行政院國家科學委員會專題研究計畫　期中進度報告

一個整合的智慧型 DNS 管理平台(1/3)

計畫類別： 個別型計畫
計畫編號： NSC92-2213-E-009-099-
執行期間： 92 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立交通大學資訊科學學系

計畫主持人： 曾憲雄

計畫參與人員： 王慶堯，蔡彥興，鄭佩琪，陳家瑜

報告類型： 精簡報告

處理方式： 本計畫可公開查詢

中　華　民　國 93 年 5 月 24 日

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ **一個整合的智慧型 DNS 管理平台** ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　　□整合型計畫
計畫編號：NSC 92—2213—E009—099
執行期間：92 年 8 月 1 日至 93 年 7 月 31 日

計畫主持人：曾憲雄教授

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊科學系

中　華　民　國　　　年　　　月　　　日

一個整合的智慧型 DNS 管理平台

A Unifying Framework for Intelligent DNS Management

計畫編號：NSC 92-2213-E009-099
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日

主持人：曾憲雄　　國立交通大學資訊科學系
計畫參與人員：王慶堯, 蔡彥興, 鄭佩琪, 陳家瑜
國立交通大學資訊科學系

一、 中文摘要

DNS 在目前網際網路軟體的基礎建設中占有很重要的地位；然而，由於 DNS 系統的分散式架構特性，我們常會發現網路上有很多運作不當的 DNS 伺服器 (例如: 錯誤的設定，不適當的規劃等等)。基本上，DNS 的問題不僅複雜，而且這些問題會隨著不同的網站而有不同的結果。再者，由於 DNS 伺服器的重要性，目前直接或是間接攻擊 DNS 系統的網路攻擊也日漸頻繁。實務上，很多 DNS 相關的規劃或是管理議題, 管理者都需要具備相關的專業知識才能夠改善目前的 DNS 系統。然而，對於大部分沒有經驗的管理者來說，這是很難達成的目標。

在本計劃中，我們打算設計並且實作一套統一架構 (例如: 包括設定，規劃與管理，教學系統等等) 的智慧型 DNS 管理系統，透過 Web 介面及專家系統的技術來幫忙經驗不足的管理者，讓他們的 DNS 系統可以運作地更好。我們提出的研究中將會包括問題分析以及大部分的 DNS 管理者會遇到的問題，並進而找出 DNS 輔助系統該具備的功能，以便能夠幫忙 DNS 管理者解決這些複雜的問題並減輕負擔。透過專家系統的技術，專家的知識可以被擷取出並且存到知識庫中。為了讓 DNS 的相關知識可以被其他系統所分享或是再用，我們計劃設計並且建造 DNS-ontology, 以及在專家系統的開發過程中引入物件導向模型。

英文摘要(Abstract)

The Domain Name System (DNS) is an essential part of the Internet software infrastructure. However, due to the complex and distributed nature of the DNS system, we could often find lots of poorly performed DNS servers (i.e. by mis-configuration, inappropriate planning, etc.) on lots of Internet sites. Some latest DNS survey showed that nearly 70% of the DNS servers of commercial sites (e.g., ".COM" Zones) have some configuration errors. Furthermore, given the importance of DNS servers, direct or indirect attacks on the DNS systems are common.

The DNS is a special kind of distributed directory service for people to create and access the network information systems by (1) allowing local control of its segments; (2) making each segment's data available to Internet using a client-server scheme. However, few administrators have the expertise to do the jobs well since this distributed mechanism is a double-edged sword; it allows DNS to scale to Internet size, but it also allows for incredible mis-configurations.

DNS problem domain is rather complex and varies greatly on different sites. Novice administrators or administrators that manage a small scale of network usually do not know the theoretical and practical knowledge of DNS system very well. Besides, there are many planning and management issues that need expertise for administrators to improve the DNS system. However, this is not an easy job for most inexperienced administrators. On many occasions, it needs the guidance of the DNS domain experts. But, it is a pity that domain experts are so hard to find and cannot always standby for those inexperienced administrators under emergency conditions.

Typically, knowledge based systems (KBSs) are developed to solve very complex problems or even problems which are not entirely understood. By using the expert system technology, the knowledge from the domain experts can be extracted and encoded into a knowledge base. To enable the sharing and reuse of DNS knowledge, we propose to design and build a DNS-ontology and introduce the OOP model for the expert system development.

In this project, we propose to design and implement a unifying framework (e.g., including configuration, outstanding traffic monitoring and analysis, planning and management, tutoring, etc.) for supporting intelligent DNS management using web interface and expert system technology to help inexperienced administrators in insuring the smooth operation of their DNS systems. The proposed study will include an analysis of what problems and difficulties most DNS administrators might encounter and provide the insights into how various DNS assistant sub-systems could be designed and deployed to help solve the complex problems or alleviate these DNS administration job loadings.

二、 計畫緣由與目的

DNS 是一種特別的分散式目錄服務，我們可以透過它的特性 (1)允許每個 DNS 管理它自己區段的資料 (2)允許每個區段用 client-server 的方式來開放資料，開放或是存取位於網路上的資訊系統；然而，因為分散式架構就猶如一把雙面刃，一方面它可以讓 DNS 比較容易隨網際網路規模而調整，另一方面它也造成一些難以致信的錯誤設定。例如在近期國外進行的 DNS 抽樣調查報告[13]中指出，將近 70% 由商業網站 (所謂 「.COM」) 使用的 DNS 伺服器有設定上的錯誤。由此來看，有相當大部分的系統管理者都缺少 DNS 的專業知識來處理 DNS 的問題。

基本上，DNS 的問題不僅複雜，而且這些問題會隨著不同的網站而有不同的結果。再者，由於 DNS 伺服器的重要性，目前直接或是間接攻擊 DNS 系統的網路攻擊也日漸頻繁。實務上，很多

DNS 相關的規劃或是管理議題，管理者都需要具備相關的專業知識才能夠改善目前的 DNS 系統。然而，對於大部分沒有經驗的管理者來說，這是很難達成的目標。在很多的情況，他們需要有 DNS 領域的專家可以提供他們一些建議或是引導，但是很可惜的，在很多緊急的情況下，要隨時找到一個可以提供諮詢的專家是很難的。

在本計劃中，我們將設計並實作一套整合架構的智慧型 DNS 管理系統 (包括設定，網路流量監控與分析，規劃與管理，教學系統等等)，透過 Web 介面來操作並以專家系統的技術來幫忙多數的管理者，讓他們的 DNS 系統可以運作的更好。我們的研究將會包括， DNS 基本問題分析以及大部分的 DNS 管理者會遇到的設定與規劃問題，並進而找出 DNS 輔助系統該具備的功能，以便能夠幫忙 DNS 管理者解決這些複雜的問題並減輕負擔。因此於本計畫中，我們希望以三年三階段完成以下目標：

第一階段(第一年)

1. 分析並找出大部份的 DNS 問題以輔助 DNS 知識的擷取(Knowledge Acquisition) 並進而建立 DNS Ontology
2. 完成 iDNS-MS 的架構設計並開始實作 iDNS-MS 雛型系統(包含 DNS 偵錯跟 DNS 設定子系統)
3. 開始提供 iDNS-MS 網站服務，並且將我們所整理的資料與服務提供給網路使用者以達到知識共享的目標 另外使用者的使用回饋(Feedback) 也可以提供我們更多的使用案例與改進方向。
4. 開始研究 DNS 建置的相關問題。

第二階段(第二年)

1. 完成 iDNS-MS 子系統，並加入 web-service 提供服務 (同時蒐集用戶意見，以利後續分析問題及改進系統功能的參考)。
2. 各個子系統的 problem solving methods 的探討並強化 iDNS-MS 系統各子系統的相互支援。
3. 開始進行 DNS tutoring 子系統的研究課題。

第三階段(第三年)

1. 完成 iDNS-MS Tutoring 子系統，並加入 web-service 提供服務 (同時蒐集用戶意見，以利後續分析問題及改進系統功能的參考)。
2. 完成 iDNS-MS Security 子系統，並加入 web-service 提供服務。
3. 結合國內外相關 DNS 系統安全的研究。嘗試結合 TWMIC DNS 系統弱點分析計畫成果。
4. 進一步進行 DNS 等異常 log analysis/mining 等。

三、 想法與討論

目前坊間雖然有 DNS 相關的書籍，但是對於 DNS 的管理者來說，這些書籍所能提供的資訊往往無法滿足他的需求。例如當 DNS 管理者把 DNS Server 架設起來以後，如果有一些 DNS 的異常狀況、或是因為 DNS 的設置不當而導致 DNS 查詢出現錯誤，這時 DNS 管理者需要的就不單單只是書籍上的知識，更需要的是有 DNS 專家可以就近提供協助。根據統計資料顯示，目前的網際網路中，.商業應用 (例如 .COM) 的 DNS 設定有錯誤，這也導致目前的 DNS 流量因而大量的增加。所以我們希望可以利用專家系統的方法，來建立 DNS 專家系統，以便可以提供任何時間、任何地點 (Anytime, Anywhere) 的服務。

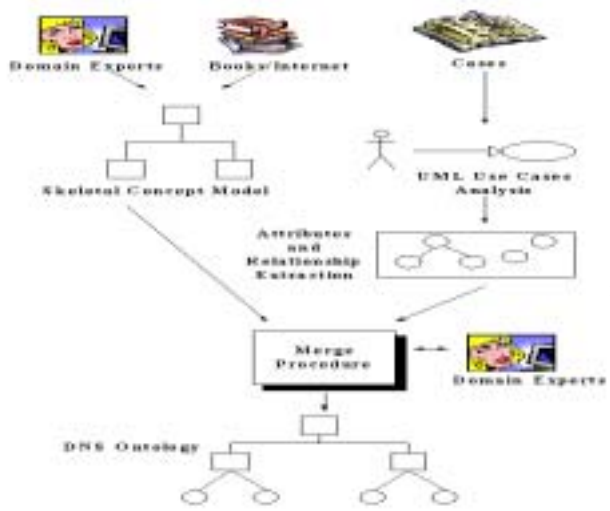
建構 DNS 專家系統，需要先從知識擷取著手；把 DNS 專家的知識透過知識擷取的過程轉換成專家系統的知識表達法並進而建立知識庫。我們提出了一個透過使用者案例分析的分法[4]來達到知識擷取的目標；首先我們先訪談 DNS 專家並且參考相關 DNS 書籍，整理出 DNS 相關的問題分類。在該表格中我們列出了 DNS 重要的議題，例如 DNS 的正確性、安全性、效能等等。

表一. 常見的 DNS 系統設計的問題分類

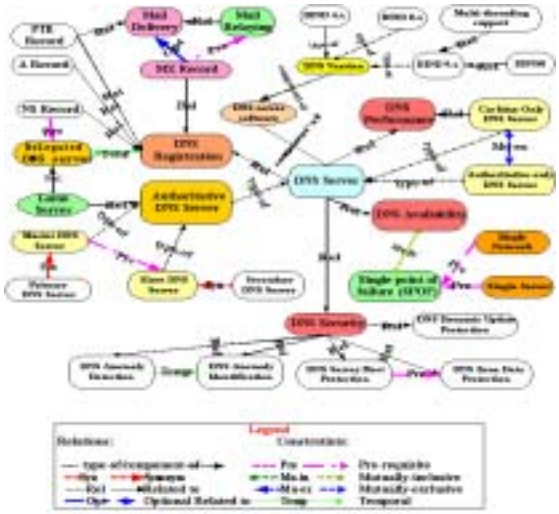
ISSUES	DESCRIPTIONS
1. Correctness	Delegations of domain zones, illegal setting of DNS entries, etc.
2. Availability	Master/slave architecture, data synchronization among authoritative servers, etc.
3. Performance	DNS caching, forwarding, etc.
4. Security	Access control, Dynamic Update, Intrusion detection, etc.
5. Interoperability	BIND, Microsoft DNS, etc.

這些議題可以組成 DNS 管理的大架構；另外我們收集使用者的使用案例，以建立 DNS 管理知識的底層架構，然後再以 Merge 的方式把這兩者知識作一個整合；整個流程如下圖一所示。

經過上述的過程，我們建立了底下的 DNS Ontology；在 DNS 的 Ontology 架構圖中呈現出 DNS 相關的管理議題關係 (Relationship)、特性 (Properties) 以及限制 (Constraints)。



圖一. 知識擷取與匯整的流程式意圖



圖二. DNS Ontology 部分圖示

- 4 種關係:

1. "is_a": 普遍化關係,可以用來描述在 class 階層中的 parent-child 關係; 例如, master DNS server 是一種 DNS server。
2. "Syn": 同義詞關係, 可以用來描述具有相同意義的不同詞。
3. "Rel": 關聯性關係, 可以用來描述具有關聯性的 Ontology concepts; 例如 DNS Server class 跟 DNS Security class 具有相關聯的關係。
4. "Opt":非必須關係, 用來描述非必須的關係; 例如:在 DNS 註冊的時候, MX record 是非必須的, 當 MX record 不在的時候, DNS Server 還是可以透過 A record 來作 mail 的處理。

- 3 種限制:

1. Pre-requisite constraint: 描述事件發生的順序現制。
2. Temporal constraint: 描述事件發生的時間順序現制。
3. Mutually inclusive constraint: 描述兩個事件的依靠性關係。

在專家系統的建制上，我們採用 DRAMA/NORM 專家系統工具；DRAMA/NORM 的物件資料庫型態與 Ontology 的知識型態很接近，有助於我們將 Ontology 的知識轉換成 DRAMA/NORM 知識庫資料；此外，DRAMA/NORM 的 client-server 架構可以讓我們建立 Web 環境的專家系統：

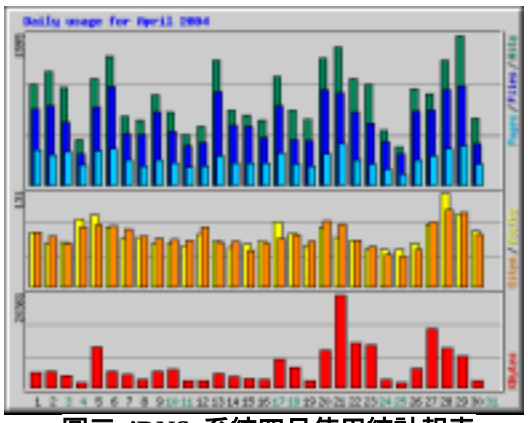
總括來說，目前我們的系統具有底下的特性:

- 利用了專家系統的技術, 除了讓使用者可以簡單的偵測出問題之外, 可以進一步根據使用者的個別需求，透過本實驗室所開發出的 DRAMA/NORM 專家系統來進行推論，並且提供一個最適合使用者 DNS 環境的建議；
- 即使是尚未架設過 DNS 的使用者, 也可以透過簡單的問題詢問方式, 讓專家系統提供一個適合的系統模板 (configuration template)；
- 除此之外，DNS Ontology 的建構也達到知識分享的目標，讓專家的知識可以透過 Ontology 而分享出去，並且可以利用 DNS Ontology 來建構 DNS Tutoring 系統, 建立初學者的正確 DNS 觀念。

四、初步計畫成果自評

在本計劃的第一階段中，我們訪談 DNS 專家，再分析整理出許多重要的 DNS 問題並進而建立出 DNS Ontology 雛型，以及建構出 DNS Ontology 上層的結構;另外從使用者的問題以及網路上的討論區收集到使用案例，透過使用案例分析建立 DNS Ontology 的底層結構；最後結合這兩部分的結構已建立一個比較完整的 DNS Ontology。這部份的成果已經發表了一篇期刊論文[10]。目前該系統也已經提供網路服務 (系統網站是 http://idns-pms.nctu.edu.tw)；下圖三是四月的使用統計圖，平均每天會有 950 hits、70 人次的使用；除此之外，珍對一些系統設計不周全的部份，或是其它的 DNS 問題，使用者也都會透過我們設置的討論區發表意見。希望可以透過該系統解決 DNS 管理者的問題，另外也可以從使用者的使用回饋資料中進而改進系統。

未來在下一階段中, 除了強化目前的系統, 我們將會建立其他 DNS 的子系統 (例如 DNS 教學系統), 讓該系統更加的完整；並且讓這些子系統的功能可以相互支援。



圖三. iDNS 系統四月使用統計報表

五、參考文獻

[1]. Chandrasekaran, B. and Jorn R. Josephson, V. Richard Benjamins. (1999). What Are Ontologies, and Why Do We Need Them?, IEEE Intelligent Systems. 14 (1): pp. 20 - 26.

[2]. C. S. Chen, S. S. Tseng, and C. L. Liu, "A Unifying Framework for Intelligent DNS Management", International Journal of Human - Computer Studies, Vol. 58/4, pp 415 – 445.

[3]. Chen, C.S., Tseng, S.S., Liu, C.L. (2002b). A distributed intrusion detection model for the domain name system. Special Issue on Parallel and Distributed Systems, Journal of Information Science and Engineering, Vol.18, pp.999-1009.

[4]. Chen, C.S., Tseng, S.S., Liu, C.L., Ou, C.H. (2002c). Building a DNS ontology using METHONTOLOGY and Protege-2000. To appear in Proceedings of 2002 International Computer Symposium Workshop on Artificial Intelligence, Dec. 18-21, 2002 .

[5]. Evi Nemeth, Nevil Brownlee “DNS Damages – Measurements at a Root server“, CAIDA at the North American Network Operators' Group (NANOG) meeting, February 2002

[6]. Fernandez, M.L. (1999). Overview of methodologies for building ontologies. In Proceedings of the IJCAI-99 Workshop on Ontologies and Problem-Solving Methods: Lessons Learned and Future Trends. CEUR Publications.

[7]. Gaines, B.R., and Shaw, M.L.G. (1993). Eliciting Knowledge and Transferring it Effectively to a Knowledge-Based System, IEEE Transactions on Data and Knowledge Engineering, 5(1), pp.4-14.

[8]. Hanley, Sinead. "DNS Overview with a discussion of DNS Spoofing." 6 Nov. 2000. URL: http://www.sans.org/infosecFAQ/DNS/DNS.htm (9 Feb. 2001).

[9]. Koh, J.L. (2001). Recent Developments and Emerging Defenses to D/DoS: The Microsoft Attacks and Distributed Network Security. SANS Institute, URL: http://www.sans.org/infosecFAQ/DNS/developments.htm.

[10]. Liu, C.L., Tseng, S.S., Chen, C.S. (2004). Design and Implementation of an Intelligent DNS Management System. (To appear in Expert Systems With Applications, September 2004)

[11]. Man-Mice Company. (2002). Domain Health Survey for .COM - August 2002, http://www.menandmice.com/6000/61_recent_survey.html

[12]. MOECC, Taiwan. (2001). Network Traffic Statistics on TANet, MOECC Newsletter (2001), URL:http://www.edu.tw/moecc/art/brief.htm.

[13]. Musen, M.A. (1992). Dimensions of knowledge sharing and reuse, Computers and Biomedical Research. 25, pp.435-467.

[14]. Ou, C.H. (2002). Design of An Intelligent DNS Planning and Management System, Master Thesis, Dept. of Computer and Information Science, National Chiao-Tung University, Taiwan

[15]. Shadbolt, N., O'Hara, K., and Cottam, H. (2000). The Use of Ontologies for Knowledge Acquisition. In: J. Cuena, et al., (eds) Knowledge Engineering and Agent Technology. IOS Press, Amsterdam.

[16]. Sugumaran, V., Storey, V.C., (2002). Ontologies for conceptual modeling: their creation, use, and management, in Data & Knowledge Engineering, Vol 42, p.251-271