**SƠ ĐỒ LAB DỊCH VỤ FTTH**

****

1. **Bài lab sẽ bao gồm các khối (1) và (2), được kết nối với nhau bằng dây RJ45**
2. **Chức năng của các phần tử cần lab:**
3. Các thành phần của (1) sẽ được cấu hình trong router cisco (hiện tại bọn e chưa nắm được chủng loại router nào có thể hỗ trợ được yêu cầu của bài lab, nhờ a tư vấn giúp bọn e ạ)
* BRAS: gồm các chức năng cấp DHCP, NAT, Routing. Có nhiệm vụ tạo phiên kết nối PPPOE, cấp địa chỉ IP WAN (public or private) xuống cho router và định tuyến địa chỉ này ra internet. Đồng thời nó gửi các trường star/stop time,… cho Radius để đếm lưu lượng của user
* RADIUS: là giao thức bảo mật mạng dựa theo mô hình client-server, nó dùng giao thức UDP. Radius Client (ở đây chính là BRAS) là các dạng thiết bị có thể truyền thông tin đến RADIUS server được chỉ định trước và sau đó đóng vai trò phúc đáp mà nó trả về. Radius Server làm nhiệm vụ: xác thực (Authentication), Cấp quyền (Authorization) và Tính cước (Accounting)
* **Xác thực (Authentication)**: Xác thực dùng để nhận dạng người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu lưu trong LDAP
* **Cấp quyền (Authorization)**: Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó.
* **Tính cước (Accounting)**: Accounting cho phép nhà quản trị có thể thu thập thông tin như thời gian bắt đầu, thời gian kết thúc người dùng truy cập vào hệ thống, các câu lệnh đã thực thi, thống kê lưu lượng, việc sử dụng tài nguyên và sau đó lưu trữ thông tin trong hệ thống cơ sở dữ liệu quan hệ. Nói cách khác, accounting cho phép giám sát dịch vụ và tài nguyên được người dùng sử dụng.
* LDAP: là CSDL chứa Username và Password cũng như các thông số liên quan đến khách hàng khi đăng kí dịch vụ
1. Các phần tử của (2) sẽ được gói gọn trong router TPL740-741 (bỏ qua hộp TB và ONT): làm nhiệm vụ quay số PPPoE với Username/Password được cấp bởi BRAS
2. **Nguyên lý hoạt động PPPoe từ BRAS đến Router**
* Khi một Acc muốn vào mạng nó gửi một bản tin yêu cầu được kết nối đến BRAS
* Khi đến BRAS ( BRAS là một PPPoe sever, còn router là một PPPoe client). BRAS sẽ đọc bản tin yêu cầu thiết lập kết nối mà Router gửi, trong đó có hai tham số chính dung để xác thực là Username và password.
* Các thông số này ( user và PW) sẽ được BRAS chuyển đến Radius sever để làm nhiệm vụ AAA ( xác thực, phân quyền và tính cước ). Lúc này BRAS đóng vai trò là Radius client.
* Radius sẽ kiểm tra trong cơ sở dữ liệu của mình ( LDAP).
* Nếu xác thực OK, Radius báo cho BRAS là cho phép thiết lập PPP section, đồng thời cấp phát cho Router một địa chỉ IP public để ra internet
* BRAS sẽ gởi bản tin thiết lập PPP tunnel xuống Router có kèm theo địa chỉ IP, đồng thời nó cũng sẽ gửi các trường start time, stop time, ...cho RADIUS để bắt đầu đếm lưu lượng của Acc. Đồng thời BRAS sẽ làm việc như một Gateway để định tuyến địa chỉ này ra internet.