

FTP (File Transfer Protocol)



โดย...อดิศร ขาวสังข์

ทดสอบบน FC4

Update : 15/08/2548



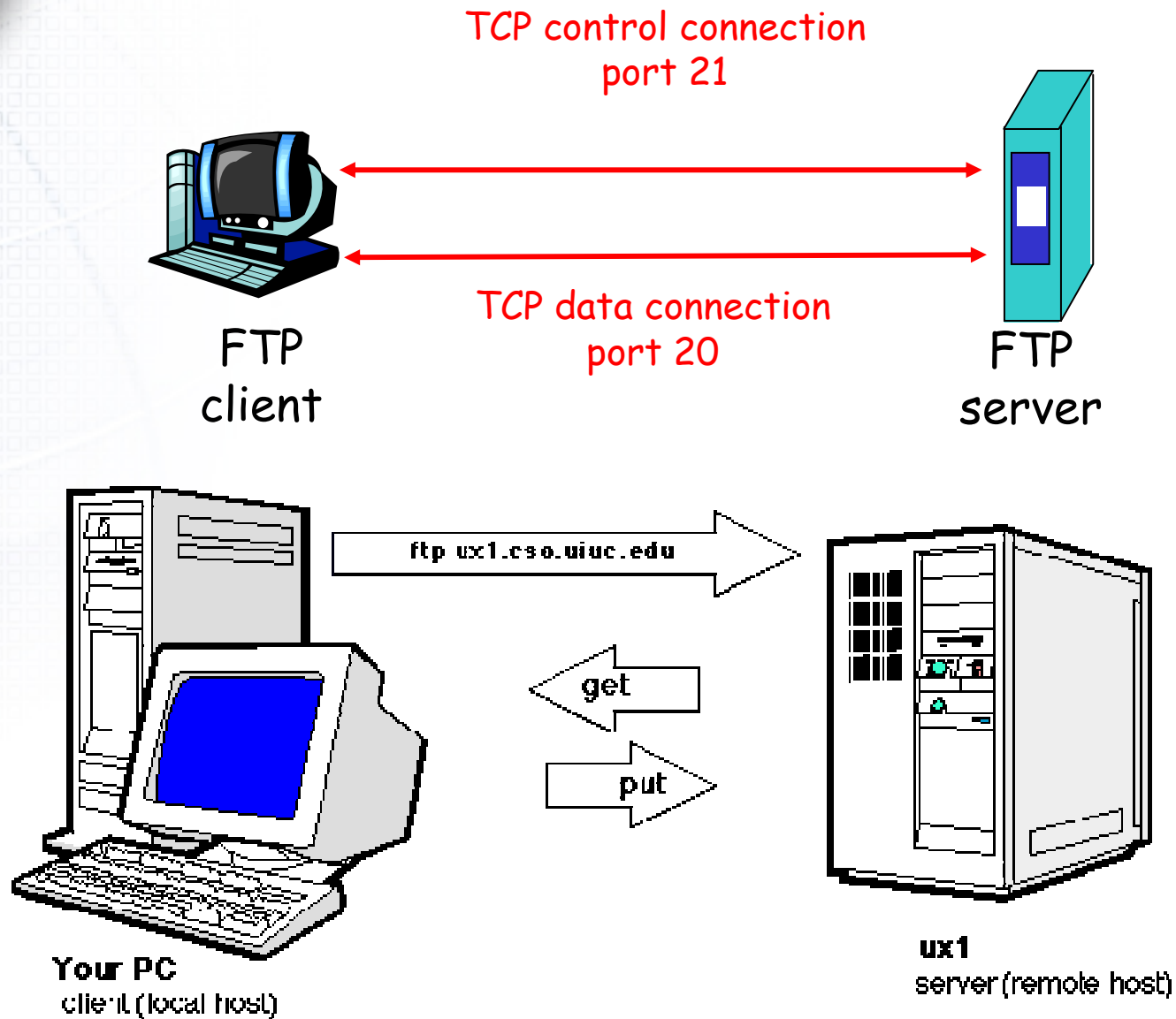
FTP : File Transfer Protocol

What is FTP

- FTP stands for the File transfer protocol and is used to transfer files between an FTP server and another computer.
- In the past, FTP was much more common than it is today and was the dominant file transfer mechanism on the Internet.
- FTP is still very popular today when a service requires that a lot of files be hosted for other to people to download.
- FTP also tends to be faster than other contemporary methods of transferring files because it was designed to do so.



FTP : File Transfer Protocol





FTP : File Transfer Protocol

What is FTP (cont.)

- FTP is a TCP based service exclusively. There is no UDP component to FTP.
- FTP is an unusual service in that it utilizes two ports, a 'data' port and a 'command' port (also known as the control port).
- Traditionally these are port 21 for the command port and port 20 for the data port. The confusion begins however, when we find that depending on the mode, **the data port is not always on port 20.**



FTP : File Transfer Protocol

- **How it works**

- **A client**

- initiates a control TCP connection
 - Port 21
 - Sends user identification and password
 - Sends command to current directory

- **A server**

- Receives a command,
 - Initiates a TCP data connection to the client side
 - Sends data to the client (one file each time)
 - Closes a connection
 - Open a new connection if another file is required

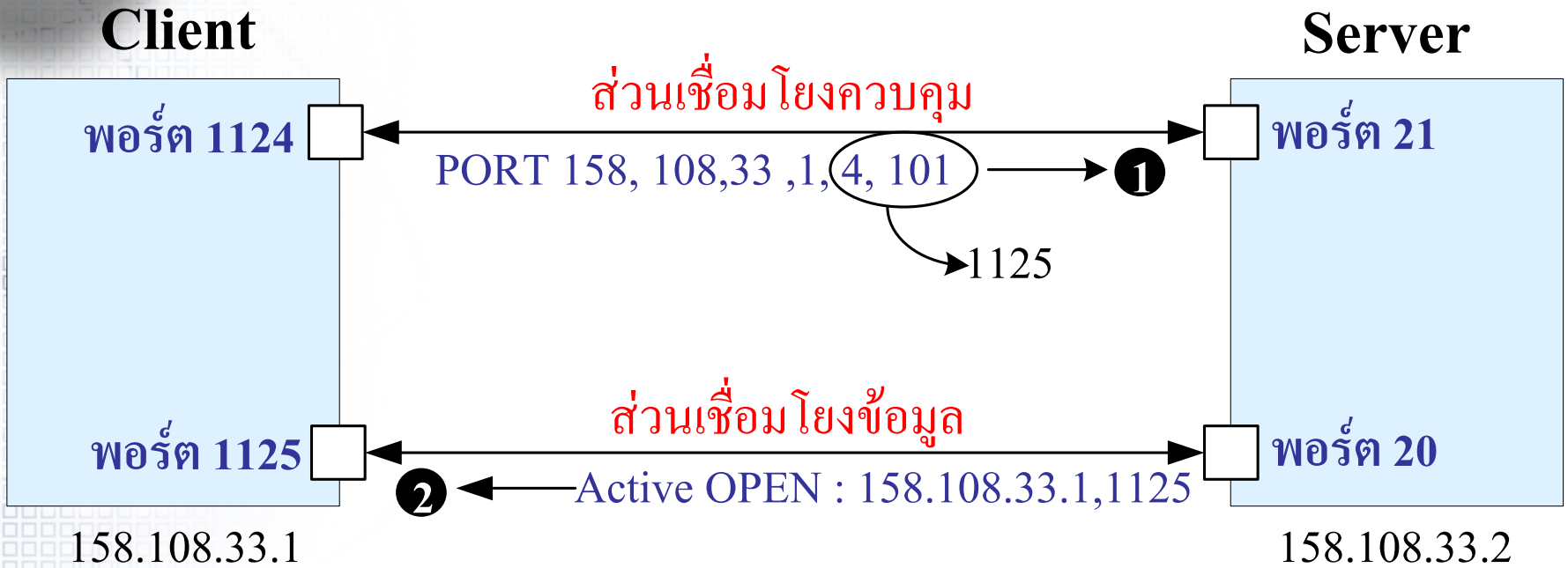
- **The control connection remains open**

- **The server maintains **state** about user**

- User account
 - Current directory



การสร้างส่วนเชื่อมโยงข้อมูล



- FTP ใช้พอร์ต TCP 21 ในการส่งผ่านคำสั่งควบคุมและใช้พอร์ต TCP 20 ส่งข้อมูล
- จากรูปสมมุติพอร์ตประจำส่วนเชื่อมโยงควบคุมของ Client คือ 1124 และเตรียมพอร์ต 1125 รอไว้สำหรับส่วนเชื่อมโยงข้อมูล



การสร้างส่วนเชื่อมโยงข้อมูล (ต่อ)

- Client จะขอเปิดส่วนเชื่อมโยงข้อมูลตามตำแหน่ง (1) โดยส่งรหัสคำสั่ง PORT ตามด้วยอาร์คิวเมนต์หกตัวแยกด้วยจุลภาคคือ IP Address (158.108.33.1) และหมายเลขพอร์ต 4, 101 ซึ่งแสดงถึงพอร์ต 1125 (เลขพอร์ตเป็นรหัส 16 บิต สองชุดติดกัน ดังนั้นตัวเลข 4 , 101 คือ $4*256 + 101 = 1125$)
- ต่อจากนั้น Server จะสถาปนา TCP จากพอร์ต 20 ไปยัง Client ที่พอร์ต 1125 ตามตำแหน่ง 2



Active FTP

- In active mode FTP the client connects from a random unprivileged port ($N > 1024$) to the FTP server's command port, port 21.
- Then, the client starts listening to port $N+1$ and sends the FTP command `PORT N+1` to the FTP server.
- The server will then connect back to the client's specified data port from its local data port, which is port 20.

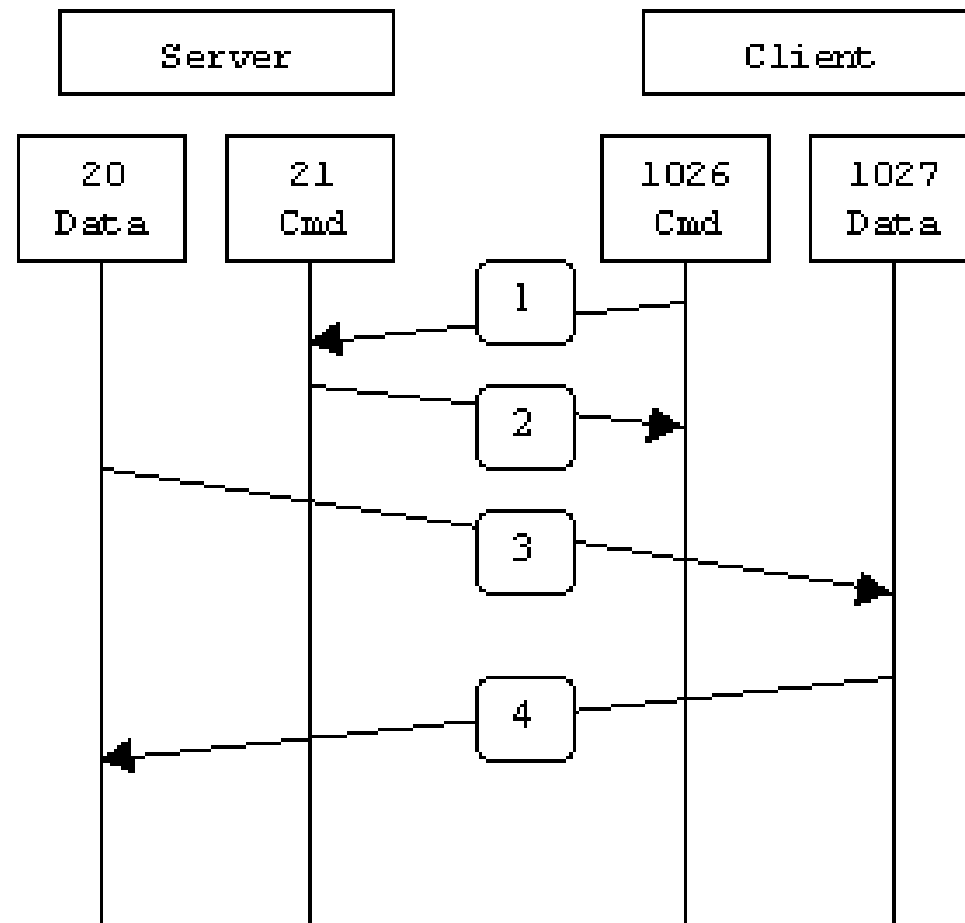


Active FTP

- From the server-side firewall's standpoint, to support active mode FTP the following communication channels need to be opened:
 - FTP server's port 21 from anywhere (Client initiates connection)
 - FTP server's port 21 to ports > 1024 (Server responds to client's control port)
 - FTP server's port 20 to ports > 1024 (Server initiates data connection to client's data port)
 - FTP server's port 20 from ports > 1024 (Client sends ACKs to server's data port)



Active FTP





Passive FTP

- In passive mode FTP the client initiates both connections to the server, solving the problem of firewalls filtering the incoming data port connection to the client from the server.
- When opening an FTP connection, the client opens two random unprivileged ports locally ($N > 1024$ and $N+1$).
- The first port contacts the server on port 21, but instead of then issuing a PORT command and allowing the server to connect back to its data port, the client will issue the PASV command.
- The result of this is that the server then opens a random unprivileged port ($P > 1024$) and sends the PORT P command back to the client. The client then initiates the connection from port $N+1$ to port P on the server to transfer data.

Issuing = การปล่อยออก

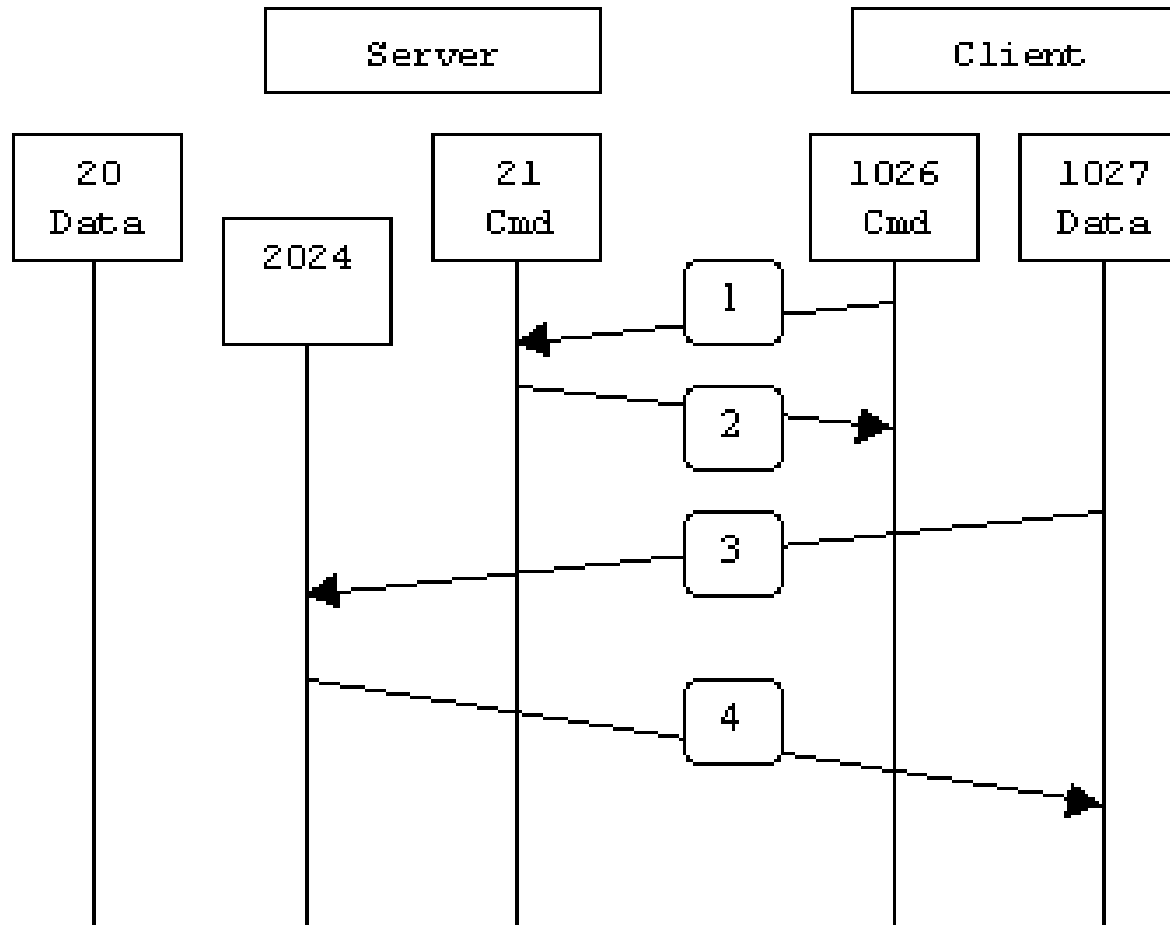


Passive FTP

- From the server-side firewall's standpoint, to support passive mode FTP the following communication channels need to be opened:
 - FTP server's port 21 from anywhere (Client initiates connection)
 - FTP server's port 21 to ports > 1024 (Server responds to client's control port)
 - FTP server's ports > 1024 from anywhere (Client initiates data connection to random port specified by server)
 - FTP server's ports > 1024 to remote ports > 1024 (Server sends ACKs (and data) to client's data port)



Passive FTP





FTP Softwares

- **FTP Client**

- **Command line**
- **gftp**
- **WS-FTP Pro**
- **Cute-ftp**
- **FTP ผ่าน Browser**

- **FTP Server**

- **FTP ที่มากับ IIS**
- **WS_FTP Server**
- **Serv-U---FTP Server for Windows**
- **ArGoSoft FTP Server**
- **Wuftp**
- **Vsftp**



ประเภทของล็อกอินในบริการ FTP

- ล็อกอินด้วยผู้ใช้ที่มีอยู่ในระบบ (Real FTP) ผู้ใช้บริการจะต้องมีชื่อ บัญชีผู้ใช้อยู่จริงบนเซิร์ฟเวอร์ สามารถเปลี่ยนไคลเอนต์ไปที่อื่นได้
- ล็อกอินด้วยผู้ใช้ที่มีอยู่ในระบบแต่จำกัดขอบเขต (Guest FTP) คล้ายกับ Real FTP ต่างตรงที่ ไม่สามารถเปลี่ยนไคลเอนต์ไปไหนได้เกินขอบเขตที่เซิร์ฟเวอร์กำหนด
- ล็อกอินด้วยผู้ใช้ที่ไม่มีอยู่ในระบบ (Anonymous FTP) การบริการ FTP แบบที่เปิดเสรีให้คนทั่วโลกมาใช้บริการ คงเป็นไปได้ที่จะมานั่งสร้างบัญชีผู้ใช้ให้รองรับคนทั่วโลก แบบนี้จึงกำหนดให้ล็อกอินโดยใช้ชื่อ anonymous ส่วนรหัสผ่านให้ระบุเป็นรูปแบบของ e-mail address



การตรวจสอบว่าติดตั้ง vsftpd แล้วหรือไม่

- ตรวจสอบจาก shell prompt

- # rpm -q vsftpd

- ตรวจสอบจาก XWindow

- จากเมนู System Settings → Add/Remove Applications

- รายการ Server → FTP Server



การติดตั้ง vsftp จาก Shell Prompt (RPM)

- โปรแกรม vsftp อยู่ในแผ่นที่ 3
- ขั้นตอนติดตั้งเป็นดังนี้ :

```
root@training:/  
File Edit View Terminal Tabs Help  
[root@training /]# mount /media/cdrom  
mount: block device /dev/hdc is write-protected, mounting read-only  
[root@training /]# cd /media/cdrom/Fedora/RPMS  
[root@training RPMS]# rpm -ivh vsftpd-2.0.3-1.i386.rpm  
warning: vsftpd-2.0.3-1.i386.rpm: Header V3 DSA signature: NOKEY, key  
ID 4f2a6fd2  
Preparing...  
##### [100%]  
 1:vsftpd  
##### [100%]  
[root@training RPMS]# cd /  
[root@training /]# umount /media/cdrom  
[root@training /]# █
```



การ Start vsftp

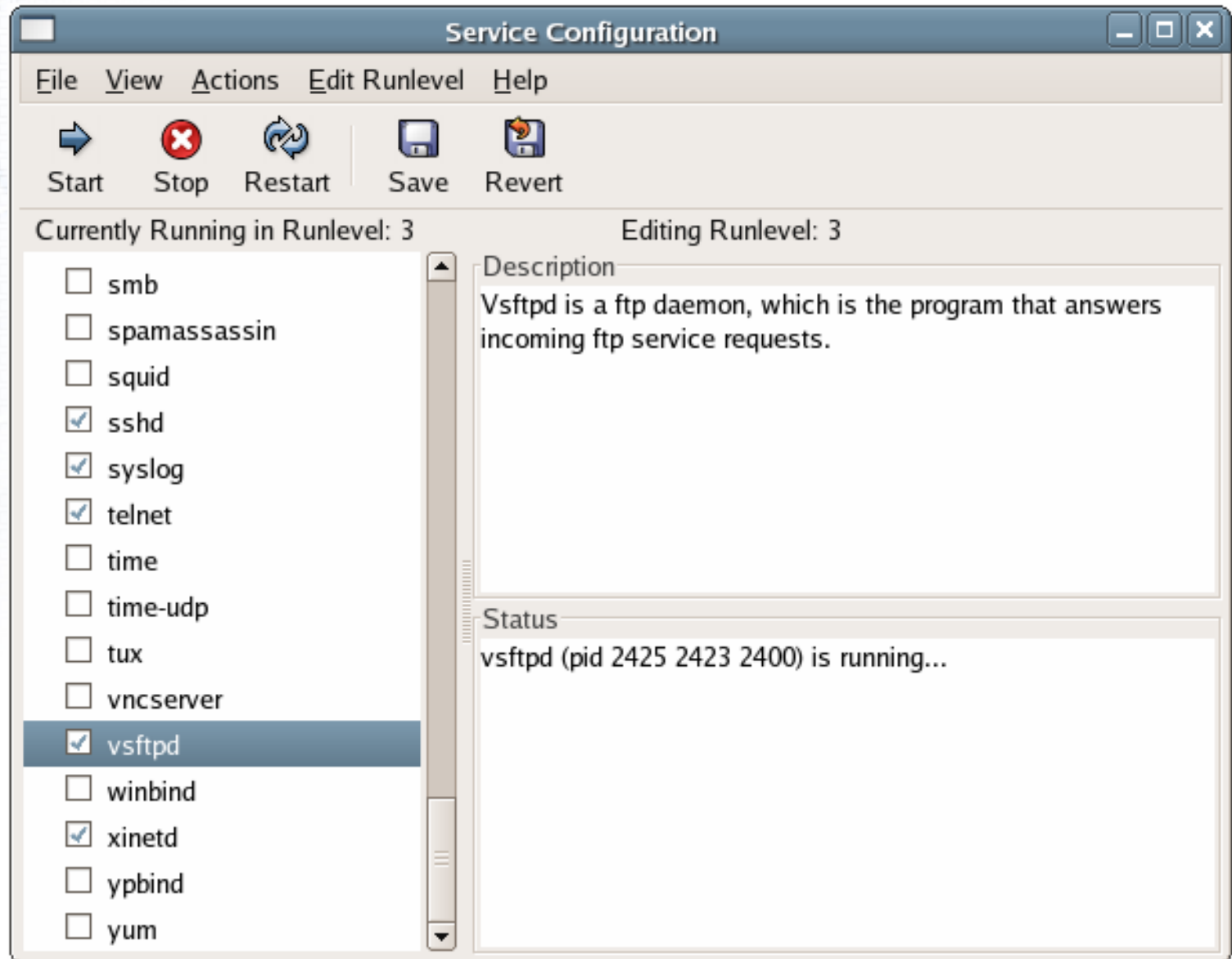
- การ Start จาก shell prompt
- การ Start จาก XWindow
 - System Settings → Server Settings → Services
- การ Start จาก shell prompt ด้วยคำสั่ง setup

การ start จาก shell prompt

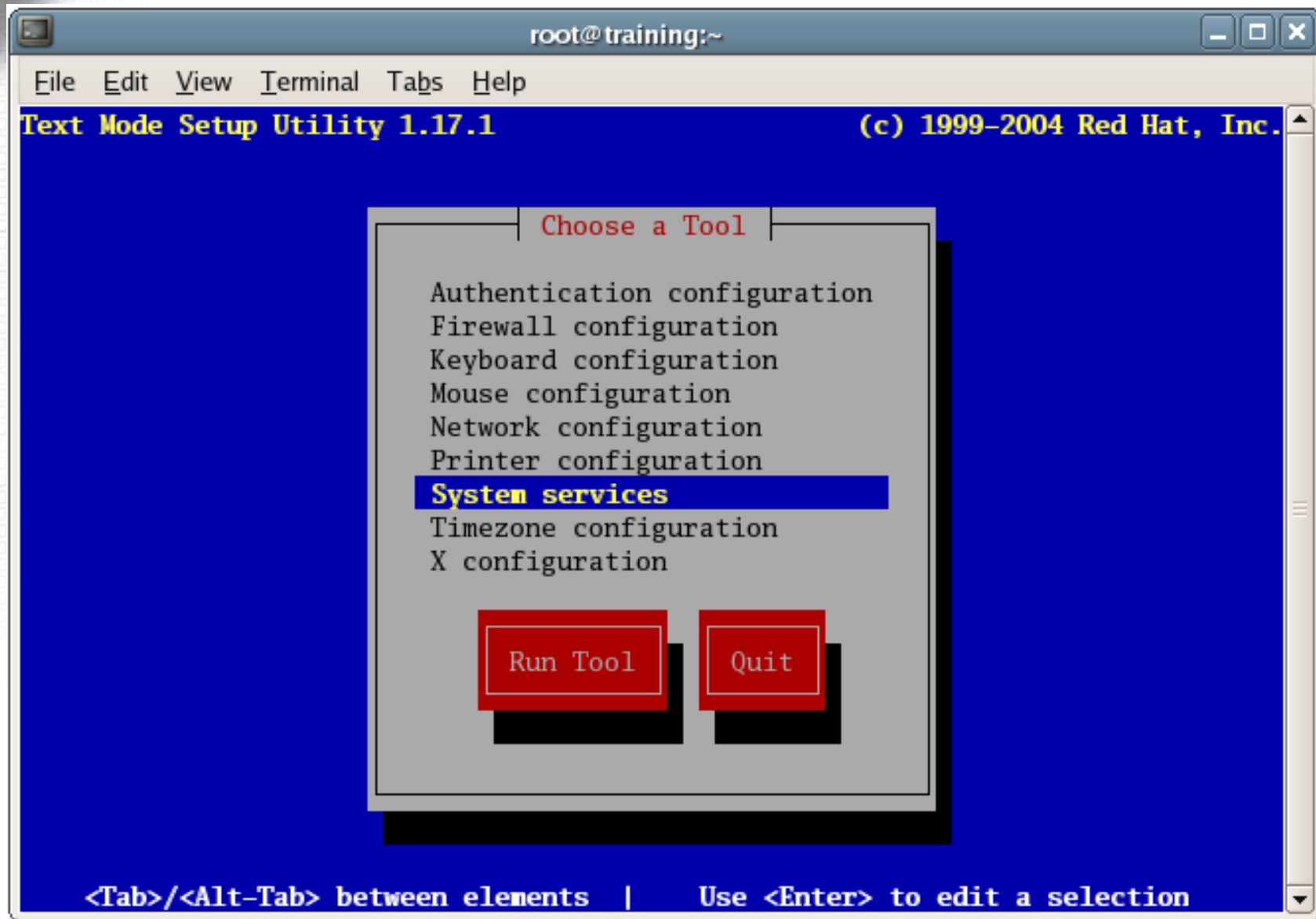
```
root@training:/  
File Edit View Terminal Tabs Help  
[root@training /]# /etc/rc.d/init.d/vsftpd start  
Starting vsftpd for vsftpd: [ OK ]  
[root@training /]# /etc/init.d/vsftpd restart  
Shutting down vsftpd: [ OK ]  
Starting vsftpd for vsftpd: [ OK ]  
[root@training /]# service vsftpd restart  
Shutting down vsftpd: [ OK ]  
Starting vsftpd for vsftpd: [ OK ]  
[root@training /]# service vsftpd status  
vsftpd (pid 2400) is running...  
[root@training /]# █
```



ກນຮ start ວາກ XWindow



การ start จาก shell prompt ด้วยคำสั่ง setup





การ start จาก shell prompt ด้วยคำสั่ง setup (ต่อ)

```
root@training:~  
File Edit View Terminal Tabs Help  
ntsysv 1.3.20 - (C) 2000-2001 Red Hat, Inc.  
  
Services  
What services should be automatically started?  
  
[ ] tux  
[ ] vncserver  
[x] vsftpd  
[ ] winbind  
[*] xfs  
[*] xinetd  
[ ] ypbind  
[ ] yun #  
  
Ok Cancel  
  
Press <F1> for more information on a service.
```



การคอนฟิก vsftp

- ไฟล์คอนฟิกหลักของ vsftp คือ `/etc/vsftpd/vsftpd.conf`
- ค่า Default หลังจากการติดตั้ง vsftpd เป็น ftp แบบ
 - Real FTP คือ ล็อกอินด้วยผู้ใช้ที่มีอยู่ในระบบ
 - `local_enable = YES`
 - Anonymous FTP คือ ล็อกอินด้วยผู้ใช้ที่ไม่มีอยู่ในระบบ
 - `anonymous_enable=YES`
- ไฟล์คอนฟิกที่เกี่ยวข้องกับ User (Default) มี 2 ไฟล์คือ
 - `/etc/vsftpd/ftpusers`
 - `/etc/vsftpd/user_list`



คำแนะนำในการคอนฟิก vsftpd

ข้อความส่วนต้นของไฟล์ `/etc/vsftpd/vsftpd.conf` แนะนำดังนี้ :

```
# Example config file /etc/vsftpd/vsftpd.conf
```

```
#
```

```
# The default compiled in settings are fairly paranoid. This sample file
```

```
# loosens things up a bit, to make the ftp daemon more usable.
```

```
# Please see vsftpd.conf.5 for all compiled in defaults.
```

```
#
```

```
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
```

```
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
```

```
# capabilities.
```

```
#
```



ไฟล์ `/etc/vsftpd/ftpusers` และ `/etc/vsftpd/user_list`

- **`/etc/vsftpd/ftpusers`**

Users that are not allowed to login via ftp

- **`/etc/vsftpd/user_list`**

- vsftpd userlist

- If `userlist_deny=NO`, only allow users in this file

- If `userlist_deny=YES` (default), never allow users in this file, and do not even prompt for a password.

- Note that the default vsftpd pam config also checks `/etc/vsftpd/ftpusers` for users that are denied.



การคอนฟิกให้เป็น Anonymous FTP

- ต้องกำหนดค่า `anonymous_enable=YES` ในไฟล์ `/etc/vsftpd/vsftpd.conf`
- ค่า default นั้น user ไม่สามารถ upload ไฟล์ได้ แต่ถ้าต้องการให้ user สามารถ upload ไฟล์ได้ ต้องกำหนด
 - `write_enable=YES`
 - `anon_upload_enable=YES`
 - ต้องกำหนด permission ในตำแหน่ง `/var/ftp/pub` (ตำแหน่ง `/etc/ftp` เป็นตำแหน่งของ Anonymous FTP เปลี่ยน Permission ไม่ได้นะ) ให้ others สามารถ write ได้ (757)
- ถ้าต้องการให้ user สามารถสร้าง directory ได้ต้องกำหนด
 - `anon_mkdir_write_enable=YES`
- ถ้าสร้างไดเรกทอรีใหม่ได้แต่พอ upload เข้าไปในไดเรกทอรีแล้วมองไม่เห็นไฟล์ต้องกำหนด
 - `anon_world_readable_only=NO` (ไม่มีค่านี้ใน default)
- ถ้าต้องการให้สามารถลบไฟล์และ Directory ได้ต้องกำหนด
 - `anon_other_write_enable=YES` (ไม่มีค่านี้ใน default)



การคอนฟิกให้เป็น Real FTP

- คำ Default ของ vsftp เป็น Real FTP อยู่แล้ว
 - `local_enable = YES`



การคอนฟิกให้เป็น Guest FTP

- การกำหนดไม่ให้ user สามารถเปลี่ยนไดเรกทอรีไปที่อื่นได้ :
 - `chroot_local_user=YES` (ไม่มีค่านี้ใน default)
- ถ้าต้องการให้ user บางคนสามารถ change directory จาก home directory ของตัวเองไปที่อื่นได้ก็ให้ทำดังนี้ :
 - `chroot_list_enable=YES`
 - ป้อนชื่อ user ที่จะอนุญาตให้ chang directory ได้ไว้ที่ `/etc/vsftpd/chroot_list` (ต้องสร้างไฟล์ขึ้นมาใหม่ โดยตำแหน่งและชื่อไฟล์นี้เป็น Default)
- ถ้าเราไม่ต้องการเก็บชื่อ user ที่อนุญาตให้ change directory ได้ไว้ในไฟล์ที่เป็น Default คือ `/etc/vsftpd/chroot_list` ก็สามารถทำได้คือ :
 - `chroot_list_file=ชื่อไฟล์` เช่น `chroot_list_file=/root/admin_ftp_user`
 - สร้างไฟล์ดังกล่าวขึ้นมา



การคอนฟิกให้เป็น Guest FTP (ต่อ)

- ในกรณีที่ต้องการให้ user บางคนสามารถ change directory ได้และต้องการให้ user ดังกล่าวซึ่งอาจจะเป็น system admin สามารถ upload ไฟล์ไปไว้ที่ตำแหน่งของ anonymous ftp ได้ก็ให้คอนฟิกดังนี้
 - ให้เปิดบริการ anonymous ftp โดยให้คอนฟิก anonymous ftp เป็นแบบ default คือต้องเปลี่ยนค่าต่าง ๆ ต่อไปนี้กลับไปดังเดิม (ด้วยการเอาเครื่องหมาย # ไว้ข้างหน้า)
 - `anon_upload_enable=YES`
 - `anon_mkdir_write_enable=YES`
 - `anon_other_write_enable=YES`
 - เพิ่ม user ที่เป็น system admin ขึ้นมา และให้เพิ่ม group ใหม่ขึ้นมา โดยให้ user ที่เป็น system admin ให้สังกัดอยู่ใน group ดังกล่าว เช่นอาจจะตั้งชื่อ group ใหม่ว่า sysadmin
 - กำหนดสิทธิ์ไดเรกทอรี /var/ftp (หรือ /var/ftp/pub แล้วแต่นโยบาย) ให้สังกัดกลุ่มของ sysadmin และกำหนด permission ในตำแหน่งดังกล่าวให้ group สามารถ write ได้ แต่ other ไม่สามารถ write ได้



Site Options - 192.168.1.100

- Host Info
- Startup
- Session
- Advanced
- SSL

Advanced

Server type: FTP

Host type: Automatic detect

Firewall: NONE

Use Passive mode for data connections

Connection retries (0 - 40 attempts): 0

Connection retry delay (5 - 300 seconds): 30

Network timeout (5-3600 seconds): 65

Remote port (usually 21): 21

Keep alive (10-3600 seconds): 0

OK



Cancel

Help

Internet Options

- General
- Security
- Privacy
- Content
- Connections
- Programs
- Advanced

Settings:

- Show friendly URLs
- Show Go button in Address bar
- Underline links
 - Always
 - Hover
 - Never
- Use inline AutoComplete
- Use Passive FTP (for firewall and DSL modem compatibility)
- Use smooth scrolling
-  HTTP 1.1 settings
 - Use HTTP 1.1
 - Use HTTP 1.1 through proxy connections
-  Microsoft VM
 - Java console enabled (requires restart)
 - Java logging enabled
 - JIT compiler for virtual machine enabled (requires restart)

Restore Defaults

OK

Cancel

Apply

ตัวอย่างการกำหนด Passive FTP