Bản ghi lịch sử

Lưu giữ thông tin về một quá trình download:

* Vị trí byte bắt đầu.
* Số byte đã truyền được.
* Cờ cho biết quá trình tải đã hoàn tất hay chưa.
* Kích thước tệp.
* Đường dẫn tệp nguồn.
* Đường dẫn tệp đích.

Dừng quá trình download

Để dừng quá trình download, nhóm em sử dụng một mảng động các con trỏ trỏ tới các biến cờ boolean, sau đó sẽ truyền các con trỏ có chỉ số trong mảng trùng với số định danh (id) của luồng download vào trong luồng download. Trong luồng download, sau mỗi lần đọc xong một khối dữ liệu, cờ kiểm tra dừng sẽ được kiểm tra. Nếu cờ này được đặt giá trị là true thì việc download sẽ được dừng và một bản ghi lịch sử sẽ được tạo ra nhằm phục vụ cho quá trình khôi phục lại sau này. Nếu quá trình download thất bại do bị gián đoạn kết nối thì cờ kiểm tra dừng sẽ được đặt giá trị true và một bản ghi lịch sử sẽ được tạo ra.

Để khôi phục lại một quá trình download chưa hoàn thành do bị người dùng dừng hoặc bị gián đoạn.

Khi bắt đầu một phiên, đọc lại tất cả bản ghi lịch sử tương ứng với địa chỉ IP của Server. Dựa vào các thông tin được lưu trong bản ghi lịch sử để khôi phục lại quá trình download.

Sự mở rộng cho IPv6 và NATs

Mục đích: Ngày nay, giao thức IPv6 đang được triển khai để thay thế giao thức IPv4 đã tồn tại trước đó. Tuy nhiên, do gặp nhiều khó khăn (Nhất là tình trạng số lượng thiết bị mạng rất lớn hiện nay), nên giao thức IPv6 chưa thể thay thế hoàn toàn được giao thức IPv4. Do đó, hai giao thức này đang tồn tại song song với nhau. RFC 1639 đã đặc tả sự mở rộng của FTP để cho phép nó tương thích với IPv6, tuy nhiên không may kỹ thuật này lại thất bại trong môi trường đa giao thức.

Các câu lệnh PORT, PASV được thay thế bằng các câu lệnh EPRT và EPSV. Do sự phổ biến của phương thức thiết lập kênh dữ liệu bị động, nên nhóm em sẽ trình bày về lệnh EPSV.

Lệnh EPSV

Lệnh EPSV yêu cầu Server lắng nghe trên một cổng dữ liệu và đợi một kết nối tới. EPSV có một tham số tùy chỉnh. Số hiệu cổng Server sẽ lắng nghe được trả về trong thông điệp phản hồi. Nếu thành công sẽ trả về mã 229.

|  |
| --- |
| 2yz Hoàn tất xác thực |
| x2z Kết nối |
| xy9 Chế độ bị động mở rộng |

Khuôn dạng thông điệp trả về

|  |
| --- |
| <text indicating server is entering extended passive mode> \ |
| (<d><d><d><tcp-port><d>) |

Xâu trong dấu ngoặc là phần xâu cần thiết cho việc mở cổng để truyền dữ liệu. Hai trường đầu tiên của xâu nên được để trống. Trường thứ ba là xâu đại diện cho số hiệu cổng TCP. Giao thức truyền thông được sử dụng bởi kênh dữ liệu sẽ giống với giao thức được sử dụng bởi kênh điều khiển. Địa chỉ mạng được sử dụng để thiết lập kênh dữ liệu sẽ phải giống với địa chỉ được sử dụng bởi kênh điều khiển. Ví dụ: thông điệp trả về bởi File Zilla Server khi gửi lệnh EPSV.  


|  |
| --- |
| Entering Extended Passive Mode (|||58844|) |

Trong đó chuỗi “58844” là số hiệu cổng mà Server sẽ lắng nghe.  
Mã báo lỗi thường là: 500 hoặc 501.

Lệnh EPSV không tham số: Server sẽ chọn giao thức truyền thông cho kênh dữ liệu dựa vào giao thức được sử dụng bởi kênh điều khiển. Tuy nhiên trong trường hợp proxy FTP, giao thức này có thể không thích hợp cho việc giao tiếp giữa hai Máy chủ. Vì thế, Máy khách cần có khả năng yêu cầu một giao thức đặc trưng. Nếu máy chủ trả về một giao thức không được hỗ trợ bởi nút mạng sẽ kết nối tới cổng đó, máy khách phải phát đi một lệnh “ABOR” để cho phép Máy chủ đóng kết nối đang lắng nghe.

Lệnh EPSV có tham số:

|  |
| --- |
| EPSV<space><net-prt> |

Nếu giao thức yêu cầu được hỗ trợ bởi Máy chủ, nó sẽ sử dụng giao thức này. Còn nếu không được hỗ trợ, Máy chủ sẽ trả về mã lỗi 522.

EPSV có thể sử dụng với tham số “ALL” để thông báo cho bộ dịch địa chỉ (Network Address Translators) rằng lệnh “EPRT” (cũng như các lệnh dữ liệu khác) sẽ không được sử dụng nữa.

Khi nhận được lệnh EPSV, máy chủ phải loại bỏ tất cả các lệnh dữ liệu đã được thiết lập trước đó (Ví dụ: EPRT, PORT, PASV, …).

Lệnh EPSV giúp cải thiện hiệu năng truyền tải qua tường lửa hoặc NATs. Sử dụng lệnh EPSV không yêu cầu NATs chuyển đổi địa chỉ mạng trong lưu lượng dữ liệu khi nó được chuyển tiếp. Cuối cùng nếu Máy khách phát đi một lệnh “EPSV ALL” có thể đặt kết nối trên một “fast path” qua bộ dịch, vì thế lệnh EPRT sẽ không bao giờ được sử dụng, do đó việc dịch phần dữ liệu của các segments là không cần thiết. Khi một máy khách chỉ mong đợi việc truyền d

Mở rộng bảo mật của FTP

Các câu lệnh mới được thêm vào để mở rộng tính năng bảo mật cho giao thức FTP

AUTH (Authentication/Security Mechanism),  
ADAT (Authentication/Security Data),  
PROT (Data Channel Protection Level),  
PBSZ (Protection Buffer Size),  
CCC (Clear Command Channel),  
MIC (Integrity Protected Command),  
CONF (Confidentiality Protected Command), and  
ENC (Privacy Protected Command).

Giao thức FTP được định nghĩa trong STD9, RFC 959 sử dụng tên đăng nhập và mật khẩu dưới ký tự không được mã hóa để xác thực máy khách (thông qua lệnh USER và PASS). Điều này khiến cho mật khẩu dễ dàng đánh cắp khi kẻ tấn công thực hiện giám sát trong mạng cục bộ hoặc mạng diện rộng. Ngoài ra, bên cạnh việc xác thực người dùng thì còn cần đảm bảo giữ an toàn cho các thông tin nhạy cảm và đảm bảo tính nguyên vẹn của chúng.

Ở mức độ cao, FTP cố gắng cung cấp một kỹ thuật trừu tượng cho việc xác thực, ủy quyền kết nối và bảo vệ tính toàn vẹn và tin cậy các câu lệnh, thông điệp trả lời, dữ liệu truyền.

Kiểu thông điệp phản hồi mới (6yz)