



# FTP

---

## *File Transfer Protocol*

---

CIS 68C2

UNIX Network Administration

# FTP

- FTP – File Transfer Protocol
  - ✗ Allows upload and downloading of files
  - ✗ One of the oldest TCP/IP services
    - ✗ And still widely in use
  - ✗ Client/Server
  - ✗ Advantages over HTTP file transfer
    - ✗ Allows inspection of file tree, includes file sizes and timestamps
    - ✗ No HTML code required
  - ✗ Caution!
    - ✗ Improperly configured ftp servers are security risks

# FTP

- Two Primary File Transfer Modes
  - ✗ ASCII (plain text)
    - ✗ End-of-line translation occurs between platforms
    - ✗ Data is consider to be only 7 bits (high order bit is lost)
  - ✗ Binary image
    - ✗ Data is transferred raw (not interpreted)
  - ✗ Other modes (EBCDIC, local) are rarely ever used
  - ✗ Mode must be set before transfer begins
    - ✗ Many clients have an auto-select mode
      - ✗ File suffix/name guides selection of transfer mode
    - ✗ Common mistake to transfer a binary file in ASCII mode
      - ✗ The download is corrupted

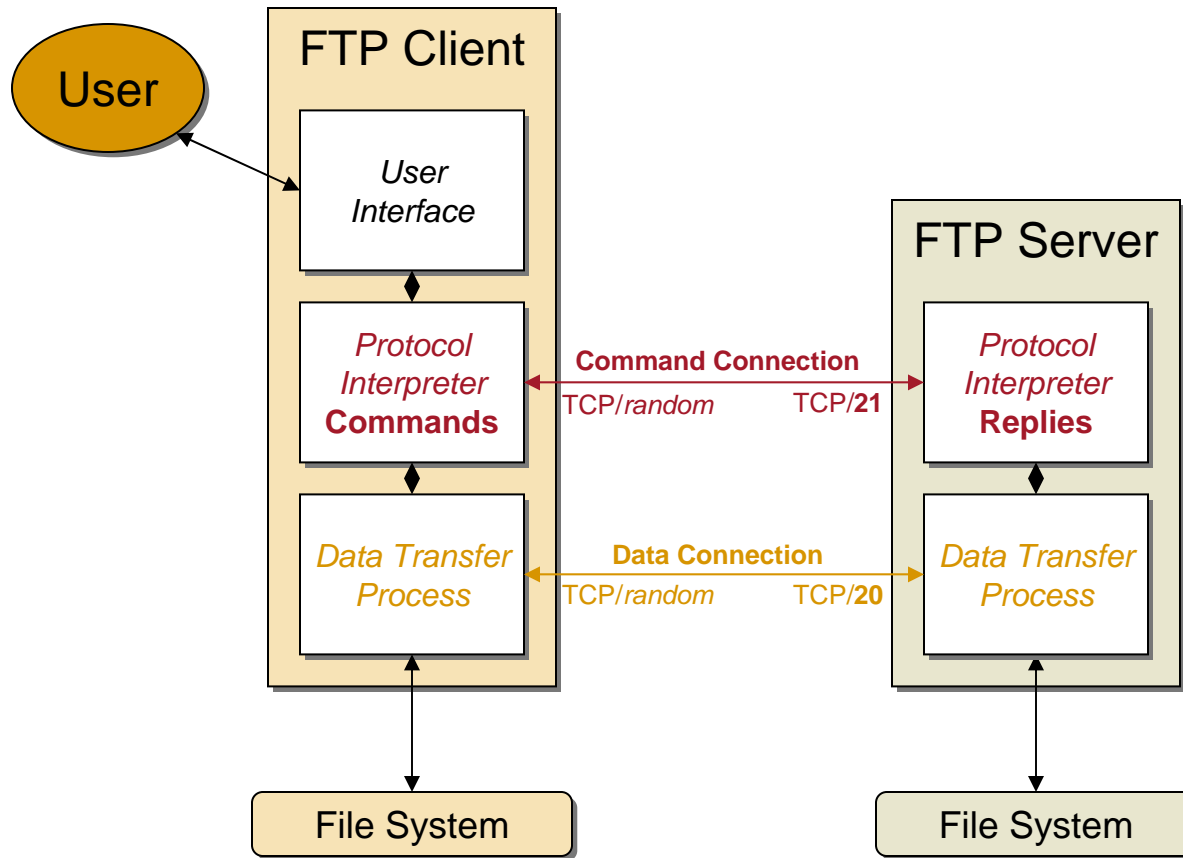
# FTP

## □ FTP Communication

- ✗ Uses 2 TCP ports: 20 (data) and 21 (command)
  - ✗ Data port defined by RFC to be the command port - 1
- ✗ Client
  - ✗ Initiates command connection to server's TCP port 21
  - ✗ Selects random high numbered port to use for data connection
  - ✗ Sends PORT command
    - ✗ Includes client's IP address and high numbered port
  - ✗ Listens for data connection on high numbered port
- ✗ Server
  - ✗ Initiates data connection to client
    - ✗ Uses IP and port number given by client's PORT command

# FTP

## □ FTP – Single Connection



# FTP

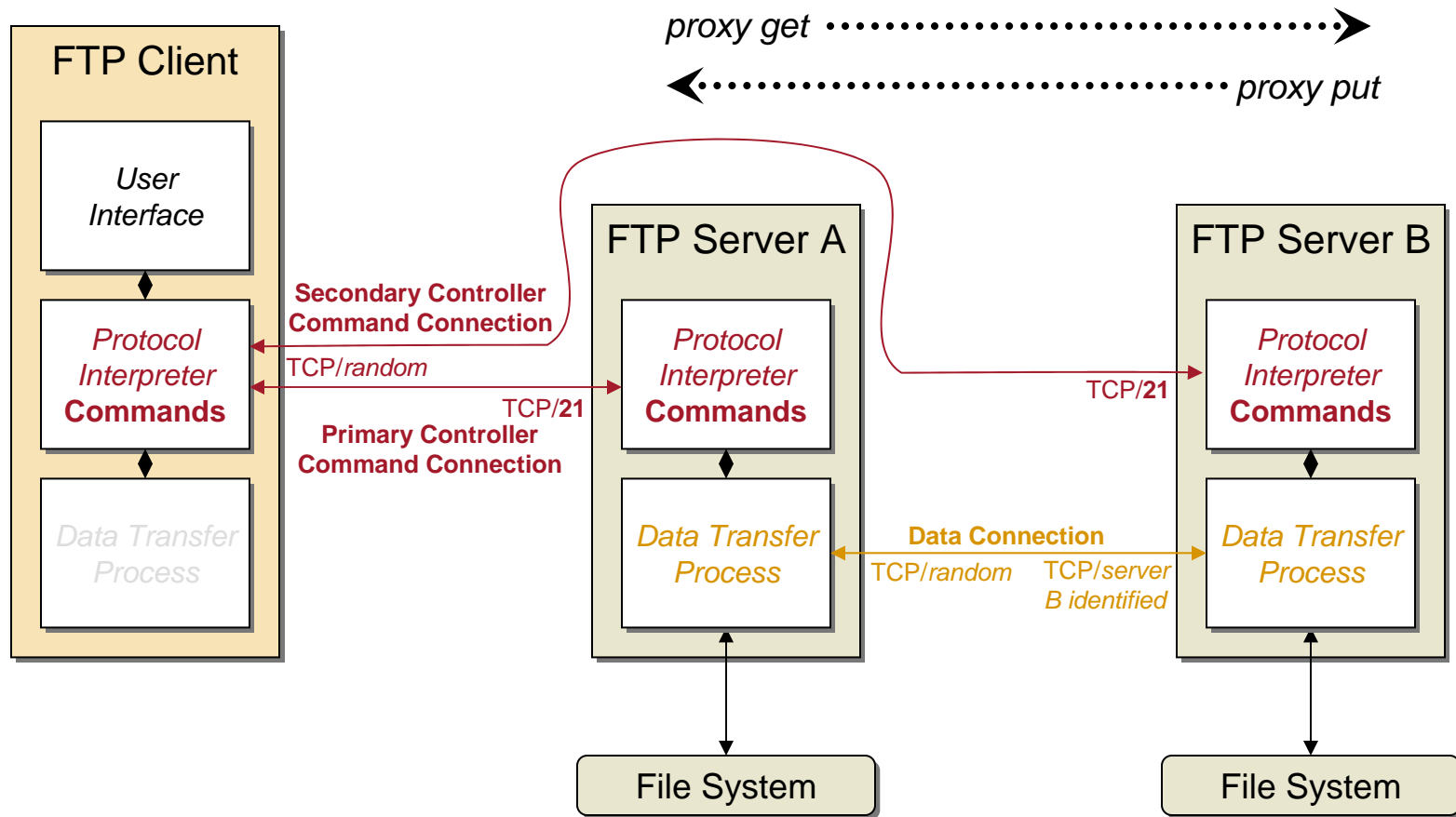
## □ FTP Communication

### ✗ PASV command

- ✗ Requests server to return an IP / port number
  - ✗ Client establishes the data connection, not the server
  - ✗ Server listens on that port number for client's connection
- ✗ Allows FTP to...
  - ✗ work through firewalls and NAT
  - ✗ act as a proxy
  - ✗ support site mirroring
- ✗ Typically used instead of PORT command
  - ✗ But both can be used to override both connection ends
  - ✗ PASV mode is considerably more secure

# FTP

## □ FTP – Proxy Connection



# FTP

- FTP – Proxy Connection
  - ✗ Secondary server must support PASV command
    - ✗ It cannot initiate the data connection to FTP Server A
  - ✗ GET transfers from primary to secondary
  - ✗ PUT transfers from secondary to primary
  - ✗ Security Alert!
    - ✗ Proxy exposes the difficult to trace Bounce Attack
      - ✗ Using proxy FTP to connect to WKS port (mail, news, etc) and sending instructions
    - ✗ Eases brute force password guessing
    - ✗ 3rd party transfers are disabled by default on most modern servers

# wu-ftp

- A leading, feature-rich FTP server implementation
  - ✗ Used by Red Hat and many other UNIX distributions
  - ✗ Makes distinction between 3 different types of users
    - ✗ Real Users
    - ✗ Guests
    - ✗ Anonymous Users

<b>Additional Features beyond RFC 959</b>	
Advanced logging (commands, transfers)	On-the-fly compression and archiving
User classifications (type and location)	Per-class limits
Per directory upload permissions	Restricted guest accounts
System wide and per directory messages.	Directory alias
cdpath	Filename filtering
Virtual hosts	

# wu-ftp

## □ wu-ftp User Types

### × Real Users

- × Login to ftp with real username and password
- × Can access entire disk structure
- × Security risk! - Use with extreme caution!

### × Guests

- × Login to ftp with real username and password
- × Chroot'ed to user's home directory – cannot escape

### × Anonymous Users

- × User: **anonymous** or **ftp**; Password: *your-email-address*
- × Chroot'ed to common, public ftp directory

# wu-ftpd

## □ Configuration Files

- ✗ /etc/ftpaccess
  - ✗ Main configuration file for most settings
- ✗ /etc/ftpconversions
  - ✗ Configuration file for on-the-fly conversions
- ✗ Generally deprecated
  - ✗ /etc/ftphosts
    - ✗ List of hosts allowed/denied ftp access
  - ✗ /etc/ftpusers
    - ✗ List of users allowed/denied ftp access

# Additional Information

- wu-ftp documentation
  - ✗ `/usr/share/doc/wu-ftpd-*`
- Many wu-ftpd related documents
  - ✗ <http://www.wu-ftpd.org/>
  - ✗ <http://www.wu-ftpd.org/rfc/>
  - ✗ <http://www.landfield.com/wu-ftpd/>
- CERT FTP Articles
  - ✗ Anonymous FTP Abuses & Configuration Guidelines
    - ✗ [http://www.cert.org/tech\\_tips/anonymous\\_ftp\\_abuses.html](http://www.cert.org/tech_tips/anonymous_ftp_abuses.html)
    - ✗ [http://www.cert.org/tech\\_tips/anonymous\\_ftp\\_config.html](http://www.cert.org/tech_tips/anonymous_ftp_config.html)
  - ✗ Bounce Attacks
    - ✗ [http://www.cert.org/tech\\_tips/ftp\\_port\\_attacks.html](http://www.cert.org/tech_tips/ftp_port_attacks.html)
- RFCs
  - ✗ 959 – FTP Protocol
  - ✗ 2577 – FTP Security Considerations