11, 並且在按下確定之後, 自動為此筆紀錄設定反解(也就是當網路查詢到2001:288:1269:11時, 會認得www.lmjh.tp.edu.tw這個網址)

在按下確定之後, 貴校的正解清單就會出現剛才設定的正解資料

 網域名稱: lmjh.tp.edu.tw,

FQDN	TTL	Type	RData	
www	14400	A	210.243.35.11	  
www	14400	AAA...	2001:288:1269::11	  

連同上一筆建立的清單, 因此目前就有兩筆正解資料, 請注意同一個網域名稱可以同時持有兩個不同格式的IP, A類型專用於設定IPv4, AAAA類型則專用於設定IPv6, 兩者並不衝突, 然而如果網域內有以下這樣的狀況:

FQDN	TTL	Type	RData
www	14400	A	210.243.35.11
web	14400	A	210.243.35.11

以上的例子將www.lmjh.tp.edu.tw跟web.lmjh.tp.edu.tw的正解紀錄都指定到210.243.35.11, 正常來說, 不同的網域名稱應該持有不同的IP, 而這樣的定義就意味著www.lmjh.tp.edu.tw跟web.lmjh.tp.edu.tw都指向同一個IP位址, 但如果我們希望這兩個網域名稱共同持有相同的IP, 但還是要以www.lmjh.tp.edu.tw為這個IP的正確持有網域名稱時, 可以使用剛才我們所提到的別名CNAME

再次點選綠色加號按鈕, 這次我們改選擇CNAME類型

新增正解記錄(RR, Resource Record)

Record Type:

FQDN: .lmjh.tp.edu.tw.

TTL: 秒

原始主機之FQDN:

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

MX: RDATA輸入之名稱不可是用CNAME設定出來的, 須有對應之A記錄, 或為外界Mail Server只文字網域名稱.

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA欄位.

以上面的例子所表示出來的意義是: 當使用者查詢 web.lmjh.tp.edu.tw這個網址時, 貴校DNS會自動將其指向到屬於 www.lmjh.tp.edu.tw這個網址的正解紀錄去, 也就是稍早設定的210.243.35.11 以及 2001:288:1269:11去

請特別注意! 在此處指定的FQDN係指該網址的完整網路名稱, 也就是說您不可以只有在原始主機之FQDN欄位內輸入 www 這麼單純的內容, 而是必須要輸入最完整的網址, 此外, 在此處輸入完整的FQDN名稱時, 務必要將最後一個句點標上, 一般我們輸入網址的時候會省略它, 但在此請不要省略

格式	意義	備註
www	網域單一主機/來源名稱	
www.lmjh.tp.edu.tw	完整主機/來源網址名稱	tw後面的句點可以省略
www.lmjh.tp.edu.tw.	FQDN	tw後面的句點 不可以 省略

當你指定了一筆CNAME類型之後, 結果也會呈現在正解的設定資料內

w3	14400	A	210.243.35.21	  
w3	14400	AAA...	2001:288:1269::21	  
web	14400	CNA...	www.lmjh.tp.edu.tw.	  

請注意CNAME指定的別稱概念, 以上面的例子是讓www主機也同時持有web這個別名, 因此這台主機的正式名稱仍然是www

不過如果我們就是不想這麼麻煩, 我就是希望www跟web共同持有這同一組IP呢? 實際上有些網站我們的確也有這樣的設定的不是嗎?

以上面的例子, 其實就只要再多新增一筆A跟AAAA正解紀錄給web就可以了!

新增正解記錄(RR, Resource Record)

Record Type: A ▼

FQDN: web.lmjh.tp.edu.tw.

TTL: 14400 秒

IPv4位址:

210.243.35.11

自動設定反解

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

MX: RDATA輸入之名稱不可用CNAME設定出來的, 須有對應之Mail Server只須輸入文字之網域名稱.

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA欄位.

如果說DNS設定當中, 不同的網域名稱都可以指向同一個IP, 那麼CNAME這個別名的功能不就不需要了嗎? 實際上, CNAME的應用並非只有這樣, 上面我們已經提過指定別名的時候, 事實上是必須要指定完整的網域名稱, 因此當我們做了一些特殊的別名應用時, 可以將學校的網址名稱, 對應到外部的網域去, 例如貴校如果有申請Google的G-Suite服務, 那麼您一定可以在原本的DNS設定當中看到這樣的指定

新增正解記錄(RR, Resource Record)

Record Type: CNAME ▼

FQDN: mail.lmjh.tp.edu.tw.

TTL: 14400 秒

原始主機之FQDN:

ghs.googlehosted.com.

輸入之字元限「a-z」(大小寫均可), 「0-9」, 及「-」

如要與學校網域名稱相同, 請輸入「@」或不輸入留空白

確定

離開

這樣的意思是說, 如果貴校的師生想要使用Google的Gmail服務, 除了直接透過Gmail信箱進行存取以外, 您也可以直接在DNS內部去指定mail.lmjh.tp.edu.tw這個網址的別名是ghs.googlehosted.com, 這筆指定就會引導使用的人一樣連線到Gmail信箱
您可能經由一連串の設定, 將許多別稱通通指定給同一個網域名稱, 例如這樣:

mail	14400	CNA...	ghs.googlehosted.com.	 
drive	14400	CNA...	ghs.googlehosted.com.	 
calendar	14400	CNA...	ghs.googlehosted.com.	 

請稍微思考一下, 這是合理也合法的設定, 請注意上述的例子所代表的意義是這樣
mail.lmjh.tp.edu.tw → ghs.googlehosted.com → mail.google.com

drive.lmjh.tp.edu.tw → ghs.googlehosted.com → drive.google.com
calendar.lmjh.tp.edu.tw → ghs.googlehosted.com → calendar.google.com

刻意將mail.lmjh.tp.edu.tw指定給mail.google.com並不是正確做法，請注意外部網址的別名轉換也有一定規則，mail.google.com是受到google本身的管轄，不是你強制把自己的網域名稱指定給它去處理，它就一定要接受，再舉個例子，應該就能理解了：

新增正解記錄(RR, Resource Record)

Record Type: CNAME ▾

FQDN: mail.lmjh.tp.edu.tw

TTL: 14400 秒

原始主機之FQDN: mail.edu.tw

這樣的設定相信你也覺得不合理吧？

這同時也反映出一個狀況，如果您想要強制將mail.lmjh.tp.edu.tw設定為mail.edu.tw的別名是不合理的，所以自然而然如果你想將mail.lmjh.tp.edu.tw的正解紀錄指定為mail.edu.tw的實際IP也是不合理的，但如果你真的想在自己的DNS上指定mail.lmjh.tp.edu.tw的正解IP是mail.edu.tw的IP呢？

在DNS設定資料內有一塊是針對Email的資料，我們使用的是MX這個參數，主要的概念就是當有人寄信給跟你所屬的網域時，DNS可以去問哪一些伺服器，以下用幾個例子來解釋這個設定方式：

(1)寄信給 john@mail.lmjh.tp.edu.tw

首先你應該要知道，我們通常是不會留 john@210.243.35.1 這樣的Email給別人的，而是留mail.lmjh.tp.edu.tw這樣的形態，既然留下的型態是名稱，而不是IP這樣的數字格式，當然就必須由DNS先進行解釋

因此當有一封信由對方的**寄信**伺服器**寄出**後，指定使用者的網址是mail.lmjh.tp.edu.tw，自然在網路上轉信到最後就會丟到我們的網路來，那麼這封信將會由我們的**收信**伺服器**收下**，但是一個網路內有多少台**收信**伺服器，其實還是貴校自己決定的，這封信到底要由誰收下，就是利用MX來決定

比方說你在DNS下設定了這樣的參數
mail IN MX ms1.lmjh.tp.edu.tw.

依照我們之前認知的想法，這意思就是當有人寄信給 mail.lmjh.tp.edu.tw這個網址時，DNS會跟對方說：我們這裡會請 ms1.lmjh.tp.edu.tw這台伺服器處理

所以對方的寄信伺服器就會跟我們的ms1.lmjh.tp.edu.tw伺服器詢問有沒有john這個帳號的存在, 如果有, 這封信就會由ms1.lmjh.tp.edu.tw這台伺服器收下, 如果沒有, 這封信就會被我們的伺服器拒絕, 而寄出這封信的伺服器也會將這封信退回給最初寄信的人

不過一般來說, 我們給對方的信件不會給這麼長, 而是給 john@lmjh.tp.edu.tw 這樣長度的就足夠了, 那這樣的話在DNS裡面要怎麼設定呢? 其實只要這麼指定就可以了!

```
@ IN MX ms1.lmjh.tp.edu.tw.
```

這裡的@所表示的就是你的網域名稱 lmjh.tp.edu.tw , 換句話說如果這樣指定, 表示所有寄信到你所屬網域的資料都交由 ms1.lmjh.tp.edu.tw這個伺服器處理

但是慢慢的會衍生出一些問題, 比方:

- 1.如果所屬單位的子單位又各自架設了自己的伺服器, 但信件寄來的時候怎麼處理?
- 2.如果所屬單位的人員太多怎麼辦? 一台伺服器夠不夠用? 如果不夠用怎麼辦?

針對第一個狀況, 就是土法煉鋼的在DNS內各自指定即可, 譬如

```
ms1 IN MX ms1.lmjh.tp.edu.tw.
```

```
ms2 IN MX ms2.lmjh.tp.edu.tw.
```

這樣的話就可以分別寄信給 john@ms1.lmjh.tp.edu.tw 跟 mary@ms2.lmjh.tp.edu.tw 了

不過很快地就面臨到假設我想寄信給不同單位的john跟mary, 但是我又希望只保留最短的網址當作這些人的email地址呢? 也就是說我希望大家的email都是 @lmjh.tp.edu.tw呢?

這個需求也同樣服膺到第二個狀況上, 也就是人太多的話怎麼辦, 只要人太多就是必要擴充硬碟容量, 因為每個人的信箱容量只能增加, 不能因為人員增加強制減少, 加上處理大家的信件效能, 不是只有每增加一個帳號就消耗一點效能這麼單純, 而是必須去考量擴增郵件伺服器的數量, 所以就有了MX紀錄的順序概念產生

上面的兩個做法可以一次用以下的方式解決

```
@ IN MX 1 ms1.lmjh.tp.edu.tw.
```

```
@ IN MX 2 ms2.lmjh.tp.edu.tw.
```

你很容易發現在設定的架構上多了一個數字的部位, 這個部位指的是DNS回覆給對方的順序, 也就是以下的狀況:

a.假設寄給 john@lmjh.tp.edu.tw(確實存在於 **ms1**.lmjh.tp.edu.tw)

由DNS上取得的MX紀錄, 第一次會先回復ms1.lmjh.tp.edu.tw這個伺服器給對方, 因此對方伺服器會先詢問是否有 john@ms1.lmjh.tp.edu.tw 的存在, 此信收下

b. 假設寄給 mary@lmjh.tp.edu.tw (確實存在於 ms2.lmjh.tp.edu.tw)

由DNS上取得的MX紀錄, 第一次會先回復 ms1.lmjh.tp.edu.tw 這個伺服器給對方, 因此對方伺服器會先詢問是否有 mary@ms1.lmjh.tp.edu.tw 的存在, 但實際上mary並不在ms1伺服器內, 因此伺服器會拒絕收下此信, 除非當下 ms1.lmjh.tp.edu.tw 並沒有正常回應對方, 而此時DNS上還有第二順位的MX紀錄, 因此會再次回復 ms2.lmjh.tp.edu.tw 這個伺服器給對方, 對方伺服器就會知道有 mary@ms2.lmjh.tp.edu.tw 的存在, 此信最後仍收下, 但您應該會發現如此 mary@ms2.lmjh.tp.edu.tw 掉信的情況就會非常嚴重!! 因為她收到信的機會就是第一台 ms1.lmjh.tp.edu.tw 掛掉的時候

c. 假設寄給 alvin@lmjh.tp.edu.tw

如果這些伺服器都沒有alvin這個帳號的存在, 此信當然最後還是被拒絕, 寄件者收到退信通知

d. 假設ms1, ms2都有john這個帳號

這個情形當然還是會存在 (因為單位之間可能彼此不互通導致帳號重疊), 此時就會以DNS的順序來決定由哪一個帳號收下這封信, 依照上面的設定, 則會是 john@ms1.lmjh.tp.edu.tw 收下, 而 john@ms2.lmjh.tp.edu.tw 則無法收到信

還有另外的情形是, 雖然Email的格式是 @lmjh.tp.edu.tw, 感覺上這個收信的伺服器也應該在我們所屬的網域下, 但就像之前我們所說的CNAME一樣, MX也具備了同樣的效果, 我們可以在DNS紀錄上, 直接將收信的資料移轉到外部網站去處理, 比方說這樣的設定

```
@ IN MX aspmx.l.google.com.
```

這樣的意思就是說, 當有人寄信給 john@lmjh.tp.edu.tw 時, 這封信會被移轉到 aspmx.l.google.com 這個網址去處理, 此時這封信會從原本要求我們網域內的伺服器去處理的前提, 直接交由Google去處理, 而Google處理的時候就是把 john@lmjh.tp.edu.tw 當成一個完整的帳號去檢查是否有此帳號的存在, 而不僅僅只是查看是否有john這個帳號的存在, 試想john這個帳號有多少單位在使用, 但是 john@lmjh.tp.edu.tw 對Google來說就只有單一個帳號了

不過由於Google這種超大型的網路, 如果信件只有交付給單一個網域去處理, 可能在效能跟穩定度上不足, 所以一樣可以透過設定順序的方式, 來提供穩定的信件交換水準

```
@ IN MX 1 aspmx.l.google.com.  
@ IN MX 3 alt1.aspmx.l.google.com.  
@ IN MX 5 alt2.aspmx.l.google.com.  
@ IN MX 7 alt3.aspmx.l.google.com.
```

注意MX設定的時候, 只看數字順序, 並沒有刻意強調數字一定要一個接著一個, 所以上面的例子就是1,3,5,7按數字大小順序回應, 如果改成 10,20,30,40不會影響結果

解釋了這麼多，最終還是要把這些紀錄登記在集中系統內，以下即為一筆範例：

新增正解記錄(RR, Resource Record)

Record Type:

FQDN: .lmjh.tp.edu.tw.

TTL: 秒

Preference Value:

郵件伺服器之FQDN:

輸入之字元限「a-z」(大小寫均可),「0-9」,及「-」
如要與學校網域名稱相同,請輸入「@」或不輸入留空白

基本上因為我們將信件服務交由Google管理，所以在FQDN的欄位上可以省略(或輸入@符號)，注意Preference Value就是輸入這筆資料的順序，以上面圖形的例子本意就是這個設定：

```
@ IN MX 1 aspmx.l.google.com.
```

請記得貴單位有多少筆MX順序紀錄，請全數輸入完畢

接著我們來討論TXT，前文我們有提到這個參數主要是對某一個網域名稱做文字的描述，並且可用來作為驗證所屬網域的用途，如果你的所屬網域，相關網路服務都是由自己架設及管理，那麼你的DNS紀錄裡面就有可能沒有TXT紀錄的存在，這是正常現象！

但是相反的，如果你的單位信件是交付給Google這樣的外部單位管理，那麼你的DNS紀錄裡面就不可能沒有TXT資料，主要是因為Google必須要確認你申請服務的時候，你所申請的網域名稱的確是受到你的管轄，而要檢驗這個網域是不是歸你所屬的有效方式，當然就是透過DNS紀錄檢查

因此，Google會要求你必須依照它的指示，在DNS記錄內以TXT的形式保存一份它設計的格式內容，然後Google依照這個格式去詢問你管轄的DNS，如果可以得到相同的結果，當然就可以確認這個網域是歸你所管了

TXT的設定語法範例

```
google._domainkey IN TXT "v=DKIM1; k=rsa;  
p=MIGBiNXzuzjXCf1Krz7GS40B40BiNXzuzjXCf1Krz7GHIGBiNXzuzjXCf1Krz7GKrz7  
GS40Br9DKZiuIGBiNXzuzjXCf1Krz7GuzjXCf1Krz7GS40BiNXzuzjXCf1KrzLkokuMjP1
```

c714TGlgJqFexTk8VsSS40BiNXzIGBiNXzuzjXCf1Krz7GCf1Krz7GS40BzuzjXCf1Krz7
GHrSo3GJ8S40BiNXzuzjXCf1KrzDAQAB"

如果你有申請Google服務，必然可以在你的DNS紀錄上看到類似這樣的一排設定，這意思就是當有外部單位跟你巡查google._domainkey時，DNS就會回傳那一大串加密文字，而這串加密文字即是Google提供給你放置在DNS記錄內的，用以驗證你的確可以管轄（修改）網域的相關資訊

設定在集中系統，要把google._domainkey擺在FQDN欄位，然後把要求的字串內仍貼到RDATA欄位內（注意不要加上雙引號）

新增正解記錄(RR, Resource Record)

Record Type:

FQDN:

TTL: 秒

RDATA:

如RecordType為:

A: RDATA請輸入IPv4 Address.

AAAA: RDATA請輸入IPv6 Address

MX: RDATA輸入之名稱不可用CNAME設定出來的, 須Server只文字網域名稱

CNAME: FQDN之名稱不可用在NS, MX等記錄之RDATA

有關SRV的設定說明

文後補充其一：設定DNS CAA紀錄

當DNS建置之後，除了負責名稱解析的基本功能之外，上述的幾項功能，其實也在連帶告訴我們DNS設置的重要性，也就是信件或服務轉送的功能，以及網域的安全驗證功能上

隨著對網頁安全的提升，在2019年春季，全世界有一半以上的網站已經採用預設https的加密連線，甚至強制將過去http的標準連線也轉為https連線形式，畢竟提供使用者資料上的安全，也是網路連線傳輸當中非常重要的課題



世界上採用https作為預設連線的網站比例(來源 W3Techs.com)

在檢驗網站的安全性是否穩定的機制上，有一個基本的也是重要的檢驗方式，稱之為DNS CAA

首先要帶入一個基本概念，為什麼https連線是比較安全的機制？

這絕對不是因為https走 443 port, 而傳統http走80 port這麼單純而已, port號只是一個進出的管道, 重點是在傳輸的內容上, 傳統http傳輸的內容是沒有經過加密的, 這意味著如果你在網路瀏覽的過程中被截聽, 傳送的內容將會一覽無遺, 當然這包含你的瀏覽紀錄, 連帶帳號密碼以及對話紀錄等等, 而https則是將你的傳送或瀏覽內容, 將進行加密包裝之後再派到網路傳送, 即使被截聽, 也絕對不是那麼容易就被破解, 如果你把自己的網站安全驗證等級提升到一個層次, 那麼被破解的可能性幾乎可以說是不可可能的任務

然而網站是否安全, 是否能以https的形式進行加密傳送, 並不是你自己說了算, 而是必須要製作所謂的數位驗證, 也就是所謂的憑證, 然後請瀏覽你網站的人安裝好這份憑證, 這樣就可以達成雙方的安全連線工作

但是你會發現這樣實在太麻煩了, 總不能我跟某個網站連線就得安裝它的憑證在我的瀏覽器裡面, 這樣我如果跟一百個不同的網站連線還得了? 所以我們有了另一個變通的方法, 請第三方協助製作驗證, 只要我可以跟第三方申請憑證, 那麼這個安全連線就可以被認為值得信賴

這個做法有一個非常大的缺失, 因為世界上可以作為第三方驗證的機構實在是太多了, 我可以跟任何一家提出申請, 不表示其他想盜用我機構身分的人不會透過其他第三方機構闖關, 換言之第三方機構提供了憑證的安全機制, 卻也連帶產生了被有心人士盜用的另一種漏洞

那麼怎麼解決這個困擾呢？當然還是要靠DNS來幫忙啦！因為全世界只有你可以管轄所屬機構的DNS紀錄，所以如果你知道你的第三方憑證是向誰申請的，而且你也把它登記在你的DNS記錄內，自然儘管廣大的第三方憑證機構再大再多，也沒有辦法再接受任何人的憑證申請了，因為第三方憑證機構透過你的DNS紀錄知道，你已經有申請憑證了，這個驗證機制就稱之為DNS CAA(Certification Authority Authorization)

相較於已經快速發展出來的 https連線規範，DNS CAA出乎意料的進度緩慢，採用DNS CAA驗證的網站，在前十五萬個熱門網站當中的比例不到10%，顯見極大多數的機構仍然高度信賴第三方機構設置憑證的機制，但第三方機構派發憑證的作法確有安全疑慮與漏洞，我們必須自我防衛，避免設置安全機制反而白忙一場

目前在市網中心的DNS集管設定當中還沒有辦法在線上設定DNS CAA機制，但是這部分已經請相關的老師處理，相信很快就能加入

至於如果你想在現有的BIND內設定DNS CAA，可以參考這篇文章進一步了解如何設定（前提是你已經完成網站的https第三方憑證申請）

<https://ezbox.idv.tw/112/dns-caa-protoc-ssl-tls-certificate/>

反解設定說明

相較正解設定，反解幾乎沒有多少需要刻意指定或設定的部分，因為它的功能就真的很單純：將指定的IP對應回網域名稱

此外，當你在指定正解的IPv4或IPv6紀錄時，集管系統就已經完成反解的對應紀錄，所以當你去檢視反解紀錄時，應該早就全數建置完畢了

跟正解紀錄比較不一樣的地方是 反解紀錄會根據IPv4或IPv6分成兩個區塊設定，但你仍然可以分項確認看看



點選IPv4的反解紀錄，會看到第一個欄位並不是標準的IPv4格式

+ IP:210.243.35.0/24, 反解:35.243.210.in-addr.arpa.

FQDN	TTL	Type	RData	
11.35.243.210.in-addr...	14400	PTR	www.lmjh.tp.edu.tw.	  
2.35.243.210.in-addr...	14400	PTR	wlog.lmjh.tp.edu.tw.	  
1.35.243.210.in-addr...	14400	PTR	dns.lmjh.tp.edu.tw.	  
3.35.243.210.in-addr...	14400	PTR	w2.lmjh.tp.edu.tw.	  
4.35.243.210.in-addr...	14400	PTR	schoolday.lmjh.tp.edu.tw.	  
5.35.243.210.in-addr...	14400	PTR	wp.lmjh.tp.edu.tw.	  
6.35.243.210.in-addr...	14400	PTR	cooc.lmjh.tp.edu.tw.	  
7.35.243.210.in-addr...	14400	PTR	blog.lmjh.tp.edu.tw.	  
8.35.243.210.in-addr...	14400	PTR	reading.lmjh.tp.edu.tw.	  
10.35.243.210.in-addr...	14400	PTR	...	  

如果仔細觀察，就會發現這些數字被刻意顛倒過來排列，比方說

11.35.243.210.in-addr.arpa. IN PTR www.lmjh.tp.edu.tw.

數字的部分必須倒回來看，也就是說這筆反解紀錄指的是
www.lmjh.tp.edu.tw 是 210.243.35.11

在BIND的設定當中，可以利用\$ORIGIN這個變數指定較為恆定的內容，讓你整個設定的內容較為簡潔，比方說改成這樣的內容

```
$ORIGIN 35.243.210.in-addr.arpa.  
11 IN PTR www.lmjh.tp.edu.tw.  
2 IN PTR wlog.lmjh.tp.edu.tw.
```

這樣設定的本意就跟以下設定的內容是一樣的

```
11.35.243.210.in-addr.arpa. IN PTR www.lmjh.tp.edu.tw.  
2.35.243.210.in-addr.arpa. IN PTR wlog.lmjh.tp.edu.tw.
```

可以看得出來簡潔很多，而且也不容易在未來不小心打錯數字或內容

IPv6的部分只有一點稍微需要強調，就是數字的部分除了反序擺放以外，還會改造成每一個數字都被隔開

