NSCOM01

TCP-based Network Application Protocols

3rd Term– AY2022 – 2023

Instructor: Dr. Marnel Peradilla

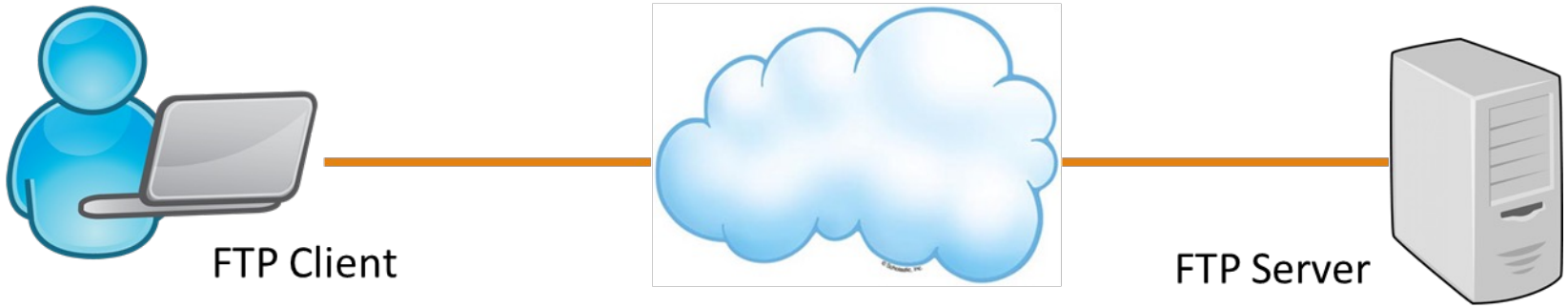
SPIRAL REVIEW: TRANSPORT SERVICES

- **The Transport Control Protocol (TCP) is a connection-oriented transport protocol used in TCP/IP networks**
- **Provides reliable communication between pairs of processes (TCP users) across a variety of reliable and unreliable networks**
  - Features:
  1. Stream-oriented – Data is sent in segments but handled as streams
  2. Connection Oriented – Includes mechanisms to establish, track state and terminate a connection between 2 hosts
  3. Guaranteed delivery – packets are acknowledged by receiving hosts
  4. Flow control - Data transmission adapts to network conditions and host capability
  5. Ordered delivery – Segments may arrive out of-order but are reassembled in the correct sequence

FTP

FILE TRANSFER PROTOCOL

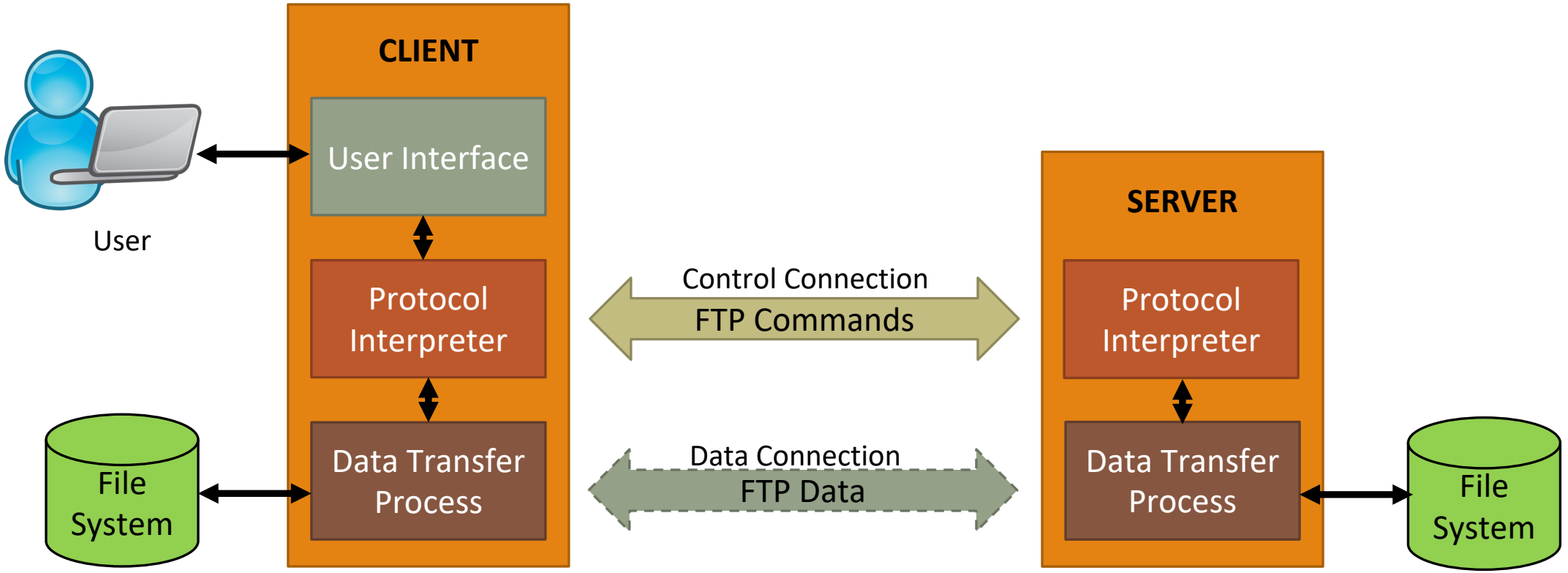
- One of the earliest application protocols of the TCP/IP suite that was developed to allow sharing of files across a network
- Abstracts the underlying file storage method of a system so that a common mechanism may be used to manage, download and upload files among hosts of different types
- Operates using client-server model using TCP as the transport layer to provide a reliable data transfer service, hence can be practically used across the Internet
- Currently defined by RFC 959 as an Internet standard



FTP BASIC OPERATION

- **FTP requires 2 connection between client and server: a control connection and a data connection**
  - Control connection carries FTP commands and responses
  - Data connection carries the file data being transferred
- **FTP server listens for incoming connections using TCP port 21 (FTP Command)**
- **Client connects and communicates needed operations with the server through the control connection. Protocol Interpreter (PI) takes care of receiving and replying to FTP commands**
- **When a file transfer needs to happen, a data connection is separately established between client and server to transfer file data then closed when the transfer is completed. Data Transfer Process (DTP) takes care of sending and receiving the file data stream or directory listing**
- **Control connection is closed when transaction is completed**

FTP BASIC OPERATION



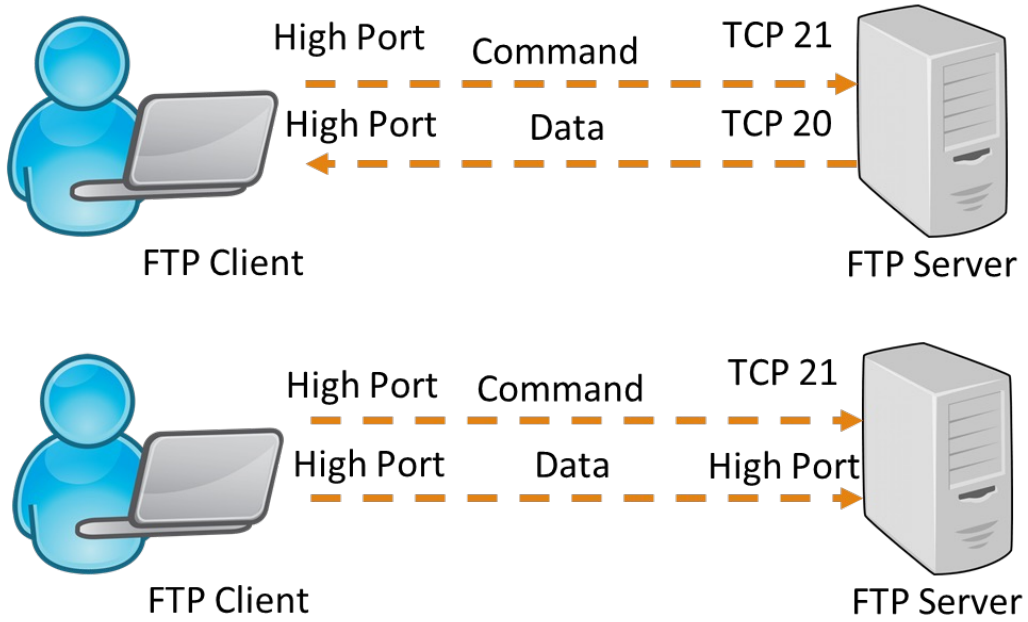
FTP DATA TRANSFER METHODS

❑ Active Mode

- FTP server initiates the data connection to the client from port 20 to a high range port on the client then
- Uses the same data connection for all transfers for the current FTP session

❑ Passive Mode

- FTP client instructs the server what port to bind to, then client initiates the connection to the server port.
- Client creates a new data connection for each file it transfers
- More commonly used by current FTP clients due to firewalls normally set to not allow incoming connections to a network



FTP COMMANDS

- **FTP commands always follow the general format**

```
<command> ::= <mnemonic> [<parameter>] <CRLF>
<parameter> ::= <SP> <string>
```

- **FTP commands fall into 3 groups:**
  - Access control commands - Commands that are part of the user login and authentication process, are used for resource access, or are part of general session control
  - Transfer parameter commands - Commands that specify parameters for how data transfers should occur
  - FTP service commands - Commands that perform file operations, such as managing, sending and receiving files

FTP COMMANDS

❑ Common Access Control Commands

Mnemonic	Command	Function
USER	User Name	Identifies the user attempting to establish an FTP session.
PASS	Password	Specifies the password for the user given previously by the USER command during login authentication.
CWD	Change Working Directory	Allows the user to specify a different directory for file transfer during an FTP session
QUIT	Logout	Terminates the FTP session and closes the control connection.

FTP COMMANDS

❑ Common Transfer Parameter Commands

Mnemonic	Command	Function
PORT	Data Port	Used to tell the FTP server that the client wants to accept an active data connection on a specific port number.
PASV	Passive	Requests that the FTP server allow the client to initiate passive data connections. (Server is supposed to reply with port it will use for data conn)

FTP COMMANDS

❑ Common Service Commands

Mnemonic	Command	Function
RETR	Retrieve	Tells the server to send the user a file.
STOR	Store	Sends a file to the server.
DELE	Delete	Deletes a specified file on the server.
RMD	Remove Directory	Deletes a directory on the server.
MKD	Make Directory	Creates a directory.
LIST	List	Requests a list of the contents of the current directory from the server, including both names and other information.
ABOR	Abort	Tells the server to abort the last FTP command and/or the current data transfer.

FTP REPLIES

- FTP Replies consist of a 3-digit response code followed usually by a response argument containing a description of the reply, and optional additional parameters as needed
- First response code digit indicates in general whether a command was successful or not:

Value	Meaning	Description
1	Positive Preliminary Reply	An initial response indicating that the command has been accepted and processing of it is still in progress. The user should expect another reply before a new command may be sent.
2	Positive Completion Reply	The command has been successfully processed and completed.
3	Positive Intermediate Reply	The command was accepted, but processing of it has been delayed, pending receipt of additional information. Commonly used in the middle of command sequences.
4	Transient Negative Completion Reply	The command was rejected and no action was taken, but the error is temporary and the command may be tried again.
5	Permanent Negative Completion Reply	The command was rejected and no action was taken. Trying the same command again is likely to result in another error.

FTP REPLIES

- Second response code digit indicates the functional group category of the response

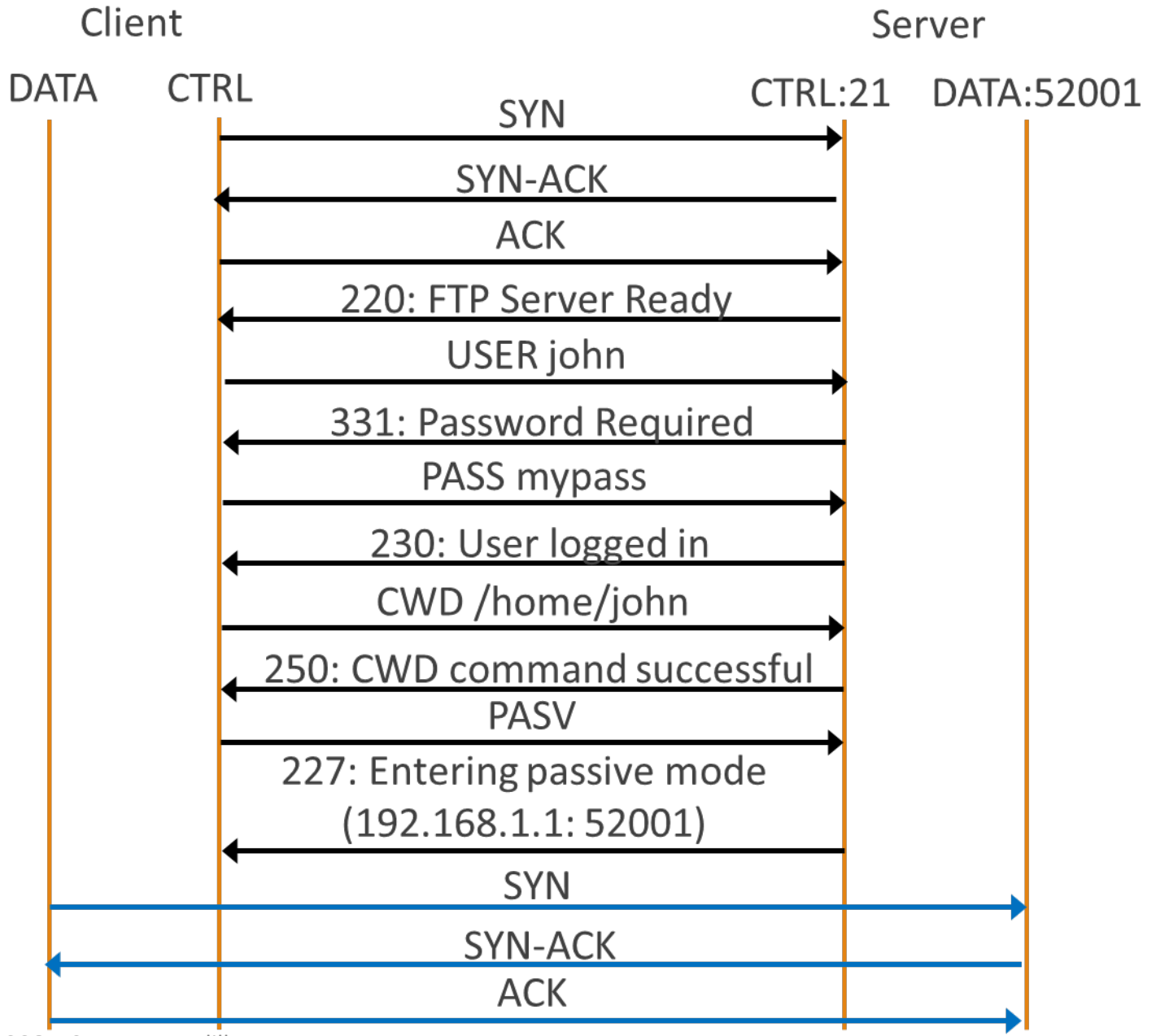
Value	Meaning	Description
0	Syntax	Syntax errors or miscellaneous messages.
1	Information	Replies to requests for information, such as status requests.
2	Connections	Replies related to the control connection or data connection.
3	Authentication and Accounting	Replies related to login procedures and accounting.
4	Unspecified	Not defined.
5	File System	Replies related to the server's file system.

- Third response code digit indicates a specific type of message within each of the functional groups

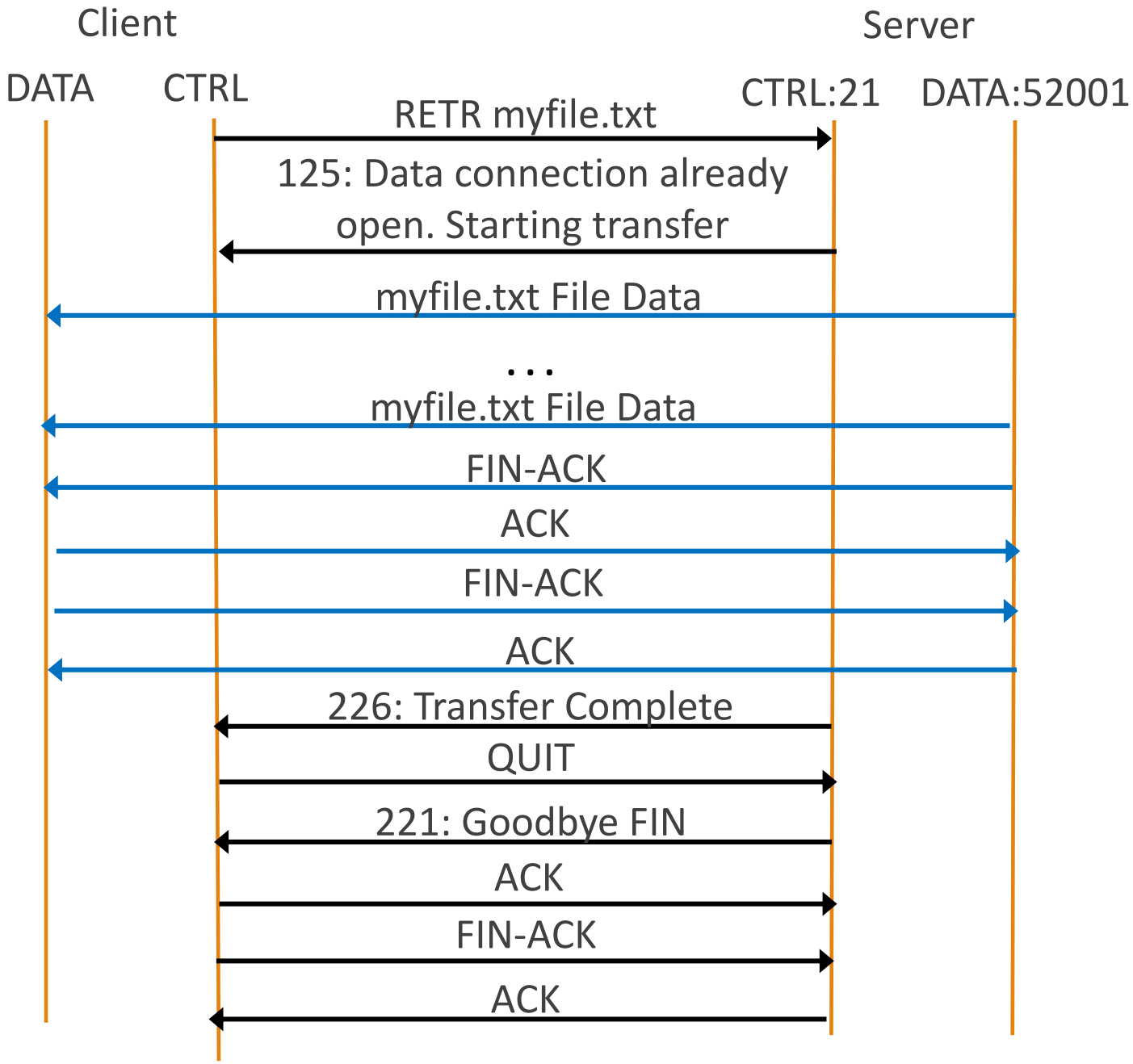
SAMPLE FTP REPLIES

- **Code 331 is used to further request for a password after receiving the username**
  - 3 → Positive Intermediate Reply (username was received but need additional input)
  - 3 → Authorization and Accounting
  - 1 → Message 1 within the Authorization and Accounting function
- **Code 530 is used to indicate a failed login to the server:**
  - 5 → Permanent Negative Completion
  - 3 → Authorization and Accounting
  - 0 → Message 0 within the Authorization and Accounting function

SAMPLE FTP EXCHANGE SEQUENCE (1/2)



SAMPLE FTP EXCHANGE SEQUENCE (2/2)



FTP CONSIDERATIONS

- **Commands and data are sent in plaintext- hence all login credentials and data from unencrypted files can be captured from the networked using packet sniffers**
- **It doesn't use strong authentication.**
- **It is based on password logins which can be brute forced to gain unauthorized access**
- **SFTP, or secure FTP, is a program that uses SSH to transfer files.**
  - Functionally similar to FTP but is a different protocol (not compatible with regular FTP)
  - Encrypts both commands and data for protection against sniffing
  - Supports methods for user authentication

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."