

建置校園可擴充之輕量化網路身分認證系統：以交通大學為例

林明樺 陳昌盛 王英鼎

交通大學資訊技術服務中心

{ mhl, cschen, pcbug } @mail.nctu.edu.tw

摘要

本論文旨在探討交通大學使用 Nullpop[1]程式建置校園跨平台之輕量化網路身份驗證系統的開發經驗與維運成效。本研究的主要發現與貢獻，歸納如下：(1)提供高效率的認證服務：新建輕量化 Nullpop 認證系統，簡化第一步的登入驗證(除去了原先 e-mail 信箱處理的工作)，大幅減少等待時間，讓使用者在使用線上服務時，可立即獲得登入是否成功的結果；(2)建立可調整的多源(multi-source)認證系統：原先僅能以特定 e-mail 系統之 POP3[2]伺服器(單一來源)的帳號資料，作為身分認證，但在導入新建的 authentication proxy (nullpop 系統)後，我們修改認證處理流程為詢問後端帳號資料庫的方式，並進一步利用資料庫同步處理，可接受多個不同資料來源(包括自動與手動建立)，整合跨平台之特定類別的帳號；(3)建立身分差別化網路服務：新建系統可有效控管各服務所允許的使用者身份(例如，在學、已畢業等)，對線上服務的使用資源分配上更趨制度化。

關鍵詞： Nullpop、Authentication proxy、MySQL 資料庫

Abstract

This paper aimed to explore the issues on developing a light-weighted, hybrid authentication service for providing students with different services on various network systems. In this paper, we had developed a use case modeling of the authenticating system and conducted a series of experiments to study the performance and effectiveness of this approach. The major findings are as follow: (1) we had developed a light-weighted, nullpop authentication service which greatly reduced login processing time; (2) the new established system had been enhanced with a multi-source database approach (including both manual adding and auto-sync capability); (3) the new established system could provide different kinds of users with differential services.

Keywords: Nullpop、Authentication、MySQL

1. 前言

本論文旨在探討交通大學(以下簡稱交大)使用 nullpop 程式建置校園跨平台之多源(multi-source)、輕量化網路身份驗證系統的開發經驗與維運成效。在 TANet 各校的網路環境中，使用 e-mail 帳號以 POP3 作為多項網路服務的認證方式(例如無線網路跨校漫遊)，已經行之有年，是一種很方便的網路服務建置模式。另一方面，隨著國際化的潮流，過去幾年間，許多學校逐漸採行保留畢業校友 e-mail 帳號的政策，以利畢業校友維繫同學間以及校友與學校的情誼。隨著時間的推演變化，各校畢業校友人數的累積以及校園網路環境的變遷，上述的政策考量，也逐漸對許多單位原先的網路系統維運，產生諸多行政管理以及維運技術上的衝擊。

基本上，因校園內師生在職在學期間通常都會申請一組校內 E-mail 帳號，以供電子郵件往返使用，故電子郵件帳號即可用做身分認證帳號使用，例如交大目前已經有多項與學生相關的網路服務(包括宿舍網路、無線網路、SSL-VPN、電腦教室 NAT、校園軟體授權[3]等)，是採用 POP3(校內 D2 e-mail 帳號)認證。如圖 1(左半邊)，交大學生用戶要使用前述網路服務前，必須通過登入認證，方式是透過網路設備後端的 Radius Server[4]詢問學生 E-mail POP3 Service，再由 Radius Server 判斷 POP3 Service 回應的帳號密碼是否正確，進而回傳給服務是否允許登入。

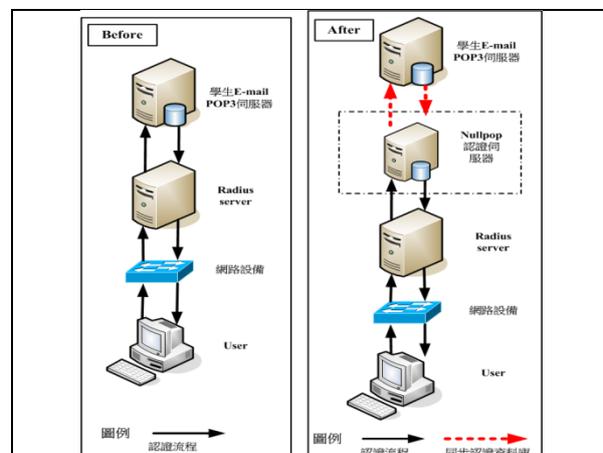


圖 1 導入 Nullpop 前後之網路認證系統架構對照

然而，2011年中，因為短時間內多起校園資安事件(大量 SPAM 以及宿舍電腦中毒產生攻擊校內網路系統)，造成當時學生 E-mail 系統在處理 E-mail 工作時遭受暴力猜測帳號密碼的攻擊，以致系統負載繁重，再者多數校友的 E-mail 帳號於畢業後即不再使用，常被有心人士盜用來作為登入網路服務使用，增加相關系統資訊安全上的風險，進一步也影響其他透過 e-mail 系統驗證的校園宿舍網路、無線網路、SSL-VPN、電腦教室 NAT、校園授權軟體 (CA) 等服務的登入驗證，造成上述網路無法使用的窘境。

目前交大學生網路服務認證系統乃同步學生 E-mail (NCTU-D2) 帳號，在校方保留校友 E-mail 帳號的政策下，學生 E-mail 的帳號累積至今已將近 5 萬多筆，且每年持續增加中。其次，在許多實務的管理經驗中，我們也發現以往各網路服務直接詢問學生 E-mail POP3 帳號時，無法有效地區分出不同身分(例如，在學、休學、或畢業學生)的帳號，以致學生畢業後成為校友，舊的學生 E-mail 帳號，仍可用來使用校方提供的多項網路服務，造成資源配置不合理以及管理上的漏洞。有鑑於此，如圖 1 的右半部所示，我們評估之後，乃決定另行利用 nullpop 程式建置一套輕量化 POP3 Service (Nullpop)，提供高效能與高度帳號擴充彈性的 POP3 帳號驗證系統，以提供需透過 E-mail 帳號作為認證的服務使用。

為驗證目前學生 POP3 server 與 Nullpop 系統在處理效能上的差異，我們由學生 POP3 伺服器上隨機選出 100 組使用者帳號與密碼資料，利用這些帳號與密碼分別以 POP3 協定連線學生 E-mail POP3 與 Nullpop 系統，並紀錄程式每一筆連線完成的時間。根據前述紀錄，由於學生帳號上的 e-mail 信箱大小以及數量不同等因素，透過一般 e-mail 系統 (POP3) 登入的時間差異較大(數秒到接近 100 秒上下)，相對而言，透過 nullpop 的連線，完成登錄的時間幾乎都在 0.02 秒左右，粗估約有 100 到 1000 倍的差距，相當明顯。相關內容，我們將在論文的後面實驗與討論部分，加以詳細說明。

本研究的主要發現與貢獻，歸納如下：(1) 新建輕量化 Nullpop 認證系統以提供高效率的認證服務：簡化第一步的登入驗證(除去了原先 e-mail 信箱處理的工作)，大幅減少等待時間，讓使用者在使用線上服務時，可立即獲得登入是否成功的結果；(2) 建立可調整、可擴充的多源(multi-source)認證系統：原先僅能以特定 e-mail 系統之 POP3 伺服器(單一來源)的帳號資料，作為身分認證，但在導入新建的 authentication proxy (nullpop 系統) 後，我們修改認證處理流程為詢問後端帳號資料庫的方式，並進一步利用資料庫同步處理，可接受多個不同資料來源(包括自動與手動建立)，整合跨平台之特定類別的帳號；(3) 建立身分差別化網路服務：新建系統可有效控管各服務所允許的使用者身份(例如，在學、休學、已畢業等)，對線上服務的

使用資源分配上更趨制度化。

2. 研究動機及背景說明

2.1 設計考量-校園線上網路服務認證方式

現今網路服務的提供者，在開放服務供使用者使用的當下所要思考的幾個關鍵問題：

1. 適用對象:思考所要服務的對象是誰?
2. 有效的驗證機制:如何確認上線的使用者就是符合明確規定合法的使用者?
3. 系統規劃彈性:能否彈性調整適用對象(身分差異化服務)?
4. 效能問題:能否隨需求成長，調整系統配置規劃?

在前 2 點的需求下，身分認證就成為使用服務的最初步驟，目前常見的身分認證方式有身分證、Smart Card、憑證與帳號密碼組合等。實務上，帳號和密碼的搭配性組合是目前最常使用的登入驗證方式，在登入服務之前驗證合法使用者才知道的帳號與密碼，可確保網路服務使用的過程中，就是可被允許的登入使用者。由於資訊技術發展等歷史因素以及資訊安全、經濟考量等因素，在帳號認證的需求下，亦衍生出多項認證機制供需要做認證的服務採用，最常見的有：NIS Server[5]、LDAP Server[6]、Radius Server、AD Server 等，登入帳號的資料來源常見的亦有：NIS Database、LDAP、POP3、AD 等。另外，針對上述第 3 與第 4 點，我們將在本論文的第三與第四節加以詳細說明與討論。

2.2 研究動機 - 導入輕量化的 nullpop 服務

在本小節中，我們將針對利用標準 POP3、nullpop 以及 LDAP 作為網路身分驗證系統的適用性，分別做一組簡單的對照比較與說明(參見表 1 和表 2)。

本研究中，為了思考解決當時 E-mail POP3 Server 除須正常負責 E-mail 收信服務外，在遭受網路攻擊(如暴力猜測帳號密碼)時，會造成 POP3 Server 在處理這些 Session 下會延後回應網路服務 RADIUS 的 POP3 詢問，在 RADIUS 等待回應時間內未收到 POP3 Server 的正確回應後，即造成登入失敗使用者便無法正常使用網路服務。因此，當時評估之後決定把網路服務認證用的 POP3 Server 分割出來。其次，考量 POP3 要能夠快速回應的效能，遂選用 Nullpop 做為認證用 POP3 Server。

表 1 是傳統 POP3 服務與 Nullpop 服務的簡單比較。Nullpop 是一種簡化式的 POP3 Service，在登入後僅檢查帳號與密碼是否正確，可提供使用者登入驗證之用，無回報 E-mail 信件數量與內容的功能，故在回應 POP3 詢問時速度可比一般正常服務的

POP3 Service 還快速，如果單做為認證用途，是一個相當好用的工具。

表 1 一般 POP3 Service 與 Nullpop Service 比較表

POP3 Service	一般 POP3	Nullpop
驗證登入帳號	是	是
具回傳 E-mail 資訊功能	是	否
系統耗用資源	較多	較少
處理時間	較長	較短

由於我們希望進一步能夠針對不同的使用者作差別化的管理 (在校生、休學生、預修生、外籍新生、畢業未離校、畢業校友等)，我們決定另外改良認證方式，修改成將認證帳號與密碼資料放入網路資料庫的方式來進行，並且可分別從多個不同的帳號來源 (包括學務處、教務處、資訊中心等) 取得身分證號資料，並加以區隔，以利吾人對校園網路資源做合理有效地運用。

2.3 Radius 主機

RADIUS (Remote Access Dial In User Service) 是一種集 AAA (Authentication、Authorization、Accounting) 三種服務協議為一身的網路傳輸協議，針對服務 (主機、設備) 提出的驗證或計費要求對使用者進行驗證或計費後回應結果。目前交大線上服務僅使用到 RADIUS 的驗證功能，進行身分的認證，並不使用計費的功能。

3. 研究方法

本研究所建置的可擴充性認證系統 (Nullpop) 旨在改善目前透過 POP3 做為認證的網路服務在遇到 E-mail POP3 Server 忙碌時無法正常認證成功的問題，並且提供資料庫式的帳號儲存方式，可彈性的透過資料庫同步帳號資料達到擴充的功能，透過資料庫進行資料的處理，可應用在不同需求上，如目前的 Nullpop 系統可提供在學學生 E-mail 帳號資料庫，與在學學生含校友的學生 E-mail 帳號資料庫，透過資料庫的處理，分離出兩種不同身分的帳號資料庫供需求的服務使用，彈性設計出符合使用需求的認證系統。

3.1 Nullpop 驗證運作流程

圖 2 表示交大 Nullpop 驗證運作流程。交大於校園內外提供的多項網路服務，在使用前須確認使用者身份，由各線上服務系統提供使用者登入畫面，讓使用者輸入用戶身份資訊 (帳號、密碼、驗證碼等)；其中，帳號與密碼資訊會透過後台的 RADIUS Server，視使用者輸入的帳號格式來選擇詢問教職

員 E-mail POP3 伺服器或學生的 Nullpop 系統，學生帳號與密碼由 RADIUS 以 POP3 協定連線 Nullpop 系統，由 Nullpop 查詢本機上學生資料庫後判斷帳號是否存在 (在學與否) 與帳號與密碼是否正確，最後結果回覆給 RADIUS，由 RADIUS 告知線上服務所登入的帳號是否認證成功，是否可允許使用者登入使用。

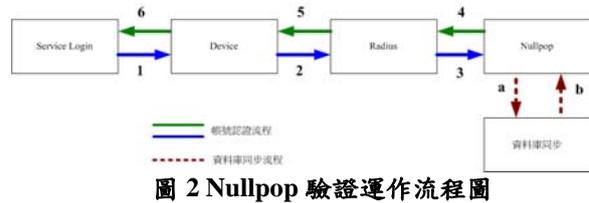


圖 2 Nullpop 驗證運作流程圖

3.2 交大現有 Nullpop 系統之整體架構

如圖 3，目前交通大學幾個常見的學生校園網路服務的認證系統架構大致分成四層，從用戶端開始，經由網路設備端，然後再到認證詢問層 (通常為 Radius 伺服器；備註 1)，再到認證帳號所在的 Nullpop 系統。此時，Nullpop 主機則負責檢查 POP3 帳戶中的帳號密碼是否正確，因僅查詢帳號密碼，不會去檢查 POP3 的 Mailbox，故可快速的回應各服務的 RADIUS 帳號密碼驗證是否正確。

- 備註 1: 如圖 3，部分應用 (如本校「電腦教室認證」與「校園授權軟體認證」系統)，經蒐集使用者認證後直接詢問 Nullpop server (並未經由網路設備服務代轉認證訊息)。

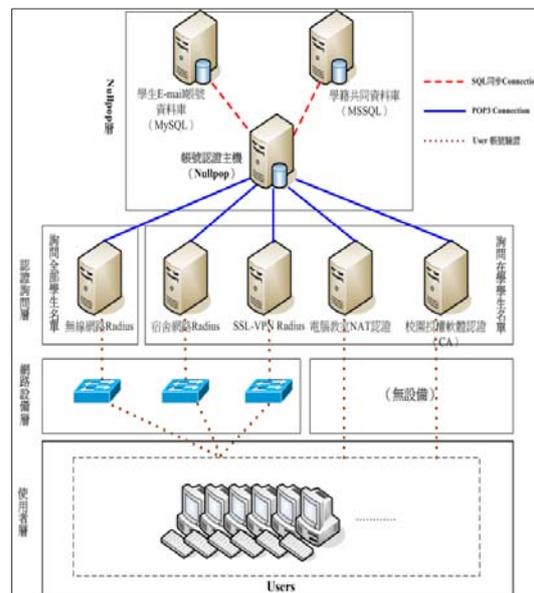


圖 3 交大學生網路服務驗證系統之整體架構

3.3 系統分析-主要功能之案例圖

如圖 3 (架構圖) 與圖 4 (案例圖) 所示，交大 Nullpop 系統除了建置 Nullpop 程式處理 POP3 連線外，還加上資料庫系統處理與儲存帳號資料。首先，

才執行程式，否則不去執行同步資料庫的動作，確保程式執行期間僅只有一個 Session 在處理，避免因其它因素在程式同步資料庫後造成資料庫資料的錯誤，

- (3).再來檢查連線學籍共同資料庫後是否有資料存在，如資料數大於 0 筆才開始進行資料同步，以確保程式不會因連線上的問題而清空資料庫內資料，最後同步回在學學生的學號資料，並且把程式 pid 欄位的值改成 0，待下次程式執行前檢查用。

二、在學與非在學 E-mail 帳號同步程式：

- (1).同樣的，在開始進行同步之前，會先檢查資料庫中的程式 pid 值是否為 0，如非為 0 即程式結束不作任何動作。
- (2).如資料庫 pid 值=0，隨後取出程式執行的 pid 值更新資料庫中的 pid 值。
- (3).利用 MySQL join 在學學生資料表與學生 E-mail 帳號資料表--先刪除已不是在學生資料表中的學號(即離校)對應的學生 E-mail 帳號，之後加入新增於在學生資料表中的學號(即新進)對應的學生 E-mail 帳號，並且把程式 pid 欄位的值改成 0，待下次程式執行前檢查用。

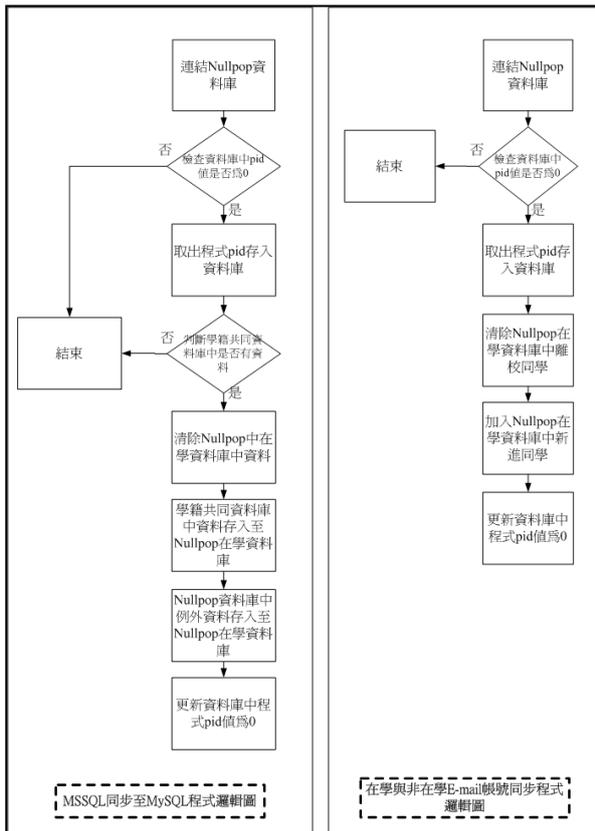


圖 6 資料庫同步程式邏輯圖

4 系統實作與結果

4.1 虛擬平台規格環境

目前本 Nullpop 系統平台架設於 VMWare 虛擬

平台主機上的軟硬體配置，整理於表 2 中。

表 2 Nullpop 系統硬體與軟體配置表

軟硬體項目	軟硬體說明
平台	VMWare 虛擬平台
記憶體	1GB RAM
CPU	2 顆 2.5GB CPU
硬碟	2 顆分別為 2GB 與 12GB 的硬碟
作業系統	FreeBSD 8.2
安裝軟體	PHP 5.2、MySQL5.5、修改後的 Nullpop 0.3 程式

4.2 MySql 資料表彙整效能

MySQL 關聯式資料表 Join 效能的問題，在目前學生 E-mail 帳號筆數約略 52,000 筆與在學學生加上例外學生學號資料筆數約略 12,000 筆作 MySQL Join 下，欲比對目前在學學生 E-mail 帳號數約 10,000 筆的資料是非常消耗系統資源的。

為了改善處理效能的問題，我們於欲處理的資料表中加入欄位的 index，來加速 MySQL 資料庫在 Join 資料表的處理，在加入 index 後其處理效能已從原本的約 28 分鐘，縮短為現今的約 20 分鐘。

5 數據分析與問題探討

5.1 Nullpop 與 POP3 登入反應時間比較

為驗證學生 POP3 server 與 Nullpop 系統在處理效能上的差異，我們由學生 E-mail POP3 伺服器上隨機選出 100 組使用者帳號與密碼，利用這 100 組帳號與密碼分別以 POP3 協定連線學生 E-mail POP3 與 Nullpop，並紀錄程式每一筆連線完成的時間。

圖 7 是我們選用 100 組學生 E-mail 帳號以 POP3 協定和 Nullpop 測試登入的數據比較圖。

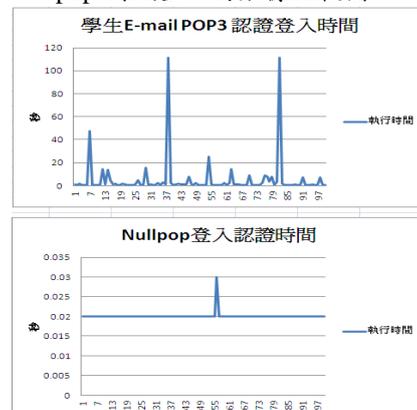


圖 7 POP3 登入數據比較圖

我們可以發現測試當時學生 E-mail POP3 伺服

器在沒有網路攻擊或其它因素造成系統忙碌的狀態下作連線，亦有詢問時間過長的狀況出現，反觀於 Nullpop 的測試數據顯示反應時間非常的快速，即使多項網路服務仍然透過 Nullpop 驗證下，每筆帳號驗證幾乎都於 0.02 秒內完成，足顯示 Nullpop 在驗證效能上非常優異，在回應驗證需求的服務可立即完成 POP3 驗證的工作。

5.2 認證次數使用比例

本校 Nullpop 系統於 2011 年 8 月中上線以來，以學生 E-mail 帳號作為身份認證的線上服務陸續切換至此系統上，透過 POP3 詢問的方式，向此系統驗證使用者的 E-mail 帳號、密碼是否正確。

至今透過此系統做為驗證的線上服務有宿舍網路、無線網路、SSL-VPN、電腦教室、校園軟體授權下載等五項服務，為了解各線上服務的認證使用情況，故以最近切換至此系統的五項服務在 2013 年 7 月 1 日至 2013 年 7 月 31 日的 POP3 詢問的驗證次數作一統計，一個月內的 POP3 詢問次數約 16 萬次，平均一天的詢問次數約 5 千多次，其中又以宿舍網路驗證佔總比例的 43% 為最大宗的線上使用服務，其次為 SSL-VPN 的 28%、校園授權軟體下載的 18%、校園無線網路的 8%、電腦教室的 3%。線上服務 POP3 認證數比例圓餅圖如圖 8 所示。

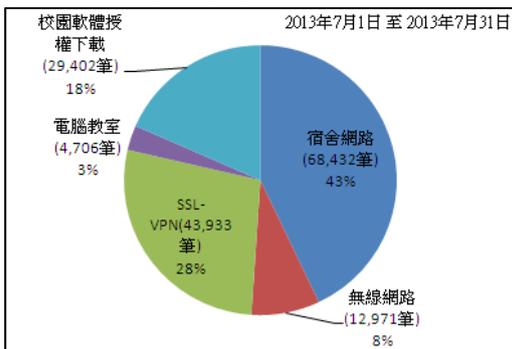


圖 8 線上服務 POP3 認證數比例圓餅圖

5.3 政策面上的問題 - 畢業未離校狀態

Nullpop 系統雖以資料庫作為基礎，可彈性的為使用服務增刪使用者帳號，但在 2011 年 8 月中旬上線以來，至今納入的線上服務數越來越多的情況下，難免會出現無法兼顧各項服務的帳號權限的情況。例如，各線上服務的使用權限是否該由 Nullpop 統一處理？這問題在 2013 年暑假，年度畢業旺季之後，突顯出來（因畢業班學生資料庫切換，導致部分「畢業未離校」的學生於七月結束後無法使用校園網路服務）。

- 如第四節所描述，nullpop 系統每日均會進行 MSSQL 與 MySQL 的學生資料庫同步。因部分畢業班(101 學年)學生在 7 月學期結束，仍未辦理離校，原因包括：(1)仍有少部分畢業學分未達畢業門檻，必須於暑修後(課程至八月底)

才可畢業；(2) 部分學生因協助老師處理事務而延長在學校的時間至八月底，這類的學生因未在下學年的在學名單中，亦不屬在學的學籍共同資料庫中有資料，以至於學籍共同資料庫切換成下學年的在學名單之後，發生仍在校的「畢業未離校」身分的學生無法認證登入的狀況。

- 短期解決方案：於此問題發生之後，我們隨即著手透過學籍共同資料庫管理單位所提供的畢業未離校的學生學號清單手動新增至 Nullpop 資料庫中，即解決此問題。
- 長期解決方案：未來，將再請學籍共同資料庫管理單位新增加「畢業未離校」身分的學生學號資料至同步的資料庫中，以自動化的方式透過資料庫同步解決此問題。

6 結論與未來研究方向

本論文旨在探討交通大學使用 nullpop 程式建置校園跨平台之輕量化網路身份驗證系統的開發經驗與維運成效。本研究的主要發現與貢獻，歸納如下：(1)新建輕量化高效率的認證服務，大幅減少等待時間，讓使用者可立即獲得登入是否成功的結果；(2)建立可調整的多源(multi-source)認證系統：新建的 authentication proxy (nullpop 系統)後，利用資料庫同步處理，可接受多個不同資料來源(包括自動與手動建立)，整合跨平台之特定類別的帳號；(3)新建系統可有效控管各服務所允許的使用者身份(例如，在學、已畢業等)，對線上服務的使用資源分配上更趨制度化。

其次，目前系統上，1 個月約 16 萬次的詢問，平均每天約 5 千多次的詢問，這一部分需要比較有系統，以自動化的方式來分析統計這些 Log，這是下一階段要進行的項目。

參考文獻

- Nullpop, <http://www.freebsdports.info/ports/mail/nullpop.html>, Retrieved Aug 5 2013.
- J. Myers and M. Rose, Rfc 1939, "RFC 1939 – Post Office Protocol – Version 3", <http://www.ietf.org/rfc/rfc1939.txt>, May 1996.
- 交大軟體授權 (NCTU CA), <https://ca.nctu.edu.tw/>
- Radius, from Wikipedia, <http://en.wikipedia.org/wiki/RADIUS>, Retrieved Aug 5 2013.
- NIS, <http://en.wikipedia.org/wiki/NIS>, Retrieved Aug 10 2013.
- LDAP, "Lightweight Directory Access Protocol(LDAP)", <http://en.wikipedia.org/wiki/LDAP>, Retrieved Aug 5 2013.
- Unified Modeling Language, http://en.wikipedia.org/wiki/Unified_Modeling_Language, Retrieved Aug 9 2013.