

## UTM / UTM 系列报导

何谓『FQDN』。

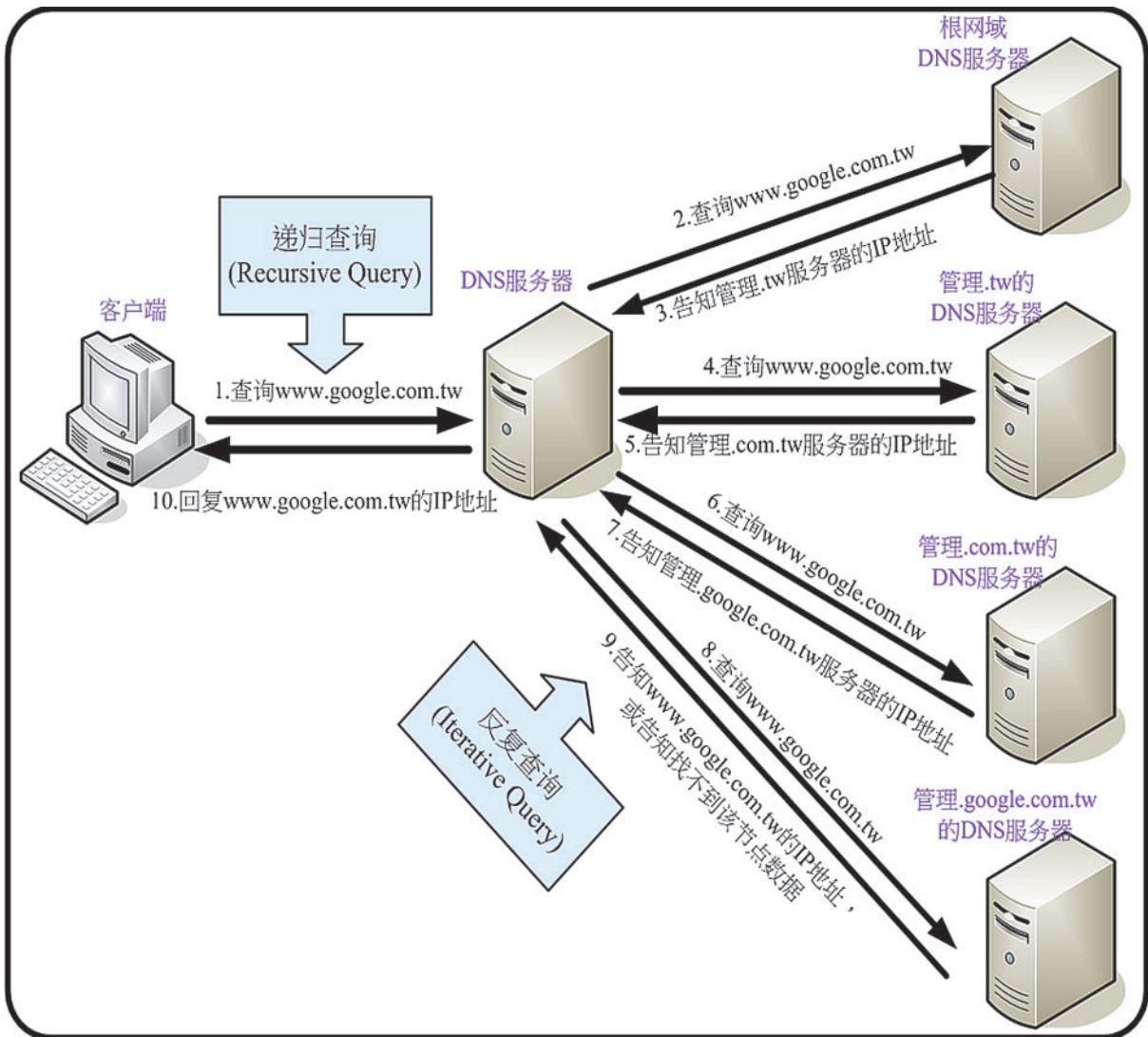
随着因特网的发达，多元的网络功能，为生活带来便利，导致生活型态的转变。便利的网络生活，使得人民对网络越来越依赖，举凡：实时新闻、网络购物、交友、求职…等网络行为。这些行为则在网络世界中透过TCP/IP通讯协议来沟通，并利用IP地址辨别在因特网的每台计算机，就像是人类使用的身分证；但IP地址多达12位数，不符合一般人的记忆方式，因此，为方便使用者容易记住因特网的地址，产生了网域名称(Domain Name)对应的概念；例如：使用者要连上google的网站，不需记住72.14.203.99这组难记的IP地址，只需记住其『完整网域名称』www.google.com.tw就可对应。

何谓『完整网域名称』(Fully Qualified Domain Name, FQDN)？

『FQDN』是由『主机名称』+『网域名称』+『.』所组的URL。从『FQDN』中所包含的信息可以看出主机在「网域名称」树状结构中的位置。例如，www.ncyu.edu.tw，其中www是网页服务器的主机名称、ncyu.edu.tw为网页服务器所在的网域名称；但是，其网址『www.ncyu.edu.tw』还不算是FQDN，真正标准的『FQDN』应该是『www.ncyu.edu.tw.』，就是多了最后的那一点，才成为标准『FQDN』。最后这一个『.』代表在DNS架构中的根网域(Root Domain)，所以输入网址时可省略最后这一个『.』(因为大部分网络应用程序解读名称时，会自动补上『.』，以方便我们使用)。还有，整个『FQDN』的长度不得超过255个字符(包含『.』)，以及不管是主机名称或是网域名称，都不得超过63个字符。

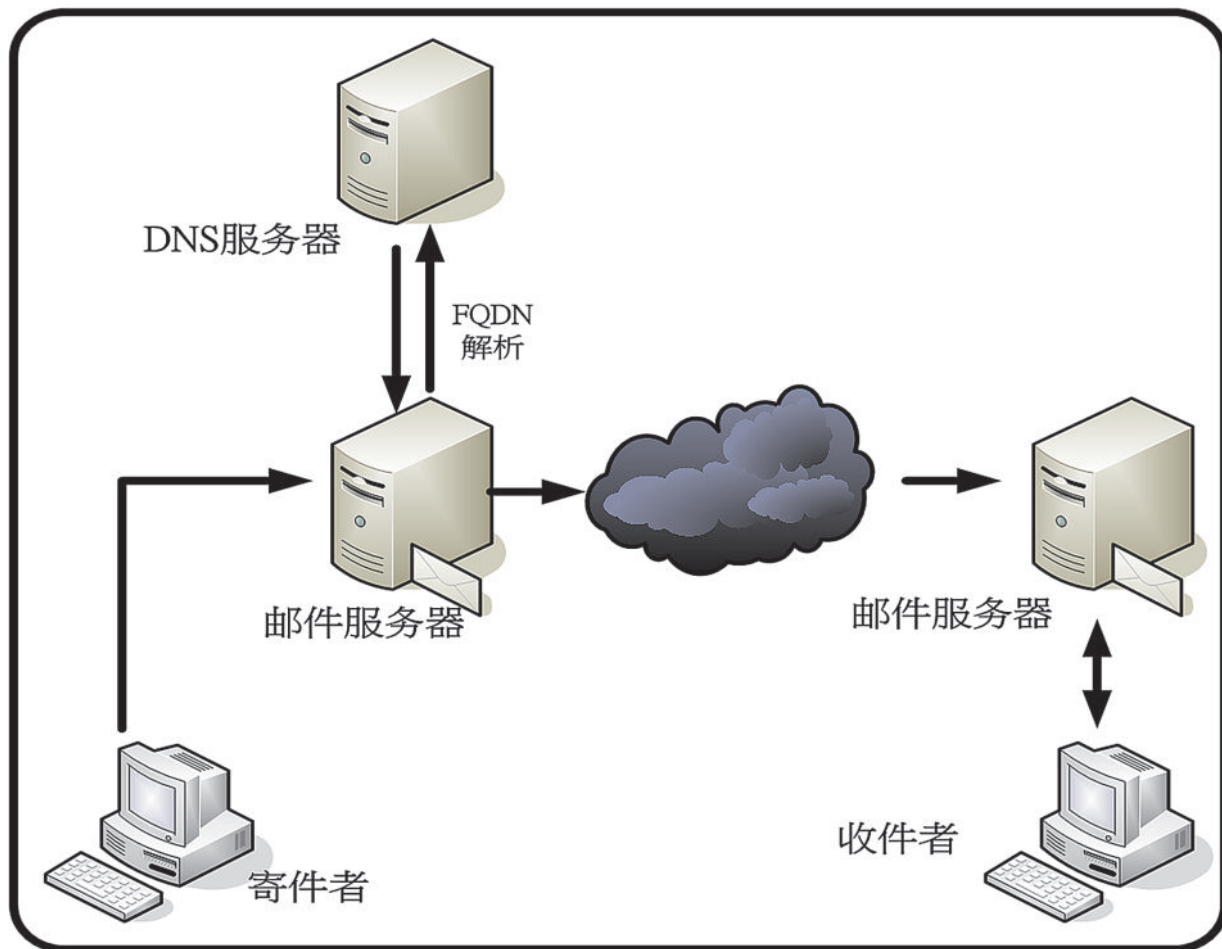
因特网中是透过何种机制将『FQDN』解析为IP地址，这种机制称之为网域名称系统(Domain Name System; DNS)，由DNS Server和DNS Client所组成；主要的目的是『FQDN』与IP地址间的转换。『FQDN』与DNS有下列二项重要关系：

1. 使用者浏览某个网站：计算机使用者在浏览器的网址列输入此网站之『FQDN』后，DNS客户端会向DNS服务器要求查询此『FQDN』的IP地址，而服务器则会去对照其数据库内的数据，并将IP地址回复给客户端。但若没查到，就会发生「DNS Not Found」的情形。所以，一旦DNS Server当机，就如同路标被毁坏，不知将资料送往何处。其运作原理如图1：



图一 解析网站FQDN的运作流程

2. 使用电子邮件寄送/接收：电子邮件就使用『FQDN』作为收信者的电子邮件地址，以 `simking@yahoo.com.tw` 为例，其中收信者的名称为 `simking`，而 `@` 符号后面是邮件服务器的『FQDN』。因此，客户端使用 Outlook Express (MUA) 撰写一封信，将送至所属的邮件服务器 (MTA)，而 MTA 先将此信件暂时存放在队列 (Queue) 中，且会检查信件目的地，并向 DNS 服务器要求查找收件者『FQDN』的 IP 地址，则利用 SMTP 通讯协议将邮件传送到此收件者的所属邮件服务器，收件者即可利用 POP3 或 IMAP 的通讯协议至所属的邮件服务器下载或直接读取邮件。其运作流程如图 2。




图二 邮件『FQDN』解析的运作流程

然而，也因为『FQDN』所拥有的便利性，受到大众的喜爱，新软系统同样注意到这份需求，秉持着不断求新与满足使用者需求的理念，近期于『UTM』与『MHG』系列中所内建之「外部网络地址表」功能里，在IP地址范围字段中新增『FQDN』机制。此机制常用在拥有多个IP的网站，如：“facebook”、“yahoo”…；像“facebook”同时使用了多组IP（如：69.171.228.14、69.171.224.39…）。而且管理人员于『FQDN』字段中填入目标网站的「主机名称+网域名称」，若网址为「<http://www.facebook.com/#!/profile.php?id=1055205>」的网站则于『FQDN』字段中填入「[www.facebook.com](http://www.facebook.com)」即可，操作画面既容易又简单，如图3。



图三 外部网络地址表填入目标网站的『FQDN』

除了『FQDN』功能外，在「UTM/ MHG」系列中『网站黑/白名单』、『网站类别数据库』功能亦也可以达到禁止或允许存取特定网站的目的，但这两个功能主要是针对HTTP在运作，像是FTP、HTTPS…这些仅次于HTTP的常用网络服务就鞭长莫及了。所以在以往，这些管理上的缺口必须透过IP、网段…方式再封锁。而这种封锁方式相对麻烦，也因部分网站同时拥有多个IP，极易造成有遗漏的情况发生。因此，管理人员于系统之『外部网络地址表』功能，设定禁止或允许存取特定网站的『FQDN』，再于管制条例中套用并可防止这些种种情况发生。

文  余光明 kongmeng@nusoft.com.tw