**TÌM HIỂU VÀ TRIỂN KHAI LDAP**

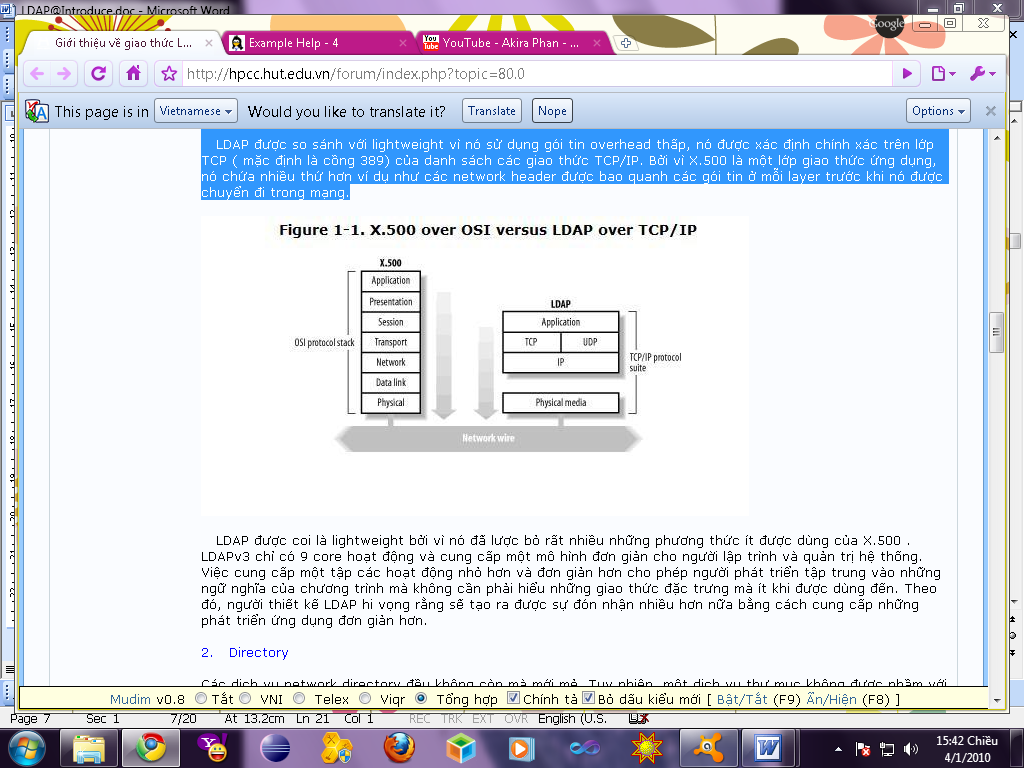
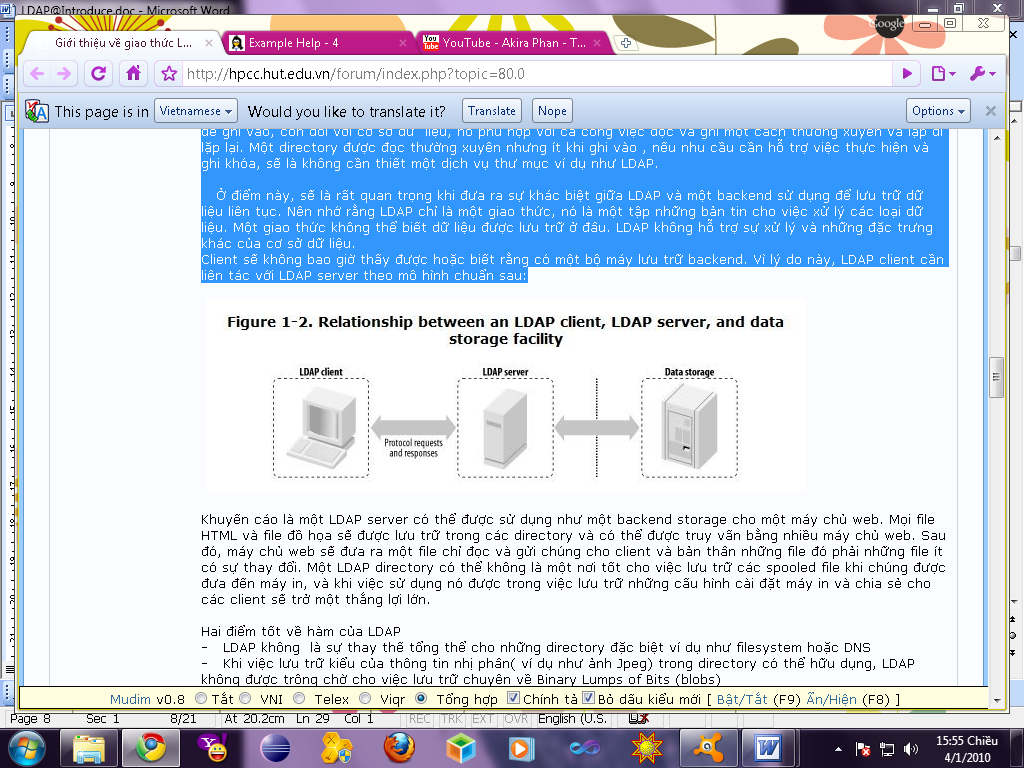
1. **Danh sách thành viên & công việc**

|  |  |  |  |
| --- | --- | --- | --- |
| **Họ tên** | **MSSV** | **Công việc** | **Tiến độ** |
| Nguyễn Thế Tuyển | 175A071418 | Tìm hiểu LDAP | Hoàn thành |
| Nguyễn Thế Tuyển | 175A071418 | Hướng dẫn cài đặt | Hoàn thành |
| Nguyễn Thế Tuyển | 175A071418 | Hướng dẫn sử dụng |  |
| Nguyễn Thế Tuyển | 175A071418 | Hướng dẫn phát triển |  |

1. **Nội dung nghiên cứu**
   1. **Giới thiệu:**
      * **LDAP là gì?**

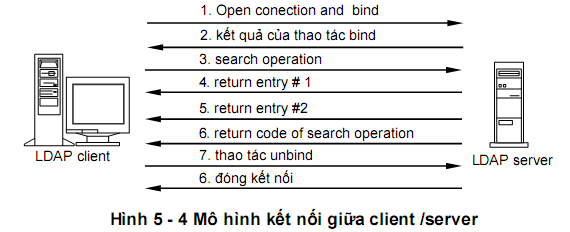
* **LDAP** (Lightweight Directory Access Protocol) – là giao thức truy cập nhanh các dịch vụ thư mục - là một chuẩn mở rộng cho nghi thức truy cập thư mục.
* **LDAP** là một giao thức tìm, truy nhập các thông tin dạng thư mục trên server. Nó dùng giao thức dạng Client/Server để truy cập dịch vụ thư mục.
* **LDAP** chạy trên TCP/IP hoặc các dịch vụ hướng kết nối khác.
* Có các LDAP Server như: OpenLDAP, OPENDS, Active Directory, …

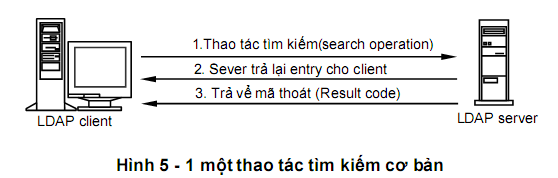
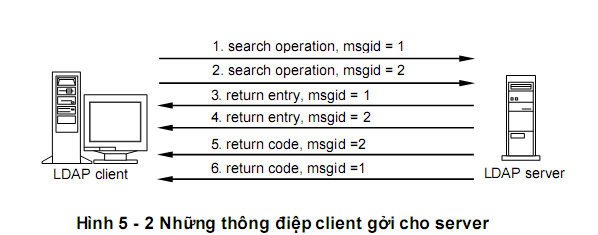
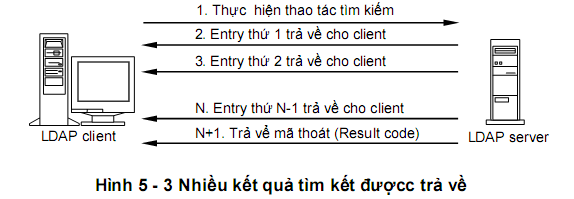
**Giải thích cụm từ “Lightweight Directory Access Protocol”**

* + - **Lightweight**
* Bản chất của LDAP là một phần của dịch vụ thư mục X.500. LDAP thực chất được thiết kế như một giao thức nhẹ nhàng, dùng như gateway trả lời những yêu cầu của X.500 server.
* X500 được biết như là một heavyweight, là một tập các chuẩn. Nó yêu cầu client và server liên lạc với nhau sử dụng theo mô hình OSI.
* LDAP được so sánh với lightweight vì nó sử dụng gói tin overhead thấp, nó được xác định chính xác trên lớp TCP (mặc định là cồng 389) của danh sách các giao thức TCP/IP. Còn X.500 là một lớp giao thức ứng dụng, nó chứa nhiều thứ hơn, ví dụ như các network header được bao quanh các gói tin ở mỗi layer trước khi nó được chuyển đi trong mạng.
* Tóm lại, LDAP được coi là lightweight bởi vì nó đã lược bỏ rất nhiều những phương thức ít được dùng của X.500 .
  + - **Directory**
* Dịch vụ thư mục không được nhầm với một cơ sở dữ liệu. Thư mục được thiết kế để đọc nhiều hơn là để ghi vào, còn đối với cơ sở dữ liệu, nó phù hợp với cả công việc đọc và ghi một cách thường xuyên và lặp đi lặp lại.
* LDAP chỉ là một giao thức, nó là một tập những thông tin cho việc xử lý các loại dữ liệu. Một giao thức không thể biết dữ liệu được lưu trữ ở đâu. LDAP không hỗ trợ sự xử lý và những đặc trưng khác như của cơ sở dữ liệu.
* Client sẽ không bao giờ thấy được hoặc biết rằng có một bộ máy lưu trữ backend. Vì lý do này, LDAP client cần liên tác với LDAP server theo mô hình chuẩn sau:
  + - **Access Protocol**
* LDAP là một giao thức truy cập. Nó đưa ra mô hình dạng cây của dữ liệu.
* Giao thức truy cập client/server của LDAP được định nghĩa trong RFC, một client có thể đưa ra một loạt những yêu cầu và những trả lời cho những yêu cầu đó lại được trả lời theo những cách sắp xếp khác nhau.

**Phương thức hoạt động của LDAP**

* + - **Ldap dùng giao thức giao tiếp client/sever**
* Giao thức giao tiếp client/sever là một mô hình giao tiếp giữa một chương trình client chạy trên một máy tính gởi một yêu cầu qua mạng đến cho một máy tính khác đang chạy một chương trình sever.
* Chương trình server này nhận lấy yêu cầu và thực hiện sau đó nó trả lại kết quả cho chương trình client
  + - **Đây là một tiến trình hoạt động trao đổi LDAP client/server :**



* Client mở một kết nối TCP đến LDAP server và thực hiện một thao tác bind. Thao tác bind bao gồm tên của một directory entry ,và uỷ nhiệm thư sẽ được sử dụng trong quá trình xác thực, uỷ nhiệm thư thông thường là pasword nhưng cũng có thể là chứng chỉ điện tử dùng để xác thực client.
* Sau khi thư mục có được sự xác định của thao tác bind, kết quả của thao tác bind được trả về cho client. Client phát ra các yêu cầu tìm kiếm.
* Server thực hiện xử lý và trả về kết quả cho client.
* Server gởi thông điệp kết thúc việc tìm kiếm.
* Client phát ra yêu cầu unbind, với yêu cầu này server biết rằng client muốn huỷ bỏ kết nối.
* Server đóng kết nối.
  + - **LDAP là một giao thức hướng thông điệp**
* Do client và server giao tiếp thông qua các thông điệp, Client tạo một thông điệp (LDAP message) chứa yêu cầu và gởi nó đến cho server. Server nhận được thông điệp và xử lý yêu cầu của client sau đó gởi trả cho client cũng bằng một thông điệp LDAP.
* Ví dụ: Khi LDAP client muốn tìm kiếm trên thư mục, client tạo thông điệp tìm kiếm và gởi cho server. Sever tìm trong cơ sở dữ liệu và gởi kết quả cho client bằng một thông điệp LDAP.
* Nếu client tìm kiếm thư mục và nhiều kết quả được tìm thấy, thì các kết quả này được gởi đến client bằng nhiều thông điệp
* Do nghi thức LDAP là giao thức hướng thông điệp nên client được phép phát ra nhiều thông điệp yêu cầu đồng thời cùng một lúc. Trong LDAP, message ID dùng để phân biệt các yêu cầu của client và kết quả trả về của server.
* Việc cho phép nhiều thông điệp cùng xử lý đồng thời làm cho LDAP linh động hơn các nghi thức khác.
* Ví dụ như HTTP, với mỗi yêu cầu từ client phải được trả lời trước khi một yêu cầu khác được gởi đi, một HTTP client program như là Web browser muốn tải xuống cùng lúc nhiều file thì Web browser phải thực hiện mở từng kết nối cho từng file, LDAP thực hiện theo cách hoàn toàn khác, quản lý tất cả thao tác trên một kết nối.

**Cấu trúc file Ldif**

* **Khái niệm LDIF**
* LDIF ( LDAP Interchange Format) được định nghĩa trong RFC 2849, là một chuẩn định dạng file text lưu trữ những thông tin cấu hình LDAP và nội dung thư mục.
* File LDIF thường được sử dụng để import dữ liệu mới vào trong directory của bạn hoặc thay đổi dữ liệu đã có. Dữ liệu trong file LDIF cần phải tuân theo một luật có trong schema của LDAP directory.
* Schema là một loại dữ liệu đã được định nghĩa từ trước trong directory của bạn. Mọi thành phần được thêm vào hoặc thay đổi trong directory của bạn sẽ được kiểm tra lại trong schema để đảm bảo sự chính xác. Lỗi vi phạm schema sẽ xuất hiện nếu dữ liệu không đúng với các luật đã có.
  + - **Cấu trúc file ldif**
* Mỗi tập entry khác nhau được phân cách bởi dòng trắng
* Một tập chỉ dẫn cú pháp để làm sao xử lý thông tin
* Lời chú thích được gõ sau dấu # trong 1 dòng
* Thuộc tính được liệt kê bên trái dấu “:” và giá trị được biểu diễn bên phải.
* Thuộc tính dn định nghĩa duy nhất cho một DN xác định trong entry đó.
  + - **Entry là gì ?**
* Một entry là tập hợp của các thuộc tính, từng thuộc tính này mô tả một nét đặt trưng tiêu biểu của một đối tượng. Một entry bao gồm nhiều dòng.
  + - **Một số thuộc tính cơ bản trong file ldif**

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên** | **Mô tả** |
| 1 | dn | Distinguished Name : tên gọi phân biệt |
| 2 | c | country – 2 kí tự viết tắt tên của một nước |
| 3 | o | organization – tổ chức |
| 4 | ou | organization unit – đơn vị tổ chức |
| 5 | objectClass | mỗi giá trị objectClass hoạt động như một khuôn mẫu cho các dữ liệu được lưu giữ trong một entry. Nó định nghĩa một bộ các thuộc tính phải được trình bày trong entry (Ví dụ: entry này có giá trị của thuộc tính objectClass là eperson, mà trong eperson có quy định cần có các thuộc tính là tên, email, uid ,…thì entry này sẽ có các thuộc tính đó) |
| 6 | givenName | tên |
| 7 | uid | id người dùng |
| 8 | cn | common name – tên thường gọi |
| 9 | telephoneNumber | số điện thoại |
| 10 | sn | surname – họ |
| 11 | userPassword | mật khẩu người dùng |
| 12 | mail | địa chỉ mail |
| 13 | facsimileTelephoneNumber | số phách |
| 14 | createTimestamp | thời điểm tạo ra entry này |
| 15 | creatorsName | tên người tạo ra entry này |
| 16 | pwdChangedTime | thời gian thay đổi mật khẩu |
| 17 | entryUUID | id của entry |

* + - **Mô hình LDAP**
* Mô hình LDAP information - xác định cấu trúc và đặc điểm của thông tin trong thư mục.
* Mô hình LDAP Naming - xác định cách các thông tin được tham chiếu và tổ chức.
* Mô hình LDAP Functional - định nghĩa cách mà bạn truy cập và cập nhật thông tin trong thư mục của bạn.
* Mô hình LDAP Security - định nghĩa ra cách thông tin trong thư mục của bạn được bảo vệ tránh các truy cập không được phép.
  1. **Hướng dẫn cài đặt trên Ubuntu sever**
     + **Các bước cài đặt**
* Cập nhật hệ thống

|  |
| --- |
|  |

* Cài đặt LDAP

|  |
| --- |
| * Tạo mật khẩu cho tài khoản admin của ldap   **-**  - Tạo mật khẩu cho admin |

* Cấu hình LDAP

|  |
| --- |
|  |

* 1. **Hướng dẫn sử dụng**
* Thêm thuộc tính với file .ldif
* Tạo file .ldif chứa thông tin cần tạo

|  |
| --- |
|  |

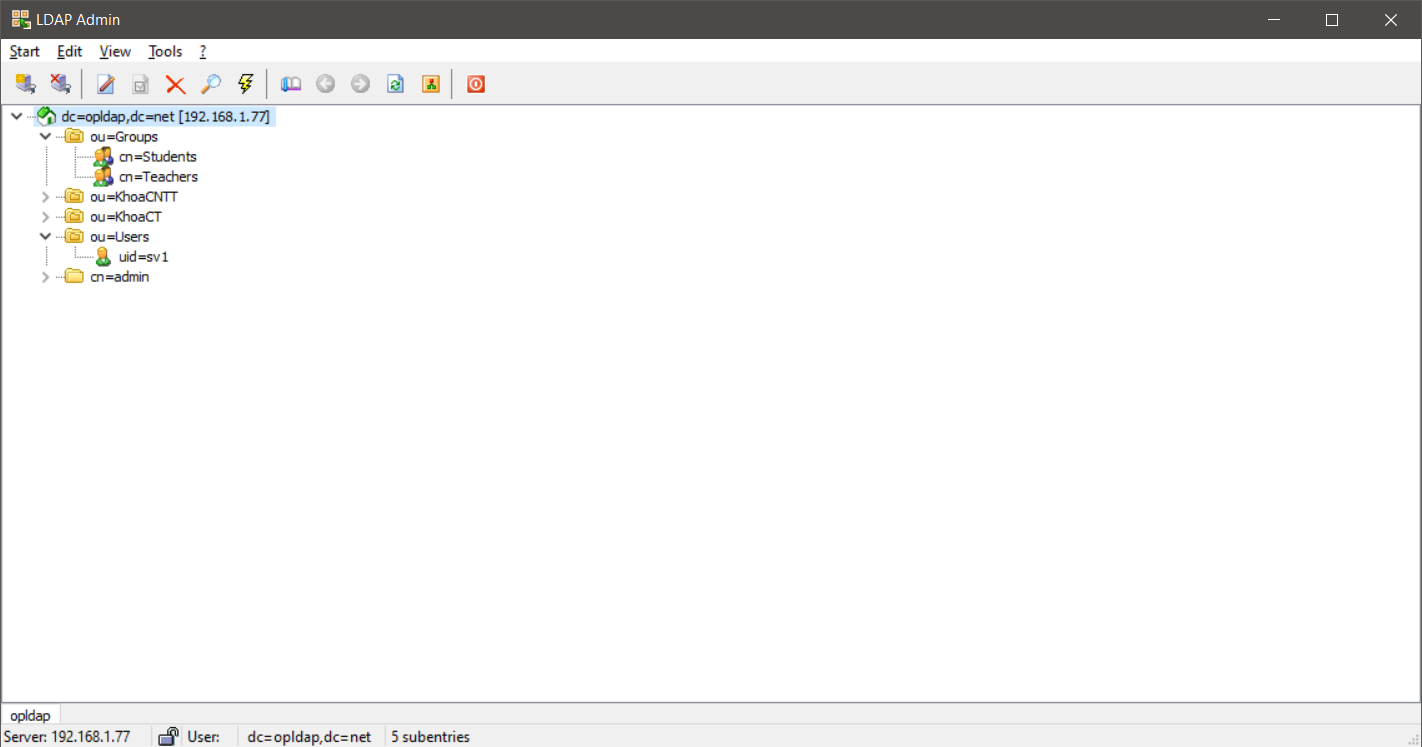
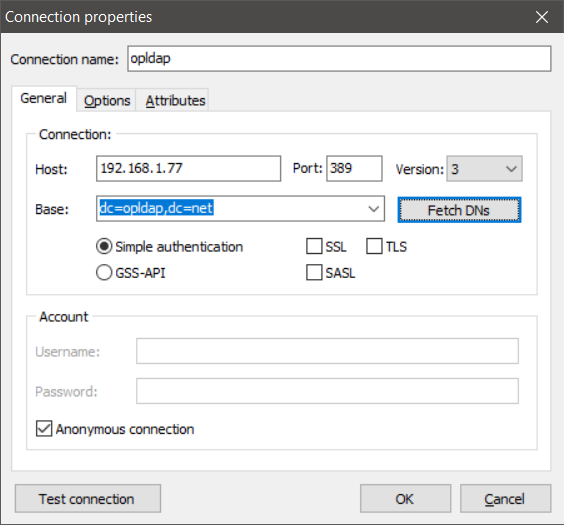
* Add entry mới vào LDAP bằng câu lệnh:

|  |
| --- |
|  |

* + - Tải ldap admin trên window

<https://sourceforge.net/projects/ldapadmin/files/ldapadmin/1.8.3/LdapAdminExe-w64-1.8.3.zip/download>

* + - Xem kết quả bằng Ldap admin



* + - Tìm kiếm

|  |
| --- |
|  |

* + - Sửa thông tin

|  |
| --- |
| * Tạo file ldif      * Chạy lênh cập nhật |

* + - Sử dụng giao diện web với phpldapadmin
* Cài đặt phpLDAPadmin

|  |
| --- |
|  |

* Sửa file config tại đường dẫn: /etc/phpldapadmin/config.php

|  |
| --- |
| * Đổi tên tại dòng 286      * Đổi domain tại dòng 300      * Đổi tên đăng nhập mặc định tại dòng 326      * Uncomment và đổi giá trị thành true tại dòng 161 |

* Đăng nhập tại trình duyệt web

|  |
| --- |
| * Truy cập vào địa chỉ <IP của máy chủ>/phpldapadmin      * Click vào login      * Nhập mật khẩu và nhấn Enter |

* Thêm entry mới

|  |
| --- |
| * Tạo entry mới bằng cách click vào create new entry here tại cây thư mục hoặc Create a child entry      * Chọn object      * Điền đầy đủ thông tin rồi click create object      * Click commit để xác nhận |

* Xóa entry

|  |
| --- |
| * Click vào entry chọn delete this entry      * Click delete để xác nhận |

* Sửa thông tin của một entry

|  |
| --- |
| * Click vào entry trên cây thư mục rồi tìm thông tin cần sửa và click update object      * Chọn update object để xác nhận thay đổi click vào ô skip tại dòng nào không muỗn thay đổi giá trị |

* Có thể đổi tên miền truy cập bằng cách sửa file hosts tại đường dẫn: C:\Windows\System32\drivers\etc

|  |
| --- |
| * Thêm dòng này tại file hosts với địa chỉ IP là địa chỉ IP của server      * Bây giờ có thể truy cập đến tên miền opldap.net/phpldapadmin |