**Мета роботи: навчитися налаштовувати FTP- сервер під управлінням ОС FreeBSD**

**FTP** ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA)*FileTransferProtocol*— [протокол передач](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85)і файлів) — [протокол](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB), призначений для передачі [файлів](http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB) у [комп’ютерних](http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C) мережах. FTP дозволяє підключатися до [сервер](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_%28%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5%29)ів FTP, переглядати вміст [каталогів](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%82%D0%B0%D0%BB%D0%BE%D0%B3_%28%D1%84%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%29) і завантажувати файли із сервера або на сервер; крім того, можливий режим передачі файлів між серверами.

FTP є одним з найстарших прикладних протоколів, що з'явився задовго до [HTTP](http://ru.wikipedia.org/wiki/HTTP), в [1971](http://ru.wikipedia.org/wiki/1971_%D0%B3%D0%BE%D0%B4) році. До початку [90-х](http://ru.wikipedia.org/wiki/1990-%D0%B5)років на частку FTP доводилося близько половини трафіку в мережі [Інтернет](http://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82). Він і сьогодні широко використовується для поширення [П](http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)З і доступу до віддалених[хост](http://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82)ів.

Протокол FTP ставиться до протоколів прикладного рівня й для передачі даних використовує транспортний протокол [TCP](http://ru.wikipedia.org/wiki/TCP). Команди й дані, на відміну від більшості інших протоколів передаються по різних [порта](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D1%82_%28TCP/UDP%29)х. [Порт](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D1%82_%28TCP/UDP%29) 20 використовується для передачі даних, [порт](http://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%80%D1%82_%28TCP/UDP%29) 21 для передачі команд. У випадку, якщо передача файлу була перервана за якимись причинами, протокол передбачає засоби для докачки файлу, що дуже зручно при передачі великих файлів.

**Проблема безпеки**

Протокол не [шифрується](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), при [аутентифікац](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F)ії передаються [логін](http://ru.wikipedia.org/w/index.php?title=%D0%9B%D0%BE%D0%B3%D0%B8%D0%BD_%28%D1%83%D1%87%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C%29&action=edit&redlink=1) і [пароль](http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C) відкритим текстом. У випадку побудови мережі з використанням [хаб](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80)у зловмисник за допомогою пасивного [сніффера](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0) може перехоплювати логіни й паролі, що перебувають у тому ж [сегменті](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82_%D1%81%D0%B5%D1%82%D0%B8)мережі користувачів FTP, або, при наявності спеціального ПЗ, одержувати передані по FTP файли без авторизації. Щоб запобігти перехопленню трафіку, необхідно використовувати протокол шифрування даних [SSL](http://ru.wikipedia.org/wiki/SSL), який підтримується багатьма сучасними Ftp-Серверами й деякими Ftp-Клієнтами.

Процес нешифрованої авторизації проходить у кілька етапів (символи \r\n означають перевід рядка):

Установка Tcp-з'єднання із сервером (звичайно на 21 порт)

Посилка команди USER *логін*\r\n

Посилка команди PASS *пароль*\r\n

Якщо до сервера дозволений анонімний доступ ( як правило, лише для завантаження даних із сервера), то в якості логіна використовується ключове слово «anonymous» або «ftp», а в якості пароля — адреса [електронної по](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0)шти:

USER anonymous\r\n

PASS someone@email\r\n

Після успішної авторизації можна посилати на сервер інші команди.

**Основні команди**

* ABOR — Перервати передачу файлу
* CDUP — Змінити директорію на вищу.
* CWD — Змінити директорію.
* DELE — Вилучити файл (DELE filename).
* EPSV —Увійти в розширений пасивний режим. Застосовується замість PASV.
* HELP — Виводить список команд, прийнятих сервером.
* LIST — Повертає список файлів директорії. Список передається через з'єднання даних (20 порт).
* MDTM — Повертає час модифікації файлу.
* MKD — Створити директорію.
* NLST — Повертає список файлів директорії в більш короткому форматі чому LIST. Список передається через з'єднання даних (20 порт).
* NOOP — Порожня операція.
* PASV — Увійти в пасивний режим. Сервер поверне адресу й порт до якого потрібно підключитися щоб забрати дані. Передача почнеться при введенні наступних команд RETR, LIST і т. д.
* PORT — Увійти в активний режим. Наприклад PORT 12,34,45,56,78,89. На відміну від пасивного режиму для передачі даних сервер сам підключається до клієнта.
* PWD — Повертає поточну директорію.
* QUIT — Відключитися
* REIN — Реініціалізувати підключення
* RETR — Скачати файл. Перед RETR повинна бути команда PASV або PORT.
* RMD — Вилучити директорію
* RNFR і RNTO — Перейменувати файл. RNFR — що перейменовувати, RNTO — у що.
* SIZE — Повертає розмір файлу
* STOR — Закачати файл. Перед STOR повинна бути команда PASV або PORT.
* SYST — Повертає тип системи(UNIX, WIN, …)
* TYPE — Установити тип передачі файлу(Бінарний, текстовий)
* USER — Ім'я користувача для входу на сервер

**Приклад**

220 FTP serverready.

USER ftp //Anonymous

230 Loginsuccessful.

PASV

227 EnteringPassiveMode (192,168,254,253,233,92)//Клієнт повинен відкрити з'єднання на переданий IP

LIST

150 Herecomesthedirectorylisting. //Сервер передає список файлів у директорії

226 Directorysend OK.

CWD incoming

250 Directorysuccessfullychanged.

PASV

227 EnteringPassiveMode (192,168,254,253,207,56)

STOR gyuyfotry.avi

150 Oktosenddata. //Клієнт передає вміст файлу

226 Filereceive OK.

QUIT

221 Goodbye.

Аргумент 192,168,254,253,207,56 означає, що з'єднання від сервера очікується на вузлі з Ip-Адресою 192.168.254.253 на порту 207\*256+56=53048.

На багатьох Ftp-Серверах існує каталог ( за назвою incoming, upload і т.п.), відкритий на запис і призначений для закачування файлів на сервер. Це дозволяє користувачам наповнювати сервер свіжими даними.

**PASSIVE MODE**

Споконвічно протокол припускав зустрічне TСP-з'єднання від сервера до клієнта для передачі файлу або вмісту каталогу. Це унеможливлювало спілкування із сервером, якщо клієнт перебуває за [IP NAT](http://ru.wikipedia.org/wiki/NAT), крім того, часто запит з'єднання до клієнта блокується [фаєрволом](http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD). Щоб цього уникнути, було розробленo розширення протоколу FTP passivemode, коли з'єднання для передачі даних теж походить від клієнта до сервера. Важливим моментом є те, що клієнт встановлює з'єднання з адресою й портом, зазначеним сервером. Порт сервер вибирає випадковим образом з певного діапазону (49152-65534). Тому при знаходженні ftp-сервера за NAT, слід явно вказати в настроюваннях сервера його адресу.

**NAT-PT**

Спеціально для роботи FTP-протоколу через міжмережеві екрани було зроблено розширення NAT, називане NAT-PT (rfc2766), що дозволяє транслювати вхідні з'єднання від сервера до клієнта через NAT. У процесі такого з'єднання NAT підмінює передані дані від клієнта, вказуючи серверу дійсну адресу й порт, з яким зможе з'єднатися сервер, а потім транслює з'єднання від сервера від цієї адреси клієнтові на його адресу. Незважаючи на всі заходи й нововведення, прийняті для підтримки FTP-протоколу, на практиці функція NAT-PT звичайно відключається на всіх роутерах і маршрутизаторах з метою забезпечення додаткової безпеки від вірусних загроз.

**FXP**

**FXP** ([англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA)*FileeXchangeProtocol*—протокол обміну файлами) — спосіб передачі файлів між двома Ftp-Серверами прямо, не накачуючи їх на свій [компьютер](http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) . При FXP-сесії клієнт відкриває два FTP-з’єднання до двох різних серверах, запитуючи файл на першому сервері, указуючи в команді PORT IP-адресу другого сервера.

Безсумнівною перевагою підтримки стандарту FXP є те, що на кінцевих користувачів, що бажають скопіювати файли з одного FTP-сервера на інший, уже не діє обмеження пропускної здатності їх власного інтернет-з'єднання. Немає необхідності скачувати собі файл, щоб потім покласти його на інший FTP-сервер. Таким чином, час передачі файлів буде залежати тільки від швидкості з'єднання між двома віддаленимиFTP-серверами, яка в більшості випадків більша «користувацької».

На жаль, FXP став використовуватися зловмисниками для атак на інші сервери: у команді PORT вказується IP-адреса й порт сервісу, що атакується, на комп'ютері жертви, і командами RETR/STOR проводиться звертання на цей порт від імені FTP-сервера, а не атакуючої машини, що дозволяло влаштовувати [DDoS](http://ru.wikipedia.org/wiki/DDoS)-атаки з використанням відразу багатьох FTP-серверів, або обходити систему безпеки комп'ютера жертви, якщо він покладається тільки на перевірку IP клієнта й використовуваний для атаки FTP-серверперебуває в довіреній мережі або на шлюзі. У результаті зараз практично всі сервери перевіряють відповідність IP-адреси, зазначеного в команді PORT, IP-адресі FTP-клієнта й за замовчуванням забороняють використання там IР-адрес третіх сторін. Таким чином, використання FXP неможливо при роботі з публічними FTP-серверами.

**FTP**

FTP — стандартна програма, яка працює за протоколом [TCP](http://uk.wikipedia.org/wiki/TCP), яка завжди поставляється з [операційною системою](http://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0). Її початкове призначення — передача файлів між різними комп'ютерами, які працюють у мережах TCP/IP: на одному з комп'ютерів працює програма-сервер, на іншому — програма-клієнт, запущена користувачем, яка з'єднується з сервером і передає або отримує файли через FTP-сервіс. Все це розглядається з припущенням, що користувач зареєстрований на сервері та використовує логін та пароль на цьому комп'ютері.

Дана риса і послужила причиною того, що програми FTP стали частиною окремого сервісу Інтернет. Справа в тому, що доволі часто сервер FTP налаштовується таким чином, що з'єднатися з ним можна не тільки під своїм ім'ям, але й під умовним іменем anonymous — анонім. У такому випадку для користувача стає доступною не вся файлова система комп'ютера, а лише деякий набір файлів на сервері, які складають вміст серверу anonymous FTP — публічного файлового архіву. Отже, якщо користувач хоче надати у вільне користування файли з інформацією, програмами і т. і., то йому достатньо організувати на власному комп'ютері, включеному в Інтернет, сервер anonymous FTP. Створення такого серверу — процес доволі простий, програми-клієнти FTP доволі розповсюджені, — тому сьогодні публічні файлові архіви організовані в основному як сервери anonymous FTP. Перелік інформації, яка міститься на таких серверах включає всі аспекти життя: від звичайних текстів до [мультимедіа](http://uk.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BC%D0%B5%D0%B4%D1%96%D0%B0).

Не дивлячись на розповсюдженість, у FTP є багато недоліків. Програми-клієнти FTP не завжди зручні і прості у користуванні. Користувач не завжди може зрозуміти який файл перед ним, чи той що необхідно, чи ні. Окрім того, не існує простого і універсального засобу для пошуку на серверах anonymous FTP, — хоча для цього і існує спеціальний сервіс archie, наприклад: <http://archie.icm.edu.pl/archie_eng.cgi>, але це незалежна програма, вона не універсальна і не завжди її можна ефективно застосовувати. Програми FTP доволі старі і деякі з їх особливостей, які були необхідними їх при створенні, не зовсім зрозумілі і потрібні сьогодні. Наприклад, для передачі файлів існує два режими — двійковий та текстовий, і, якщо користувач неправильно обрав режим передачі, то файл, який необхідно передати, може бути пошкодженим. Опис файлів на сервері видається у форматі операційної системи серверу, а список файлів операційної системи UNIX не завжди з розумінням сприймається користувачами DOS. Сервери FTP нецентралізовані, — звідси випливають ще деякі проблеми. Але не дивлячись на все це, сервери anonymous FTP сьогодні — це стандартний шлях організації публічних файлових архівів в Інтернет.

FTP — сервіс прямого доступу, який вимагає повноцінного підключення до Інтернет, але є можливість доступу і через електронну пошту — існують сервери, які пересилають за допомогою [електронної пошти](http://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BF%D0%BE%D1%88%D1%82%D0%B0) файли з будь-яких серверів anonymous FTP. Проте цей шлях отримання інформації досить незручний, оскільки такі сервери можуть бути сильно завантажені і запит доволі довго чекатиме своєї черги. Крім того, великі файли при пересилці діляться сервером на частини обмеженого об'єму і, якщо одна з частин загубиться і буде пересланою із пошкодженнями, то весь файл стане непридатним.

В ОС FreeBSD є досить багато можливостей реалізації FTP-сервера з анонімним доступом:

* скористатися вбудованим FTP-сервером;
* запустити FTP-сервер через inetd.conf;
* встановити FTP-сервери, які пропонуються у портах.

Перші два варіанти досить прості у налаштуванні і не вимагають якихось додаткових ресурсів. Останній варіант системні адміністратори вибирають частіше, так як він пропонує кращу гнучкістьпри доступі, захищеність при передачі і отриманні файлів, а також простоту у налаштуванні.

**Хід виконання роботи**

1. Зайти у директорію cd /usr/ports/ftp/proftpd
2. Ввести команду установки make config install
3. Після завершення установки відредактувати файл /etc/rc.conf
4. Вкінці файлу ввести: proftpd\_enable=”YES”
5. Зберегти зміни і вийти з редактору
6. Відредактувати файл /usr/local/etc/proftpd.conf
   1. В рядку ServerName ввести своє бажане ім’я FTP серверу (своє прізвище)
   2. В рядку ServerType ввести standalone
   3. Переконатися, щоб у рядку Port      стояла цифра    21
   4. В рядку Umask поставити цифру 777
   5. В рядку MaxInstances вказати максимальне число процесів для FTP
   6. Вказати, що для користувача, який підключається не потрібно логінитися User                nobody  
       Group                nogroup
   7. Дозволити перезапис файлів AllowOverwrite on
   8. Дозволити зміну прав на файли і створення каталогів <limit SITE\_CHMOD MKD>  
        AllowAll  
       </limit>
   9. Вказати папку, до якої буде здійснюватися доступ по FTP <Anonymous /usr/students>
   10. Вказати групу для користувача FTP User ftp

Group ftp

* 1. Вказати тип підключення UserAlias anonymous ftp
  2. Вказати, що користувачу по FTP не потрібна робоча оболонка RequireValidShell off
  3. Вказати максимальну кількість користувачів, але не менше, ніж вказано у п. 6.5 MaxClients
  4. Вказати, що анонімному користувачу дозволено будь-що <Limit WRITE>

AllowAll

</Limit>

</Anonymous>

1. Зберегти зміни і вийти з редактору
2. Створити папку students у директорії /usr
3. Змінити права папки students на 777
4. Перезавантажити ОС FreeBSD
5. Якщо все зроблено правильно, то можна буде зайти на створений FTP сервер, ввівши у браузері або FTP клієнті наступне: [ftp://ім’я](ftp://ім'я)\_вашої\_ FreeBSD/